MAU34106 - Galois Theory

Adam Keilthy

Trinity College Dublin

Contents

1 Introduction

Historically, Galois theory was motivated by the study of solutions to polynomial equations, with the end goal of making solving them "easy". Here, "easy"[1] could be taken to mean something along the lines of

- Writing down exact formulas for the solutions,
- Reduction of the equation to a simpler one,
- Saying literally anything about a number α other than α is a number such that $f(\alpha) = 0$.

We aim to provide this information by using symmetries of the solutions. Just as complex solutions to polynomials with real coefficients come in complex conjugate pairs (*symmetry*), the roots of a general polynomial will satisfy some symmetry constraints relative to the field in which its coefficients are defined. For example, if $f(x) \in \mathbb{Q}[x]$ and $\sqrt{2}$ is a root of $f(x)$, then so is $-\sqrt{2}$. These are the types of symmetries that Galois theory aims to exploit to say something about solutions to equations.

Before we can make much progress into Galois theory, we need to do a fair bit of field theory first, and so, rather than dive into a refresher on rings, we will first briefly discuss one of the most famous results of Galois theory, and why it is maybe surprising (or not): the insolubility of the quintic.

Theorem 1.1. *There does not exist a general formula, expressible in terms of radicals (square roots, cube roots, etc) describing the roots of a quintic equation*

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

[1] To quote Dotsenko: "One cannot find quotation marks large enough to emphasize the futility of that notion"

1.1 Solving polynomial equations

Linear equations

Given a (monic) linear equation

$$x + b = 0$$

we can easily find the solution $x = -b$.

Quadratic equations

Given a quadratic equation

$$x^2 + bx + c = 0$$

we can easily solve this, if $b = 0$. However, by completing the square, we obtain an equivalent equation

$$\left(x + \frac{b}{2}\right)^2 + c - \frac{b^2}{4} = 0$$

which implies

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

and hence

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

giving the familiar formula with $a = 1$.

Cubic equations

Given a cubic equation

$$x^3 + ax^2 + bx + c = 0$$

we can really only solve this if $a = b = 0$. Completing the cube and letting $y = x + \frac{a}{3}$ gives us a simpler equation

$$y^3 + py + q = 0, \quad p = b - \frac{a^3}{3}, \quad q = c - \frac{ab}{3}$$

but still not one we can easily solve. However, we can employ a very clever trick due to the Italian mathematicians Tartaglia and Cardano, and reduce this to a quadratic equation. Suppose we have a solution of the form $y = z_1 + z_2$ for some complex z_1, z_2. Then

$$(z_1 + z_2)^3 + p(z_1 + z_2) + q = 0$$

which we can rearrange as

$$(z_1^3 + z_2^3 + q) + (z_1 + z_2)(3z_1z_2 + p) = 0.$$

Hence, if we could find z_1, z_2 such that

$$z_1^3 + z_2^3 = -q, \quad \text{and} \quad 3z_1z_2 = -p$$

we would have a solution! Trying to solve these equations simultaneously is possible, but it is easier to try and solve

$$z_1^3 + z_2^3 = -q, \quad \text{and} \quad z_1^3 z_2^2 = \frac{-p^3}{27}$$

for z_1^3 and z_2^3. Indeed, doing so gives that z_1^3, z_2^3 are the solutions to the quadratic

$$t^2 + qt - \frac{p^3}{27} = 0.$$

Solving this for z_1^3, and considering the three complex cube roots, we can determine three possible pairs (z_1, z_2), as

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

Hence, we get three values for $z_1 + z_2$, corresponding exactly to the three roots of our original equation.

Remark 1.2. *While this does give solutions in terms of cube and square roots, it is usually awful. Even the real root of a cubic equation will usually be expressing in terms of a sum of cube roots of complex numbers.*

Quartic equations

To solve the quartic, we can try a similar game: introduce three new quantities that we can write our roots in terms of, and try to find a cubic equation that they are roots of. By letting $y = x + \frac{a}{4}$, we can always reduce solving

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

to solving an equation of the form

$$y^4 + py^2 + qy + r = 0$$

for some p, q, r. Suppose this equation has solutions y_1, y_2, y_3, y_4. Then, factorising our polynomial, we must have

$$(y - y_1)(y - y_2)(y - y_3)(y - y_4) = y^4 + py^2 + qy + r$$

and hence, by comparing coefficients

$$0 = y_1 + y_2 + y_3 + y_4, \tag{1}$$

$$p = y_1y_2 + y_1y_3 + y_1y_4 + y_2y_3 + y_2y_4 + y_3y_4, \tag{2}$$

$$-q = y_1y_2y_3 + y_1y_2y_4 + y_1y_3y_4 + y_2y_3y_4, \tag{3}$$

$$r = y_1y_2y_3y_4. \tag{4}$$

We introduce 3 new quantities

$$u := y_1 + y_2 = -y_3 - y_4, \tag{5}$$
$$v := y_1 + y_3 = -y_2 - y_4, \tag{6}$$
$$w := y_1 + y_4 = -y_2 - y_3. \tag{7}$$

Using the first equality from Equations 1, we can recover the roots from u, v, w:

$$y_1 = \frac{u + v + w}{2}, \tag{8}$$
$$y_2 = \frac{u - v - w}{2}, \tag{9}$$
$$y_3 = \frac{-u + v - w}{2}, \tag{10}$$
$$y_4 = \frac{-u - v + w}{2}. \tag{11}$$

Using Equations 5 and 1, we find that

$$\begin{aligned} u^2 + v^2 + w^2 &= -2p, \\ u^2v^2 + u^2w^2 + v^2w^2 &= p^2 - 4r, \\ uvw &= -q \end{aligned}$$

and hence u^2, v^2, w^2 are the roots of the polynomial

$$(t - u^2)(t - v^2)(t - w^2) = t^3 + 2pt^2 + (p^2 - 4r)t - q^2$$

which we know how to solve! Thus, by solving this for u^2, v^2, w^2, and picking square roots such that $uvw = -q$, we can find the solutions y_1, y_2, y_3, y_4 to our original quartic

Remark 1.3. *You might wonder if there are analogues of Equations 5 and 8 in the cubic case, and there are! If y_1, y_2, y_3 are the roots of*

$$y^3 + py + q = 0$$

then they are related to z_1, z_2 by

$$\begin{cases} y_1 = z_1 + z_2, & z_1 = \frac{y_1 + \omega y_2 + \omega^2 y_3}{2}, \\ y_2 = \omega^2 z_1 + \omega z_2, & \text{and} \\ y_3 = \omega z_1 + \omega^2 z_2, & z_2 = \frac{y_1 + \omega^2 y_2 + \omega y_3}{2} \end{cases}$$

where $\omega = e^{\frac{2\pi i}{3}}$ is a complex root of $x^3 - 1$.

So what happens with the quintic? Why can't we find clever combinations of the roots that let us reduce to solving a quartic? Well, that is why we will try to figure out.

2 Preliminaries

2.1 First reminders

The following is a crash course in fields and rings, that should mostly in theory be familiar to you. Any additional results that we need from the through of field rings and modules will be added to Appendix A as we use them. If it turns out this review is comprehensive, Appendix A will be removed.

Definition 2.1. *A (commutative) ring R is a set R equipped with two binary operations $+$ and $\cdot$ (addition and multiplication), and two distinguished elements 0_R and 1_R such that:*

- *$(R, +)$ forms an abelian group with identity element 0_R,*
- *$(R, \cdot)$ form a (commutative) monoid with identity element 1_R,*
- *Addition distributes over multiplication:*

$$(a + b) \cdot c = a \cdot c + b \cdot c$$
$$a \cdot (b + c) = a \cdot b + a \cdot c$$

We denote by $R^\times$ the set of elements with multiplicative inverses

$$R^\times = \{r \in R \mid \text{there exists } s \in R \text{ such that } rs = 1_R\}$$

This forms a group under multiplication.

In this course, we will exclusively deal with commutative rings, i.e. rings for which $rs = sr$, and so will be lazy and just use the term "*ring*" to mean "*commutative ring*". Furthermore, we will just write 0 and 1 for 0_R and 1_R if there is no risk of confusion.

Definition 2.2. *A (commutative) ring is called and integral domain if $ab = 0$ implies that $a = 0$ or $b = 0$.*

Of particular relevance for us are rings in which every non-zero element is invertible. Every such ring is an example of an integral domain.

Definition 2.3. *A field is a commutative ring K in which $0 \neq 1$ and $K^\times = K \setminus \{0\}$.*

Definition 2.4. *An ideal of a (commutative) ring R is a subset $I \subset R$ such that*

- *If $a, b \in I$, then $a + b \in I$,*
- *If $a \in R$ and $b \in I$, then $ab \in I$.*

An ideal is called a prime ideal if $ab \in I$ implies $a \in I$ or $b \in I$. An ideal is called maximal if it is not contained in any larger proper ideal

$$I \subsetneq J \subsetneq R$$

Remark 2.5. *Recall that given an ideal I of a ring R, we can define the quotient ring R/I in terms of the cosets of I. An ideal I is prime if and only if R/I is an integral domain, and an ideal I is maximal if and only if R/I is a field.*

A number of important results about rings of polynomials rely on information about the structure of their ideals, specifically that they are generated by a single element.

Definition 2.6. *An ideal I is called principal if it is of the form*

$$I = (r) = rR = \{rs \mid s \in R\}$$

for some $r \in R$. An integral domain R is called a PID (principal ideal domain) if every ideal is principal.

Theorem 2.7. *Every PID is a UFD (unique factorisation domain). This means that their elements can be uniquely factored into irreducibles, up to reordering. In particular, the greatest common divisor (gcd) and least common multiplie (lcm) are defined in a PID.*

Theorem 2.8 (Bezout's identity)**.** *In a PID R, given $r, s \in R$, there exist $u, v \in R$ such that*

$$ur + vs = \gcd(r, s).$$

Theorem 2.9. *Let K be a field. Then the polynomial ring $K[x]$ is a Euclidean domain: given $f(x)$, $g(x) \in K[x]$, with $g(x) \neq 0$, there exists a unique $q(x)$, $r(x) \in K[x]$ with $\deg(r) < \deg(g)$ such that*

$$f(x) = g(x)q(x) + r(x).$$

Corollary 2.10. *$K[x]$ is a PID and hence a UFD.*

Corollary 2.11. *Non-zero prime ideal of $K[x]$ are maximal and of the form $(f(x))$ for an irreducible polynomial $f(x) \in K[x]$.*

Finally, we recall the notion of ring and field homomorphisms.

Definition 2.12. *A ring homomorphism $f : R \to S$ is a map such that*

$$f(x + y) = f(x) + f(y), \quad \text{and} \quad f(xy) = f(x)f(y)$$

for all x, $y \in R$ and such that

$$f(1_R) = 1_S, \quad f(0_R) = 0_S.$$

A field homomorphism is a ring homomorphism between two fields.

Field homomorphisms are very structured, and are therefore quite limited. For many pairs of "nice" fields, there are only finitely many field homomorphism between them!

Proposition 2.13. *Let $f : K \to L$ be a field homomorphism. Then*

1. *For all $x, y \in K$ with $y \neq 0$, $f\left(\frac{x}{y}\right) = \frac{f(x)}{f(y)}$,*
2. *The map f is injective,*
3. *The image of f is a subfield of L.*

Proof. To prove the first point, note that

$$f\left(\frac{x}{y}\right) f(y) = f(\frac{x}{y} \cdot y) = f(x)$$

and hence

$$\left(\frac{x}{y}\right) = \frac{f(x)}{f(y)}.$$

The easiest argument to prove the second is to note that $\ker f$ is an ideal of K, and that the only ideals of a field are $\{0\}$ and K. Since $f(1) = 1$, the kernel cannot be K and must therefore be the zero ideal. Hence f is injective.

We can also prove this more directly, as if $x \neq y$, then $x - y \neq 0$, and so it is invertible. Thus

$$f(x-y)f(\frac{1}{x-y}) = f(1) = 1$$

and so $f(x-y)$ is invertible and therefore non-zero. Thus $f(x) - f(y) = f(x - y) \neq 0$ and so $f(x) \neq f(y)$.

To see the final point, we either check the axioms of a field directly, or use the first isomorphism theorem which says that given a ring homomorphism

$$\phi : R \to S$$

we have that $\operatorname{im}\phi \cong R/\ker\phi$. In the case of $f : K \to L$, the kernel is $\{0\}$ and so we get that $\operatorname{im} f \cong K$ must be a field. □

2.2 Polynomials and Symmetric Polynomials

Throughout this section, we fix a field K. We start by recalling a basic fact about polynomials.

Proposition 2.14. *Given a polynomial $f(x) \in K[x]$, the remainder on division by $(x-a)$ is $f(a)$. In particular, a is a root of $f(x)$, if and only if $(x-a)$ divides $f(x)$*

Proof. As $K[x]$ is a Euclidean domain, there exist $q(x)$, $r(x) \in K[x]$ such that

$$f(x) = (x-a)q(x) + r(x).$$

Furthermore, as $\deg r < \deg x - a = 1$, we must have that $r(x) = c$ is a constant. Evaluating both sides of the equality at $x = a$, we find

$$f(a) = (a-a)q(a) + c = c$$

as claimed. □

Corollary 2.15. *If $\alpha_1, \ldots, \alpha_k$ are distinct roots of a polynomial $f(x) \in K[x]$, then*

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)g(x)$$

for some polynomial $g(x) \in K[x]$. In particular, a polynomial of degree n has at most n roots.

Recall that not every polynomial in $K[x]$ has a root in K: x^2+1 does not have a root in $\mathbb{R}$. However, the fundamental theorem of algebra tells us that every polynomial with real coefficients has a root in the larger field $\mathbb{C}$. Throughout the following, we will often assume that, given a polynomial $f(x) \in K[x]$, we can find a larger field $L \supset K$ such that $f(x)$ has a root in L.

We will eventually prove that such an L exists, but for now we will treat it as a given.

With this in mind, Corollary 2.15 has an immediate application for us in the Viète formulas.

Theorem 2.16 (Viète)**.** *If a polynomial $f(x) \in K[x]$*

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$$

has exactly n (possibly repeating) roots $\alpha_1, \ldots, \alpha_n$ (possibly in some larger field containing K), then

$$\begin{aligned}
a_1 &= -\sum_{1 \le i_1 \le n} \alpha_{i_1} \\
a_2 &= \sum_{1 \le i_1 < i_2 \le n} \alpha_{i_1}\alpha_{i_2} \\
&\vdots \\
a_k &= (-1)^k \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k} \\
&\vdots \\
a_n &= (-1)^n \alpha_1\alpha_2\ldots\alpha_n
\end{aligned}$$

Proof. We must have that

$$f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n).$$

Expanding this out and comparing coefficients gives the desired result. □

These expressions are of particular importance and are called the elementary symmetric polynomials in $\alpha_1, \ldots, \alpha_n$.

Definition 2.17. *A polynomial $P(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ is called symmetric if it is invariant under any permutation of its variables:*

$$P(x_1, \ldots, x_n) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

for all $\sigma \in S_n$.

The elementary symmetric polynomials in $x_1, \ldots, x_n$ are

$$\begin{aligned}
e_1 &= \sum_{1 \le i_1 \le n} x_{i_1} \\
e_2 &= \sum_{1 \le i_1 < i_2 \le n} x_{i_1} x_{i_2} \\
&\vdots \\
e_k &= \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} x_{i_2} \ldots x_{i_k} \\
&\vdots \\
e_n &= x_1 x_2 \ldots x_n
\end{aligned}$$

Example 2.18. *The elementary symmetric polynomials in x_1, x_2, x_3 are*

$$\begin{aligned}
e_1 &= x_1 + x_2 + x_3, \\
e_2 &= x_1 x_2 + x_1 x_3 + x_2 x_3, \\
e_3 &= x_1 x_2 x_3
\end{aligned}$$

Theorem 2.19. *Every symmetric polynomial $P(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ can be written as a K-linear combination of products of elementary symmetric polynomials.*

Proof. We will try to prove this by a Gram-Schmidt like argument. We will introduce an order on monomials, show that we can always find a product of elementary symmetric polynomials with a given smallest monomial, and then subtract off the product corresponding to the smallest monomial in a given symmetric polynomial, and repeat this process until we get the desired combination.

First we note that in any symmetric polynomial $P(x_1, \ldots, x_n)$, the monomial $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ must appear with the same coefficient as

$$x_{\sigma(1)}^{a_1} x_{\sigma(2)}^{a_2} \ldots x_{\sigma(n)}^{a_n} = x_1^{a_{\sigma^{-1}(1)}} x_2^{a_{\sigma^{-1}(2)}} \ldots x_n^{a_{\sigma^{-1}(n)}}.$$

Next we define an order on monomials by setting

$$x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} \prec x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$$

if $a_k < b_k$ for the largest k for which they are not equal. More explicitly, if $a_n < b_n$, or $a_n = b_n$ and $a_{n-1} < b_{n-1}$, or $a_n = b_n$ and $a_{n-1} = b_{n-1}$ and $a_{n-2} < b_{n-2}$, ...

For example, in $K[x_1, x_2, x_3]$, we have that

$$1 \prec x_1 \prec x_1^2 \prec x_1^3 \prec x_2 \prec x_1 x_2 \prec x_1^2 x_2 \prec x_2^2 \prec x_1 x_2^2 \prec x_1 x_2 x_3 \prec x_3^3 \prec \cdots$$

Given any polynomial $P(x_1, \ldots, x_n)$, we call the smallest monomial with respect to this order the *lowest term*. If $P(x_1, \ldots, x_n)$ is a symmetric polynomial, the lowest term $x_1^{a_1} \ldots x_n^{a_n}$ must have that

$$a_1 \geq a_2 \geq \cdots \geq a_n$$

For elementary symmetric polynomials $e_k(x_1, \ldots, x_n)$, the lowest term is $x_1 x_2 \ldots x_k$.

Furthermore, this order is multiplicative: if

$$x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} \prec x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n} \text{ and } x_1^{c_1} x_2^{c_2} \ldots x_n^{c_n} \prec x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}$$

then

$$x_1^{a_1+c_1} x_2^{a_2+c_2} \ldots x_n^{a_n+c_n} \prec x_1^{b_1+d_1} x_2^{b_2+d_2} \ldots x_n^{b_n+d_n}.$$

In particular, this implies that the lowest term of a product is the product of the lowest terms and hence the lowest term of

$$e_1^{r_1} e_2^{r_2} \ldots e_n^{r_n}$$

is

$$x_1^{r_1+r_2+\cdots+r_n} x_2^{r_2+r_3+\cdots+r_n} \ldots x_n^{r_n}$$

Thus, if $P(x_1, \ldots, x_n)$ is a symmetric polynomial of total degree N, with lowest term $x_1^{a_1} \ldots x_n^{a_n}$, then the product

$$e_1^{a_1-a_2} e_2^{a_2-a_3} \ldots e_n^{a_n}$$

has the same lowest term. Hence, for some $c \in K$, the symmetric polynomial

$$P(x_1, \ldots, x_n) - c e_1^{a_1-a_2} e_2^{a_2-a_3} \ldots e_n^{a_n}$$

has degree at most N with a larger lowest term. As there are only finitely many monomials of degree at most N, we can repeat this process until there are no monomial left, giving $P(x_1, \ldots, x_n)$ in terms of elementary symmetric polynomials. □

Example 2.20. *The polynomial $x_1^2 + x_2^2 + x_3^2$ is symmetric, with lowest term $x_1^2 x_2^0 x_3^0$. The corresponding product of elementary symmetric polynomials is*

$$e_1^{2-0} e_2^{0-0} e_3^{0-0} = e_1^2 = (x_1 + x_2 + x_3)^2.$$

Subtracting this off, we have that

$$x_1^2 + x_2^2 + x_3^2 - e_1^2 = -2(x_1 x_2 + x_1 x_3 + x_2 x_3) = -2e_2$$

Hence

$$x_1^2 + x_2^2 + x_3^2 = e_1^2 - 2e_2.$$

Example 2.21. *The polynomial*

$$f(x_1, x_2, x_3) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2$$

is symmetric with lowest term $x_1^2x_2x_3^0$. This corresponds to

$$e_1^{2-1}e_2^{1-0}e_3^0 = e_1e_2$$

We find that

$$\begin{aligned} f(x_1, x_2, x_3) - e_1e_2 =& x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2 \\ & - (x_1 + x_2 + x_3)(x_1x_2 + x_2x_3 + x_1x_3) \\ =& -3x_1x_2x_3 = -3e_3 \end{aligned}$$

and so $f(x_1, x_2, x_3) = e_1e_2 - 3e_3$.

Example 2.22. *The polynomial*

$$f(y_1, y_2, y_3, y_4) = (y_1 + y_2)(y_3 + y_4) + (y_1 + y_3)(y_2 + y_4) + (y_1 + y_4)(y_2 + y_4)$$

corresponding to $u^2 + v^2 + w^2$ in our solution of the quartic is symmetric, we have that

$$f(y_1, y_2, y_3, y_4) = 2e_2$$

Corollary 2.23. *Let $f(x) \in K[x]$ and let $\alpha_1, \ldots, \alpha_n$ be the roots of f (possibly repeating, possibly in a larger field containing K). Then any symmetric polynomial in $\alpha_1, \ldots, \alpha_n$ is an element of K, even if $\alpha_1, \ldots, \alpha_n$ are not.*

Proof. Any symmetric polynomial can be written in terms of elementary symmetric polynomials, and by the Viète formulas, elementary symmetric polynomials evaluated at $\alpha_1, \ldots, \alpha_n$ are equal (up to a sign) to the coefficients of $f(x)$, which are elements of K. Hence, any symmetric polynomial in $\alpha_1, \ldots, \alpha_n$ can be written in terms of the coefficients of f and in particular is an element of K. □

Example 2.24. *If $\alpha_1, \ldots, \alpha_4$ are the roots of*

$$y^4 + py^2 + qy + r$$

then $u^2 + v^2 + w^2 = 2e_2(y_1, \ldots, y_4) = 2p$.

If $\alpha_1, \ldots, \alpha_4$ are the roots of

$$x^4 + 2x^3 - x^2 + 5x + 3$$

then we have that

$$\begin{aligned} \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 &= e_1^2 - 2e_2 \\ &= (-2)^2 - 2(-1) = 6 \in \mathbb{Q} \end{aligned}$$

2.3 Resultants and Discriminants

Suppose we have polynomials $A(x)$, $B(x) \in K[x]$, and let $\alpha_1, \ldots, \alpha_m$ be the roots of $A(x)$ (possibly with repetition and in some large field containing K). Then the product $\prod_{j=1}^{m} B(\alpha_j)$ is symmetric in $\alpha_1, \ldots, \alpha_m$, and hence can be expressed in terms of the coefficients of $A(x)$. In particular, it is an element of K. Via objects called resultants, we can give an explicit formula for it.

Definition 2.25. *Let*

$$A(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_m,$$
$$B(x) = b_0 x^n + b_1 x^{n-1} + \cdots + b_n$$

be two polynomials in $K[x]$. We define the resultant of A and B to be the $(m+n) \times (m+n)$ determinant

$$\mathrm{Res}(A,B) = \det \begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 & b_0 & 0 & 0 & \cdots & 0 \\ a_1 & a_0 & 0 & \cdots & 0 & b_1 & b_0 & 0 & \cdots & 0 \\ \vdots & a_1 & a_0 & \ddots & \vdots & \vdots & b_1 & b_0 & \ddots & \vdots \\ a_m & \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & a_m & \ddots & \ddots & a_0 & b_n & \ddots & \ddots & \ddots & b_0 \\ 0 & 0 & a_m & \ddots & a_1 & 0 & b_n & \ddots & \ddots & b_1 \\ \vdots & 0 & \ddots & \ddots & \vdots & 0 & 0 & b_n & \ddots & b_2 \\ \vdots & & \ddots & & \vdots & \vdots & & \ddots & & \vdots \\ 0 & & \cdots & & a_m & 0 & & \cdots & & b_n \end{pmatrix}$$

where there are n columns with coefficients from A and m columns with coefficients from B

Example 2.26. *Let $A(x) = x^2 + 2x + 2$, $B(x) = x^3 + 3x^2 + 4x + 8$. Then the resultant of A and B is*

$$\mathrm{Res}(A,B) = \det \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 & 1 \\ 2 & 2 & 1 & 4 & 3 \\ 0 & 2 & 2 & 8 & 4 \\ 0 & 0 & 2 & 0 & 8 \end{pmatrix} = 36$$

The properties of the resultant are neatly summarised here. We will not prove this result, though a proof will be given in Appendix B

Proposition 2.27. *Let $A(x)$, $B(x) \in K[x]$. Then:*

1. $\operatorname{Res}(A, B) \in K$. *If A, B have coefficients in some subring $R \subset K$, then* $\operatorname{Res}(A, B) \in R$, *e.g. integer coefficients gives an integer resultant.*

2. *If, in some sufficiently larger field,*

$$A(x) = a\prod_{j=1}^{m}(x-\alpha_j) \quad \textit{and} \quad B(x) = b\prod_{k=1}^{n}(x-\beta_k)$$

then

$$\begin{aligned}\operatorname{Res}(A,B) &= a^n b^m \prod_{j=1}^{m}\prod_{k=1}^{n}(\alpha_j-\beta_k) = a^n\prod_{j=1}^{m}B(\alpha_j)\\ &= (-1)^{mn}b^m\prod_{k=1}^{n}A(\beta_k) = (-1)^{mn}\operatorname{Res}(B,A)\end{aligned}$$

3. $\operatorname{Res}(A, B) = 0$ *if and only if A and B have a common root in some large enough field.*

Example 2.28. *If $K = \mathbb{Q}$, $A(x) = x^2 + 2$ and $B(x) = x^2 - 3$, then we can compute the resultant (which must be an integer) as the determinant*

$$\operatorname{Res}(A,B) = \det\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 2 & 0 & -3 & 0\\ 0 & 2 & 0 & -3\end{pmatrix}$$

but in this case it is actually easier to use our knowledge of the roots to compute the determinant. Since $B(x)$ has roots $\pm\sqrt{3}$, we must have that

$$\operatorname{Res}(A,B) = (-1)^4 A(\sqrt{3})A(-\sqrt{3}) = 5^2 = 25.$$

Definition 2.29. *Let $A(x) \in K[x]$ have degree $n > 0$, and leading coefficient $a_¿$ Then we define the discriminant of A to be*

$$\Delta(A) = \operatorname{disc}(A) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a}\operatorname{Res}(A,A')$$

Theorem 2.30. *Let $A(x) \in K[x]$ has roots $\alpha_1, \ldots, \alpha_n$ (possibly in some larger field). Then*

$$\begin{aligned}\operatorname{disc}(A) &= (-1)^{\frac{n(n-1)}{2}}a^{n-2}\prod_{j=1}^{n}A'(\alpha_j)\\ &= a^{2n-2}\prod_{1\le j<k\le n}(\alpha_j-\alpha_k)^2\end{aligned}$$

Proof. The first equality follows immediately from Proposition 2.27. In order to see the second equality, note that is

$$A(x) = a\prod_{k=1}^{n}(x-\alpha_k)$$

then

$$A'(x) = a\sum_{j=1}^{n}\prod_{\substack{1\le k\le n\\ k\neq j}}(x-\alpha_k)$$

and so

$$A'(\alpha_j) = a\prod_{k\neq j}(\alpha_j-\alpha_k).$$

Thus

$$\begin{aligned}\prod_{j=1}^{n}A'(\alpha_j) &= a^n\prod_{\substack{1\le j,k\le n\\ k\neq j}}(\alpha_j-\alpha_k)\\ &= a^n\prod_{1\le j<k\le n}(\alpha_j-\alpha_k)\prod_{1\le k<j\le n}(\alpha_j-\alpha_k)\\ &= (-1)^{\frac{n(n-1)}{2}}a^n\prod_{1\le j<k\le n}(\alpha_j-\alpha_k)\prod_{1\le k<j\le n}(\alpha_k-\alpha_j).\end{aligned}$$

Relabelling $j\leftrightarrow k$ in the last product, we get

$$\prod_{j=1}^{n}A'(\alpha_j) = (-1)^{\frac{n(n-1)}{2}}a^n\prod_{1\le j<k\le n}(\alpha_j-\alpha_k)^2$$

from which the claim follows. □

Corollary 2.31. *A polynomial $A(x)\in K[x]$ has repeated roots if and only if* $\operatorname{disc}(A)=0$.

Example 2.32. *Let $A(x)=ax^2+bx+c$. Then*

$$\begin{aligned}\operatorname{disc}(A) &= \frac{-1}{a}\operatorname{Res}(ax^2+bx+c, 2ax+b)\\ &= \frac{-1}{a}\det\begin{pmatrix}a & 2a & 0\\ b & b & 2a\\ c & 0 & b\end{pmatrix}\\ &= \frac{-1}{a}(ab^2+4a^2c-2ab^2) = b^2-4ac\end{aligned}$$

which should look very familiar. Indeed, we know that the number of roots of a quadratic equation, and the field in which they lie, is completely determined by this expression.

3 Field Extensions and splitting fields

3.1 Field extensions and algebraic numbers

Definition 3.1. *Let K and L be fields such that $K \subset L$. Then K is a subfield of L and L is an extension of K. We usually write L/K for L an extension of K.*

Given a (necessarily injective) field homomorphism $\iota : K \to L$, we sometimes identify K with its image and call K a subfield of L, but this is generally bad practice.

Definition 3.2. *Given a field extension L/K and elements $\alpha_1, \ldots, \alpha_n \in L$, we write $K(\alpha_1, \ldots, \alpha_n)$ for the smallest subfield of L containing K and $\alpha_1, \ldots, \alpha_n$.*

Similarly, given a subring $R \subset L$ and $\alpha_1, \ldots, \alpha_n \in L$, we write

$$R[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) \mid f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]\}$$

for the smallest subring of L containing R and $\alpha_1, \ldots, \alpha_n$.

Example 3.3. *Viewing $\mathbb{C}$ as an extension of $\mathbb{R}$, we have that $\mathbb{C} = \mathbb{R}(i)$.*

The field $\mathbb{Q}(\pi)$ can be identified with the field of rational functions in π:

$$\mathbb{Q}(\pi) = \{\frac{f(\pi)}{g(\pi)} \mid f(x),\, g(x) \in \mathbb{Q}[x],\, g(\pi) \neq 0\}$$

The ring $\mathbb{Z}[\sqrt{2}]$ is equal to the set

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a,\, b \in \mathbb{Z}\}$$

Definition 3.4. *Given a field extension L/K and an element $\alpha \in L$, we say that α is algebraic over K if there exists non-zero $f(x) \in K[x]$ such that $f(\alpha) = 0$ in L. Otherwise we say α is transcendental over K. If $K = \mathbb{Q}$, we usually just refer to numbers as being algebraic or transcendental.*

For algebraic α, the set

$$V_\alpha = \{f(x) \in K[x] \mid f(\alpha) = 0\}$$

forms a non-zero ideal in $K[x]$. Since $K[x]$ is a PID, there exists a non-zero (monic) polynomial $m_\alpha(x) \in K[x]$ such that

$$V_\alpha = (m_\alpha(x))$$

We call this the minimal polynomial of α. It is the unique monic polynomial of minimal degree of which α is a root. If it is of degree n, we call α algebraic of degree n over K.

Remark 3.5. *Recall that minimal polynomials are irreducible!*

Definition 3.6. *If L/K is a field extension such that every $\alpha \in L$ is algebraic over K, we call L an algebraic extension of K.*

Theorem 3.7. *Let L/K be a field extension and suppose $\alpha \in L$ is algebraic of degree n over K. Then*

$$K[\alpha] = K(\alpha)$$

and $K[\alpha]$ is a vector space of dimension n over K.

Proof. We first show that $K[\alpha]$ is an n-dimensional K-vector space. It is clearly a vector space over K. We claim that

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

forms a basis of $K[\alpha]$.

To see that they are linearly independent, suppose there exist constants $c_{n-1}, \ldots, c_0 \in K$, not all 0, such that

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = 0.$$

Then α is a root of the polynomial

$$f(x) = c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \in K[x]$$

which has degree at most $n-1$. But this is a contradiction, as α is algebraic of degree n, and so the minimal polynomial of α has degree $n > \deg f$. Hence, we must have $f(x) = 0$, and so $c_0 = c_1 = \cdots = c_{n-1} = 0$.

To see that they span $K[\alpha]$, we note that we can write every element of $K[\alpha]$ in the form $g(\alpha)$ for some $g(x) \in K[x]$. We can divide $g(x)$ by the minimal polynomial $m_\alpha(x)$ of α to get

$$g(x) = m_\alpha(x)q(x) + r(x)$$

for some $r(x) \in K[x]$ with $\deg(r) < \deg(m_\alpha) = n$. Letting $x = \alpha$, we see that

$$g(\alpha) = m_\alpha(\alpha)q(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha)$$

and so there exist $r_0, r_1, \ldots, r_{n-1} \in K$ such that

$$g(\alpha) = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}.$$

Hence $K[\alpha]$ is a vector space of dimension n over K with basis $1, \alpha, \ldots, \alpha^{n-1}$. Finally to show that $K[\alpha] = K(\alpha)$, we note that it suffices to show that $K[\alpha]$ is a field. Clearly

$$K[\alpha] \subset K(\alpha)$$

and $K(\alpha)$ is the minimal such field, so if $K[\alpha]$ is a field, it must equal $K(\alpha)$. Thus, all we need to do is show that any non-zero element $\beta \in K[\alpha]$ is invertible in $K[\alpha]$.

Since $1, \alpha, \ldots, \alpha^{n-1}$ span $K[\alpha]$, there exists a polynomial $h(x) \in K[x]$ of degree at most $n-1$ such that $\beta = h(\alpha)$. Since $m_\alpha(x)$ is irreducible and $\deg h < \deg m_\alpha$, we must have that

$$\gcd(h, m_\alpha) = 1$$

and hence there exist $u(x)$, $v(x) \in K[x]$ such that

$$u(x)h(x) + v(x)m_\alpha(x) = 1.$$

Evaluating this at $x = \alpha$, we find

$$u(\alpha)h(\alpha) = 1$$

and so $h(\alpha)$ is invertible with inverse $u(\alpha) \in K[\alpha]$. Thus $K[\alpha]$ is a field and $K[\alpha] = K(\alpha)$. □

Example 3.8. *Over $K = \mathbb{Q}$, if $\alpha = \sqrt{5}$, then $m_\alpha(x) = x^2 - \sqrt{5}$, and*

$$\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$$

To determine the inverse of an element of this set, we multiply by a "conjugate" element:

$$\frac{1}{a + b\sqrt{5}} = \frac{1}{a + b\sqrt{5}} \frac{a - b\sqrt{5}}{a - b\sqrt{5}} = \frac{a}{a^2 - 5b^2} - \frac{b}{a^2 - 5b^2}\sqrt{5}$$

Over $K = \mathbb{R}$, the element $\alpha = i$ has minimal polynomial $m_\alpha(x) = x^2 + 1$, and

$$\mathbb{R}[i] = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$$

To determine the inverse of an element, we multiply above and below by the complex conjugate

$$\frac{1}{a + bi} = \frac{1}{a + bi} \frac{a - bi}{a - bi} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

In contrast, if $K = \mathbb{Q}$ and $\alpha = \pi$ (or $\alpha = e$ or another transcendental number) then we have that

$$\mathbb{Q}[\pi] \cong \mathbb{Q}[x] \ncong \mathbb{Q}(x) \cong \mathbb{Q}(\pi)$$

Example 3.9. *Is $\sqrt{2}$ algebraic over $\mathbb{Q}[\sqrt{5}]$? Yes, as it is a root of $x^2 - 2$, which is an element of $\mathbb{Q}[\sqrt{5}][x]$.*

What is its degree over $\mathbb{Q}[\sqrt{5}]$? Well, its minimal polynomial must divide $x^2 - 2$, so it is either degree 1 or 2, depending on whether $x^2 - 2$ is irreducible over $\mathbb{Q}[\sqrt{5}]$. If the minimal polynomial has degree 1, then we must have $\sqrt{2} \in \mathbb{Q}[\sqrt{5}]$, and so there exist $a, b \in \mathbb{Q}$ such that

$$\sqrt{2} = a + b\sqrt{5} \quad \Rightarrow 2 = a^2 + 5b^2 + 2ab\sqrt{5}.$$

If $a, b \neq 0$, this implies $\sqrt{5} \in \mathbb{Q}$, which is false. If $b = 0$, this would imply $\sqrt{2} \in \mathbb{Q}$, which is false. If $a = 0$, this implies $\sqrt{2/5} \in \mathbb{Q}$, which is false. Thus, no such a, b exist, and $\sqrt{2}$ has degree 2 over $\mathbb{Q}[\sqrt{5}]$.

This implies that $\mathbb{Q}[\sqrt{5}][\sqrt{2}] = \mathbb{Q}[\sqrt{5}, \sqrt{2}]$ is a vector space of dimension 2 over $\mathbb{Q}[\sqrt{2}]$ with basis $\{1, \sqrt{2}\}$. Hence, every element of $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$ is of the form

$$(a + b\sqrt{5}) + (c + d\sqrt{5})\sqrt{2} = a + b\sqrt{5} + c\sqrt{2} + d\sqrt{10}.$$

The set of algebraic numbers over a given ground field K can be shown to be a field, using a slight variation on resultants!

Theorem 3.10. *Let L/K be a field extension. Given $\alpha, \beta \in L$, algebraic over K, we have that*

$$\alpha + \beta, \quad \alpha - \beta, \quad \alpha\beta, \quad \frac{\alpha}{\beta}$$

are all algebraic over K (assuming $\beta \neq 0$ for division.)

Proof. First we note that it suffices to show that

$$\alpha + \beta, \quad \alpha\beta, \quad -\beta, \quad \frac{1}{\beta}$$

are all algebraic over K (where they are defined) These are all trivial (or undefined) if $\alpha = 0$ or $\beta = 0$, so we may assume they are both non-zero. Let $A(x)$ be the minimal polynomial of α and $B(x)$ be the minimal polynomial of β.

Then note that $-\beta$ is a root of $\tilde{B}(x) := B(-x) \in K[x]$, so $-\beta$ is algebraic over K. Similarly, if $\deg B = n$, then $\frac{1}{\beta}$ is a root of $\overline{B}(x) := x^n B(\frac{1}{x}) \in K[x]$. Hence $\frac{1}{\beta}$ is algebraic over K.

To show that $\alpha + \beta$ is algebraic, we consider the polynomials

$$A(y),\ B(x-y) \in K[x][y] \subset K(x)[y]$$

as polynomials in y with coefficients in $K[x] \subset K(x)$. Computing the resultant

$$C(x) := \mathrm{Res}_y(A(y), B(x-y))$$

of these (where the entries in our determinant will be polynomials in $K[x]$, we obtain a polynomial $C(x) \in K[x]$.

Let $\alpha = \alpha_1, \ldots, \alpha_m$ be the roots of $A(x)$ in some large enough field extension, and let $\beta = \beta_1, \beta_2, \ldots, \beta_n$ be the roots of $B(x)$ in some large enough field extension. From the properties of resultants, we have that

$$C(x) = \prod_{j=1}^{m} B(x - \alpha_j) = \prod_{j=1}^{m} \prod_{k=1}^{n} (x - \alpha_j - \beta_k).$$

The $j = k = 1$ factor is $(x - \alpha - \beta)$ and so $C(\alpha + \beta) = 0$. Hence $\alpha + \beta$ is algebraic.

To show that $\alpha\beta$ is algebraic, we can make a very similar argument. Define

$$D(x) = \mathrm{Res}_y(A(y), y^n B(\frac{x}{y}) \in K[x].$$

Expanding this out as a product of linear factors in the same way, we quickly find $D(\alpha\beta) = 0$ and so $\alpha\beta$ is algebraic over K. □

Example 3.11. *The sum $\sqrt{2}+\sqrt{5}$ is algebraic over $\mathbb{Q}$ and is a root of*

$$\mathrm{Res}(y^2-2, y^2-2xy+x^2-5) = \det\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -2x & 1 \\ -2 & 0 & x^2-5 & -2x \\ 0 & -2 & 0 & x^2-5 \end{pmatrix}$$

which we can compute to be x^4-14x^2+9.

Remark 3.12. *In general, the polynomial we get from a resultant computation will not be irreducible and is not the minimal polynomial. In this case, it happened to be irreducible, but this is unusual!*

3.2 Degree of extensions and tower law

Definition 3.13. *Let L/K be a field extension. WE call the dimension of L as a vector space over K the degree of L over K*

$$[L:K] := \dim_K L$$

If $[L:K] < \infty$, we call L a finite extension of K

Example 3.14.

$$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$$

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = \begin{cases} \deg\alpha \text{ if } \alpha \text{ is algebraic,} \\ \infty \text{ if } \alpha \text{ is transcendental.} \end{cases}$$

Theorem 3.15. *Every finite extension is algebraic*

Proof. Let L/K be finite of degree n and let $\alpha \in L$. Then $1, \alpha, \alpha^2, \ldots, \alpha^n$ are $n+1$ elements in an n-dimensional vector space, and so are linearly dependent: there exist $c_0, \ldots c_n \in K$, not all 0 such that

$$c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0.$$

Thus, α is a root of

$$f(x) = c_n x^n + \cdots + c_1 + c_0 \in K[x]$$

and is therefore algebraic over K. This holds for every element of L, so L is algebraic over K. □

Corollary 3.16. *If α is algebraic over K, so is every element of $K[\alpha]$.*

Remark 3.17. *The converse does not hold! Indeed, the field of complex numbers algebraic over $\mathbb{Q}$ is an infinite extension. Even more directly, the field extension*

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots)/\mathbb{Q}$$

is infinite.

Proposition 3.18 (Tower Law)**.** *If $K \subset L \subset M$ is a chain of finite extensions, then*

$$[M : K] = [M : L][L : K]$$

Proof. Let $[L : K] = r$ and $[M : L] = s$. Suppose that $\ell_1, \ldots, \ell_r$ is a basis of L over K, and $m_1, \ldots, m_s$ is a basis of M over L. We claim $\{\ell_j m_k\}_{\substack{1 \le j \le r \\ 1 \le k \le s}}$ is a basis of M over K, from which the claim follows.

First note that if $m \in M$, there exist $\lambda_1, \ldots, \lambda_s \in L$ such that

$$m = \sum_{k=1}^{s} \lambda_k m_k.$$

For each k, there exist $\mu_{1,k}, \ldots, \mu_{r,k} \in K$ such that

$$\lambda_k = \sum_{j=1}^{r} \mu_{j,k} \ell_j.$$

Hence

$$m = \sum_{j=1}^{r} \sum_{k=1}^{s} \mu_{j,k} \ell_j m_k.$$

Thus $\{\ell_j m_k\}$ is a spanning set of M over K. To see that they are linearly independent over K, suppose there existed $\mu_{j,k} \in K$, not all 0 such that

$$\sum_{j=1}^{r} \sum_{k=1}^{s} \mu_{j,k} \ell_j m_k = 0.$$

This implies that

$$\sum_{k=1}^{s} \left(\sum_{j=1}^{r} \mu_{j,k} \ell_j \right) m_k = 0.$$

Since $m_!, \ldots, m_s$ are linearly independent over L we must have

$$\sum_{j=1}^{r} \mu_{j,k} \ell_j = 0$$

for each $k = 1, \ldots, s$. Furthermore, since $\ell_1, \ldots, \ell_r$ are linearly independent over K, we must have $\mu_{j,k} = 0$ for all j, k. □

Remark 3.19. *This also holds for infinite extensions!*

Example 3.20. *We have seen that*

$$[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2, \quad \textit{and} \quad [\mathbb{Q}(\sqrt{5}, \sqrt{2}) : \mathbb{Q}(\sqrt{5}] = 2$$

and hence

$$[\mathbb{Q}(\sqrt{5}, \sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$$

which fits given that we have seen that every element of this set can be written as a $\mathbb{Q}$-linear combination of 1, $\sqrt{2}$, $\sqrt{5}$ and $\sqrt{10}$.

Definition 3.21. *Let L/K and M/K be two field extensions. A K-morphism $f : L \to M$ is a field homomorphism such that $f|_K = id$ i.e $f(a) = a$ for all $a \in K$. We denote by $\mathrm{Hom}_K(L, M)$ the set of K-morphisms $L \to M$, and by $\mathrm{Aut}_K(L)$ the set of K-automorphisms of L.*

3.3 Application to constructable numbers

Suppose we are given two points in the plane, which we will call 0 and 1. A point is called constructable if we can obtain it from 0 and 1 in finitely many ruler-and-compass constructions. Identifying the plane with the complex plane $\mathbb{C}$, we obtain a subset of $\mathbb{C}$, which we call the set of constructable numbers. With same careful geometry, we can show that this set is a subfield of $\mathbb{C}$ that is closed under square roots:

- Addition corresponds to construction of a parallelogram
- Negation corresponds to reflection through 0
- Multiplication and division of are performed by constructing similar triangles
- Square roots correspond to bisecting an angle and a neat trick with a semicircle of radius $x + 1$.

In fact, we can say something stronger: every step of a ruler-and-compass construction involves solving either a linear or quadratic equation. The intersection of two lines corresponds to a linear equation, while the intersection of circle with either a line or a circle corresponds to solving a quadratic equation. Suppose we are constructing $\alpha \in \mathbb{C}$, and denote by K_i the subfield of $\mathbb{C}$ we get at step i of the process. We must have that

$$[K_{i+1} : K_i] \in \{1, 2\}$$

depending on whether or not step $i + 1$ requires us to solve a "new" quadratic equation. This implies the following result.

Theorem 3.22. *A complex number α is constructable if and only if there exists a chain of extensions*

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq K_2 \subsetneq \cdots \subsetneq K_n$$

such that $[K_{i+1} : K_i] = 2$ for each i and $\alpha \in K_n$.

Corollary 3.23. *If α is constructable, then α is algebraic of degree 2^m for some m.*

Proof. We have that α is in a finite extension, and is therefore algebraic. Thus

$$\deg \alpha = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{[K_n : \mathbb{Q}]}{[K_n : \mathbb{Q}(\alpha)]} = \frac{2^n}{[K_n : \mathbb{Q}(\alpha)]} = 2^m$$

for some $m \leq n$. □

Example 3.24. *This implies that we cannot construct $\sqrt[3]{2}$ using a ruler and compass, as this has minimal polynomial $x^3 - 2$, and hence degree 3. Similarly, we cannot trisect a generic angle θ, as that corresponds to finding a root of $x^3 - e^{i\theta}$, which is usually irreducible.*

3.4 Abstract field extensions

Up until now, we have been assuming that our polynomials had root in some sufficiently large field extension, without ever worrying about the existence of such a field extension. We will now show that this was a perfectly acceptable assumption, by constructing the necessary fields.

First recall that if $f(x) \in K[x]$ is an irreducible polynomial, the ideal $(f) \in K[x]$ is a maximal ideal and so the quotient ring $K[x]/(f)$ is a field.

Proposition 3.25. *Let $f(x) \in K[x]$ be irreducible and let $L = K[x]/(f)$. Then L is a field extension of K of degree $[L : K] = \deg f$ containing a root of $f(x)$*

Proof. By the same arguments as in Theorem 3.7, L has a basis $\{1, x, x^2, \dots, x^{n-1}\}$ over K, where $n = \deg f$. The K-span of 1 is a copy of K contained in L, and so L is an extension of K of degree $[L : K] = n$. Finally note that the image of x under the natural projection

$$K[x] \to K[x]/(f)$$

is a root of f, as $f(x) = 0$ in the quotient. □

Not only does this give us *a* field extension in which $f(x)$ has a root, but it is essentially *the* (minimal) field extension in which $f(x)$ has a root

Theorem 3.26. *Suppose L/K and M/K are two extensions of K and suppose we have $\alpha \in L$ and $\beta \in M$ with the same minimal polynomial over K. Then there exists a unique K-morphism $\phi : K[\alpha] \to K[\beta]$ such that $\phi(\alpha) = \beta$. Furthermore, it is an isomorphism.*

The set of K-morphisms $K[\alpha] \to L$ are in bijection with the roots of the minimal polynomial m_α of α in L.

Proof. We first consider the morphism ϕ. If such a morphism exists, it is unique, as any morphism $K[\alpha] \to K[\beta]$ is uniquely determined by the image of α.

As $\phi(a\gamma) = a\phi(\gamma)$ for all $a \in K$ and $\gamma \in K[\alpha]$, ϕ is a K-linear map between two vector spaces. As ϕ is a field homomorphism, it is injective, and

$$\dim_K K[\alpha] = \deg m_\alpha = \deg m_\beta = \dim_K K[\beta]$$

so it is an injective linear map between two vector spaces of the same dimension. Hence ϕ must be an isomorphism.

As for the existence, the only possible obstruction to ϕ being well defined is the requirement that $m_\alpha(\alpha) = 0$, and so we must have that

$$m_\alpha(\beta) = m_\alpha(\phi(\alpha)) = \phi(m_\alpha(\alpha)) = 0.$$

This holds, as $m_\alpha = m_\beta$ is the common minimal polynomial of α and β.

For the second half of the statement, note again that a K-morphism $\psi : K[\alpha] \to L$ is completely determined by $\psi(\alpha)$. Since

$$0 = \psi(0) = \psi(m_\alpha(\alpha)) = m_\alpha(\psi(\alpha))$$

we must have that $\psi(\alpha)$ is a root of m_α in L, and we can easily check that every such root gives a well defined K-morphism. □

Corollary 3.27. *For every extension M/K containing a root α of an irreducible polynomial $f(x) \in K[x]$, there exists a unique K-morphism*

$$\begin{aligned} K[x]/(f) &\to M \\ x &\mapsto \alpha \end{aligned}$$

Example 3.28. *The field $\mathbb{R}[x]/(x^2+1)$ is spanned by 1 and x, where $x^2+1=0$. We have 2 $\mathbb{R}$-morphisms to $\mathbb{C}$:*

$$\begin{aligned} x &\mapsto i, \\ x &\mapsto -i. \end{aligned}$$

Similarly, we have that

$$\mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[\omega\sqrt[3]{2} \cong \mathbb{Q}[\omega^2\sqrt[3]{2}]$$

where ω is a complex root of $x^3-1=0$. The three "standard" fields correspond to the three $\mathbb{Q}$-morphisms

$$\mathbb{Q}[x]/(x^3-2) \to \mathbb{C}.$$

By iterating this process, we can always construct a field extension in which a polynomial $f(x)$ has all its roots. In such a field $f(x)$ splits as a product of linear factors.

Definition 3.29. *Let $f(x) \in K[x]$. A splitting field of $f(x)$ is a field extension M/K in which f splits as a product of linear factors, and is minimal with this property.*

Remark 3.30. *If $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$, then a splitting field is $K(\alpha_1, \ldots, \alpha_n)$, though this might not be the best representation of the splitting field.*

Example 3.31. *Consider $f(x) = x^3 - 2$ over $\mathbb{Q}$. Even though f has a root in $\mathbb{Q}(\sqrt[3]{2})$, this is not a splitting field as we can only factorise f as*

$$f(x) = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$$

into a product of a linear factor and an irreducible quadratic. We can factor f into linear factors in $\mathbb{C}$, but this is way too big. An example of a splitting field is

$$\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\omega, \sqrt[3]{2}).$$

Corollary 3.32. *For every $f(x) \in K[x]$, there exists a splitting field. Furthermore, any splitting field is of finite degree.*

Proof. We can assume that $f(x)$ has no linear factors in K. Suppose $f(x)$ has an irreducible factor $h(x)$. Then, in $K_1 = K[x]/(h)$, $f(x)$ has at least one root α, and so we can factor $f(x) = (x - \alpha)f_1(x)$ for some $f_1(x) \in K_1[x]$. Arguing by induction on the degree of $f(x)$, we can say that there exists a splitting field L of $f_1(x)$ over K_1. Then viewing L as an extension of $K \subset K_1$, we get a field extension in which $f(x)$ splits. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in L. Then $K(\alpha_1, \ldots, \alpha_n) \subset L$ is a splitting field of $f(x)$ over K.

To see that every splitting field is of finite degree, we must have that every splitting field is of the form $K(\alpha_1, \ldots, \alpha_n)$ for where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$ in some sufficiently large field. Then note that

$$\begin{aligned}&[K(\alpha_1, \ldots, \alpha_n) : K] \\ &\quad = [K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})][K(\alpha_1, \ldots, \alpha_{n-1}) : K].\end{aligned}$$

The first of these factors is finite as α_n is algebraic over $K(\alpha_1, \ldots, \alpha_{n-1})$, while we can argue that the second is finite by induction. Thus the product is finite. □

Example 3.33. *Lets construct a splitting field of $x^3 - 2$ over $\mathbb{Q}$ via abstract field extensions. We first enlarge $\mathbb{Q}$ to $L = \mathbb{Q}[x]/(x^3 - 2)$. We will denote by α the image of x. Then*

$$x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2)$$

in $\mathbb{Q}[\alpha][x] \subset L[x]$. If $x^2 + \alpha x + \alpha^2$ has a root in $\mathbb{Q}[\alpha]$, we are done. If it is irreducible (non-trivial), then we let $M = \mathbb{Q}[\alpha][x]/(x^2 + \alpha x + \alpha^2)$. Then $x^3 - 2$ splits in M and so M contains a splitting field of $x^3 - 2$ over $\mathbb{Q}$.

Finally, we show that, not only do splitting fields exist, but they are essentially unique.

Theorem 3.34. *Let K be a field and let $f(x) \in K[x]$. Suppose that L is a splitting field of $f(x)$ over K, and suppose we have a field extension M/K in which f splits as a product of linear factors. Then there is a K-morphism $\rho : L \to M$. In particular, if L_1, L_2 are splitting fields of $f(x)$ over K, then there is a K-isomorphism $L_1 \cong L_2$.*

Proof. We will prove this by induction on $[L : K]$. We can assume that $f(x)$ has no linear factors, and take $\alpha \in L$ a root of $f(x)$. Let $m_\alpha(x)$ be the minimal polynomial of α over K., so that

$$K(\alpha) \cong K[x]/(m_\alpha).$$

Since $f(x)$ splits in M, and $m_\alpha(x)$ divides $f(x)$, $m_\alpha(x)$ has roots in M. Let $\beta \in M$ be such a root. By Theorem 3.26, there exists a K-morphism

$$\begin{aligned}\iota : K(\alpha) &\to M \\ \alpha &\mapsto \beta.\end{aligned}$$

As such, we can view $K(\alpha)$ as a subfield of M. Then, consider the extensions

$$L/K(\alpha) \quad \text{and} \quad M/K(\alpha).$$

We have that

$$[L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]} < [L : K]$$

and so we can argue by induction that there is a $K(\alpha)$-morphism $L \to M$. Combining this with the K-morphism ι, we get a K-morphism $L \to M$.

Finally, to see that two splitting fields are isomorphic, note that the prior argument implies we have a (necessarily) injective K-morphism $L_1 \to L_2$ and a K-morphism $L_2 \to L_1$. By injectivity of both maps, we must have that

$$\dim_K L_1 = \dim_K L_2$$

and hence the injective K-morphism is a K-isomorphism. □

As such, we can essentially freely speak of *the* splitting field of $f(x)$ over K.

3.5 Classification of Finite Fields

A finite field is a field with only finitely many elements. The classical example would be a field with a prime number of elements $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, which should be familiar from earlier courses. Recall that we require a field to have distinct additive and multiplicative elements, so the smallest possible field is $\mathbb{F}_2$. The is no field with one element.

So what finite fields do exist? To describe this, we first need to introduce the characteristic

Definition 3.35. *Let R be a ring. The characteristic of R is the (unique) non-negative $c \in \mathbb{Z}$ defining the kernel of the unique ring map $\mathbb{Z} \to R$:*

$$c\mathbb{Z} = \ker(\lambda : \mathbb{Z} \to R)$$
$$1 \mapsto 1_R.$$

That is to say that is its the smallest positive integer such that $1+1+\cdots_{ntimes}+1 = 0$ in R, or 0 if no such integer exists. We denote this by $\operatorname{char} R$.

Example 3.36.

$$\operatorname{char} \mathbb{Z}/n\mathbb{Z} = n, \quad \operatorname{char} \mathbb{C}(x) = 0$$

In the case of fields, the characteristic has limited possible values.

Proposition 3.37. *If $R = K$ is a field, the* $\operatorname{char} K = 0$ *or* $\operatorname{char} K$ *is prime*

Proof. Suppose $\operatorname{char} K = c \neq 0$. If $c = ab$, then

$$\lambda(a)\lambda(b) = \lambda(ab) = \lambda(c) = 0$$

where $\lambda : \mathbb{Z} \to K$ takes 1 to 1_K. As K is a field, this implies one of $\lambda(a) = 0$ or $\lambda(b) = 0$. As c was the minimal such integer, this implies that either $a = c$ or $b = c$, i.e. c has no proper divisors. Thus, if $c \neq 0$, c is prime. □

Example 3.38. *We have already seen a field of every possible characteristic:*

$$\operatorname{char} \mathbb{Q} = 0, \quad \operatorname{char} \mathbb{F}_p = p$$

These examples are fundamental. Indeed, every field contains a copy of one of these fields, determined by the characteristic.

Proposition 3.39. *Let K be a field. If $\operatorname{char} K = 0$ then K contains a copy of $\mathbb{Q}$. If $\operatorname{char} K = p > 0$, then K contains a copy of $\mathbb{F}_p$.*

Proof. We consider the smallest subfield containing 0 and 1. If $\operatorname{char} K = p > 0$, then the additive subgroup generated by 1 is clearly a copy of $\mathbb{F}_p$. If $\operatorname{char} K = 0$, then the additive subgroup generated by 1 is a copy of $\mathbb{Z}$, and so the smallest field containing 0 and 1 must be $\mathbb{Q}$. □

In particular, a finite field K must have prime characteristic and contain a copy of $\mathbb{F}_p$. As it is finite, it must be a finite extension of $\mathbb{F}_p$. Thus, to classify all finite fields, it suffices to classify all finite extensions of $\mathbb{F}_p$ for each prime p.

Theorem 3.40. *Let K be a finite field of prime characteristic p. Then there exists $d \in \mathbb{N}$ such that $\#K = p^d$.*

Proof. We know that K must be a finite dimensional $\mathbb{F}_p$-vector space. Suppose it has dimension $d = [K : \mathbb{F}_p]$ and let $e_1, \ldots, e_d$ be a basis. Then every element $\xi \in K$ can be uniquely written as

$$\xi = a_1 e_1 + \cdots + a_d e_d$$

where $a_1, \ldots, a_d \in \mathbb{F}_p$. Furthermore, every such linear combination defines an element of K. As there are p choices for each a_i, we must therefore have p^d elements of K in total. □

Theorem 3.41. *For every prime p and positive integer $d \in \mathbb{N}$ there exists a finite field $\mathbb{F}_q$ with exactly $q = p^d$ elements, unique up to isomorphism.*

Proof. We start with optimism: suppose such a field F with q elements exists. Then $F^\times$ is a group of order $q - 1$ with respect to multiplication, and so by Lagrange's Theorem $a^{q-1} = 1$ for all $a \in F^\times$. Thus

$$a^q = a$$

for all $a \in F$. So if such a field exists, every element is a root of $x^q - x$. So lets consider the splitting field of this polynomial over $\mathbb{F}_p$.

Let $L/\mathbb{F}_p$ be a field in which $f_q(x) := x^q - x$ splits as a product of linear factors. We first show that $f_q(x)$ has q distinct roots in L. If $f_q(x)$ has a repeated root, then it is also a root of $f_q'(x)$: if

$$f(x) = (x - a)^2 g(x)$$

then

$$f'(x) = (x - a)(2g(x) + (x - a)g'(x)).$$

So if $f_q(x)$ has a repeated root a, a is a root of

$$f_q'(x) = qx^{q-1} - 1 = p^d x^{q-1} - 1 = -1$$

since $\operatorname{char} L = p$. This clearly has no roots, and so $f_q(x)$ has q distinct roots. From our previous remarks, this implies that any field of q elements is a splitting field of $f_q(x)$

Next we claim that the set of roots forms a field. If so, then the set of roots is the splitting field of $f_q(x)$. This will be a field of size q.

To see that the set of roots forms a field, note that, if a and b are roots of $f_q(x)$, then

$$(a+b)^p = a^p + b^p \quad \Rightarrow (a+b)^q = a^q + b^q = a + b$$

and

$$(ab)^q = a^q b^q = ab$$

so the sum and product of two roots is another root. Similarly, if $a \neq 0$ then

$$(a^{-1})^q = (a^q)^{-1} = a^{-1}$$

and

$$(-b)^q = (-1)^q b^q = -b$$

(as either q is odd or $1 = -1$ in characteristic 2).

Thus the set of roots is a field and hence the splitting field. It is of size q and all other fields of size q must be isomorphic to it, by Theorem 3.34, as all other fields of size q must also be splitting fields. □

3.5.1 Constructing $\mathbb{F}_q$

The easiest way to construct $\mathbb{F}_q$ for $q = p^d$ is to find an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree d. Such a polynomial must exists (pick some construction of $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ and take the minimal polynomial of α) and then $\mathbb{F}_p[x]/(f(x))$ is an extension of $\mathbb{F}_p$ of size $q = p^d$.

Example 3.42. *Let us construct $\mathbb{F}_4$, $\mathbb{F}_8$ and $\mathbb{F}_{16}$.*

For $\mathbb{F}_4$, we need an irreducible quadratic polynomial. A quadratic is irreducible if it has no roots, so we can easily manually check all for possible quadratics to find $x^2 + x + 1$ is the unique irreducible quadratic. Then

$$\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2 + x + 1)$$

Denoting by α the image of x in the quotient, $\mathbb{F}_4$ is a two dimensional $\mathbb{F}_2$ vector space, spanned by 1 and α, with multiplication determined by $\alpha^2 = -\alpha - 1$.

For $\mathbb{F}_8$ we need an irreducible cubic polynomial. A cubic is irreducible if it has no roots, so we can quickly check that we have two options

$$x^3 + x^2 + 1 \quad \textit{and} \quad x^3 + x + 1$$

both of which produce isomorphic $\mathbb{F}_8$. In the model

$$\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3 + x + 1)$$

the space is spanned by $1, \alpha, \alpha^2$, subject to $\alpha^3 = -\alpha - 1$.

For $\mathbb{F}_{16}$, we need to find an irreducible quartic. As a reducible quartic could be the product of two quadratics, it is no longer enough to check for a root. The most efficient option would be so consider all possible products of irreducibles of lower degree, as we have already determined these irreducibles. The only product of irreducible quadratics is

$$(x^2 + x + 1)^2 = x^4 + x^2 + 1$$

and the product of a linear factor with a cubic will have a root. Thus, we can quickly find that $f(x) = x^4 + x + 1$ is irreducible. Hence

$$\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(x^4 + x + 1).$$

4 Normal and separable extensions

From the perspective of discussing roots of polynomials, there are two field properties that make a field particularly "nice". These relate to both whether we can factorise polynomials "easily", and how accurately we can talk about symmetries among the roots of a polynomial, as we will later see.

The first property is normality. A field is normal if every irreducible polynomial with a root in the field has all its roots in the field. This is clearly desirable, and conveniently easily described.

The second is separability. A field is separable if irreducible polynomials have no repeated roots. This is often a hard property to conceptualise, as essentially every field we might care about is separable. In fact, coming up with an example of a inseparable field is suprisingly involved!

4.1 Normal extensions

Definition 4.1. *Let L/K be a field extension. We call L a normal extension of K if every irreducible $f(x) \in K[x]$ that has a root in L splits as a product of linear factors in $L[x]$.*

A normal closure of a field extension L/K is a field extension M/L such that M/K is a normal extension and M is minimal with this property.

Example 4.2. *The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal, as the minimal polynomial of any $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is*

$$x^2 - 2ax + (a^2 - 2b^2) = (x - a - b\sqrt{2})(x - a + b\sqrt{2})$$

which splits as a product of linear factors in $\mathbb{Q}(\sqrt{2})[x]$.

The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal, as $x^3 - 2$ has a root in $\mathbb{Q}(\sqrt[3]{2})$, but does not split as a product of linear factors, since the other two roots are complex non-real numbers.

It turns out the classification of normal extension is quite straightforward. A finite field extension is normal if and only if it is a splitting field. As such, given a polynomial $f(x) \in K[x]$, the minimal polynomial of any algebraic combination of its roots splits entirely in the splitting field of $f(x)$!

Theorem 4.3. *A finite extension L/K is normal iff L is the splitting field of some polynomial $f(x) \in K[x]$.*

Proof. Suppose L/K is a normal extension of finite degree. Then we can find $\alpha_1, \ldots, \alpha_n \in L$ such that

$$L = K(\alpha_1, \ldots, \alpha_n)$$

by, for example, choosing a K-basis $\{\alpha_1, \ldots, \alpha_n\}$ of L. Since every element in a finite extension is algebraic, each of these α_i is algebraic, with some minimal polynomial $m_i(x) \in K[x]$.

Since each $m_i(x)$ has a root $\alpha_i \in L$, and L/K is normal, $m_i(x)$ splits as a product of linear factors in $L[x]$. Letting

$$h(x) = m_1(x)m_2(x)\cdots m_n(x)$$

the field L must therefore contain the splitting field L' of $h(x)$ over K. But the splitting field must contain K and $\alpha_1, \ldots, \alpha_n$, and so

$$L = K(\alpha_1, \ldots, \alpha_n) \subset L'.$$

Therefore $L = L'$ is the splitting field of $h(x)$ over K.

Conversely, support that L is the splitting field of some $h(x) \in K[x]$. This implies $[L : K] < \infty$. Now suppose that $g(x) \in K[x]$ is irreducible, and has a root in L. Let M/L be some extension in which $g(x)$ splits as a product of linear factors, and let $\alpha, \beta \in M$ be two roots of $g(x)$.We know that we have a K-isomorphism

$$K(\alpha) \cong K(\beta) \cong K[x]/(g(x)).$$

Furthermore, as L is the splitting field of $h(x)$ over K, we must also have that $L(\alpha)$ is a splitting field of $h(x)$ over $K(\alpha)$. It clearly contains the a splitting field, and the splitting field must contain L and α, so they must be equal.

Similarly $L(\beta)$ is a splitting field of $h(x)$ over $K(\beta) \cong K(\alpha)$. As any two splitting fields of $h(x)$ over $K(\alpha)$ are isomorphic (Theorem 3.34), we can extend the K-isomorphism $K(\alpha) \cong K(\beta)$ to a K-isomorphism $L(\alpha) \cong L(\beta)$.

While we don't know that this is an L isomorphism, we can say that

$$\begin{aligned}[L(\alpha) : L][L : K] &= [L(\alpha) : K] \\ &= [L(\beta) : K] \\ &= [L(\beta) : L][L : K]\end{aligned}$$

and so

$$[L(\alpha) : L] = [L(\beta) : L].$$

In particular, if $\alpha \in L$, we have that

$$[L(\beta) : L] = [L(\alpha) : L] = 1$$

and so $\beta \in L$. As such, if L contains one root of $g(x)$, it contains all of them, i.e. L is a normal extension. □

Corollary 4.4. *Every finite extension L/K has a (unique up to isomorphism) normal closure*

Proof. Choose a K-basis $\{\alpha_1, \ldots, \alpha_n\}$ of L, and let $m_i(x) \in K[x]$ be the minimal polynomial of α_i. Let M be the splitting field of

$$h(x) = m_1(x)m_2(x) \cdots m_n(x).$$

This is a finite normal extension of K containing L. The normal closure of L/K is then the smallest subfield of M that is a normal extension of K containing L. □

Corollary 4.5. *Let L/K be a normal extension of finite degree. Then*

a) If we have a tower of extensions $K \subset F \subset L$, then any K-homomorphism $\tau : F \to L$ extends to a K-automorphism $\overline{\tau} : L \to L$.

b) Suppose $\alpha \in L$ has minimal polynomial $m(x) \in K[x]$. Then, for any root $\beta \in L$ of $m(x)$, there exists a K-automorphism $\varphi : L \to L$ such that $\varphi(\alpha) = \beta$. That is to say that $\mathrm{Aut}_K(L)$, the group of K-automorphisms of L, acts transitively on the roots of $m(x)$.

Proof. a) As L/K is a finite normal extension, it is the splitting field over K of some $f(x) \in K[x]$. Then L is also the splitting field of $f(x)$ over F and over the subfield $\tau(F)$. From the uniqueness of the splitting field (Theorem 3.34), there must exist an automorphism $\overline{\tau}$ of L extending the K-isomorphism

$$\tau : F \to \tau(F).$$

As τ fixes K, so too must $\overline{\tau}$.

b) Taking $F = K(\alpha)$, and $\tau : F \to L$ the unique K-homomorphism such that $\tau(\alpha) = \beta$, we get the desired K-automorphism $\varphi = \overline{\tau}$.

□

4.2 Separable extensions

Definition 4.6. *Let L/K be a field extension of finite degree.*

- *We call a (non-constant) irreducible polynomial $f(x) \in K[x]$ separable over K if all its roots are distinct in the splitting field.*
- *We call an element $\alpha \in L$ separable over K if its minimal polynomial is separable over K.*

- *The extension L/K is called a separable extension if every element of L is separable over K.*
- *We call K perfect if every algebraic extension is separable.*

Remark 4.7. *As every element in an algebraic extension of K is contained in a finite extension of K, it suffices to check that every finite extension of K is separable to show that K is perfect.*

Example 4.8. *Over $\mathbb{Q}$, x^2-2 is separable, and so $\sqrt{2}$ is separable, and $\mathbb{Q}(\sqrt{2})$ is separable.*

In order to construct and example of a field extension that is not separable, we will need a couple of tools for identifying inseparable polynomials.

Proposition 4.9. *For a polynomial $f(x) \in K[x]$, the following are equivalent:*

1. $\gcd(f(x), f'(x)) \neq 1$ *in* $K[x]$,
2. $f(x)$ *and* $f'(x)$ *have a common root in some extension of* K,
3. $\operatorname{disc}(f(x)) = 0$,
4. $f(x)$ *has a repeated root.*

Proof. To see that $(i) \Rightarrow (ii)$, note that $f(x)$ and $f'(x)$ will have a common root in the splitting field of $\gcd(f(x), f'(x))$ if it is non-constant. Conversely, if they have a common root, then its minimal polynomial must be a non-constant common factor.

The equivalence of (ii) and (iii) is the content of Corollary 2.31.

To see that $(iv) \Rightarrow (ii)$, note that if

$$f(x) = (x-\alpha)^2 g(x)$$

in the splitting field, then

$$f'(x) = (x-\alpha)\left(2g(x) + (x-\alpha)g'(x)\right)$$

so α is a common root.

Finally suppose that α is a common root of $f(x)$ and $f'(x)$ in some extension. Then

$$f(x) = (x-\alpha)g(x)$$

for some $g(x)$, and so

$$f'(x) = g(x) + (x-\alpha)g'(x).$$

As $f'(\alpha) = 0$, this implies $g(\alpha) = 0$, and so α is a repeated root of $f(x) = (x-\alpha)g(x)$. □

Example 4.10. *Let $K = \mathbb{F}_p(t)$ be the field of rational functions with coefficients in $\mathbb{F}_p$ for some prime p. We claim $x^p - t$ is irreducible in $K[x]$. Suppose otherwise, and that we can write*

$$f(x) = g(x)h(x)$$

for some $g(x), h(x) \in K[x]$ with $0 < \deg g < p$. Let L be the splitting field of $f(x)$ and let $\tau \in L$ be a root of $f(x)$. We then have

$$\begin{aligned}(x-\tau)^p &= x^p - \binom{p}{1}x^{p-1}\tau + \binom{p}{2}x^{p-2}\tau^2 + \cdots + \binom{p}{p-1}x\tau^{p-1} - \tau^p \\ &= x^p - \tau^p = x^p - t\end{aligned}$$

as $\tau^p = t$ and $\binom{p}{k}$ is always divisible by p. Hence, any monic proper factor $g(x)$ of $x^p - t$ must be of the form

$$g(x) = (x-\tau)^k$$

for some $0 < k < p$. If $g(x) \in K[x]$ this implies that

$$x^k - k\tau x^{k-1} + \cdots \in K[x]$$

and in particular that $-k\tau \in K$. But $\tau \notin K$, so we must have that this is equal to 0 in $\mathbb{F}_p$, and so $k = 0$ or $k = p$. But neither of these are possible if $g(x)$ is a proper factor. Hence $f(x)$ has no proper factors in $K[x]$ and is therefore irreducible. But $f(x)$ clearly has repeated roots in the splitting field, and so $f(x)$ is inseparable.

This sort of motivates why we are considering separability over a simpler idea like being squarefree. Being squarefree depends heavily on the field: $x^p - t$ was squarefree over K, but not in the splitting field. In contrast $f(x)$ is in not separable in any field extension of K.

Proposition 4.11. *a) Every irreducible polynomial over a field of characteristic 0 is separable.*

b) Over a field K of characteristic $p > 0$, every inseparable polynomial is of the form $f(x) = g(x^p)$ for some $g(x) \in K[x]$.

c) Over a field K of characteristic $p > 0$, every irredicuble polynomial is separable if the Frobenius map

$$\begin{aligned}K &\to K \\ a &\mapsto a^p\end{aligned}$$

is surjective.

Proof. We will prove a) and b) pretty much simultaneously. Suppose we have an irreducible $f(x) \in K[x]$ that is inseparable. Then $f(x)$ and $f'(x)$ has a non-constant common factor. As $f(x)$ is irreducible, its only factors are itself and 1.

Thus, if $f'(x)$ has a common factor with $f(x)$, it must be $f(x)$ itself. But $f'(x)$ is of lower degree, and so this is only possible if $f'(x) = 0$.

Over a field of characteristic 0, this implies $f(x)$ is constant. Hence every irreducible polynomial is separable.

Over a field of characteristic $p > 0$, this implies that only the coefficients of x^{kp} in $f(x)$ are non-zero: if

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

then

$$f'(x) = nx^{n-1} + (n-1)a_1 x^{n-2} + \cdots + a_{n-1} = 0$$

implies that

$$(n-k)a_k = 0$$

which occurs iff $a_k = 0$ or $n - k$ was a multiple of p.

Hence

$$f(x) = x^{np} + b_1 x^{(n-1)p} + \cdots b_{n-1}x^p + b_n = g(x^p)$$

for some polynomial $g(x)$.

Finally, to prove c), note that if the Frobenius map is surjective, then any possibly-inseparable polynomial

$$f(x) = x^{np} + b_1 x^{(n-1)p} + \cdots b_{n-1}x^p + b_n$$

is equal to

$$f(x) = x^{np}\left(d_1 x^{n-1}\right)^p + \cdots + (d_{n-1}x)^p + d_n^p$$

where $d_k^p = b_k$. As with binomials, we can write this as

$$f(x) = \left(x^n + d_1 x^{n-1} + \cdots + d_{n-1}x + d_n\right)^p$$

and so $f(x)$ is not irreducible. □

Corollary 4.12. *a) Every field of characteristic* 0 *is perfect.*

b) Every finite extension of a finite field is separable.

c) Every finite field is perfect.

Proof. a) Every irreducible polynomial over a field of characteristic 0 is separable, and so every algebraic element in any algebraic extension is separable, and so any algebraic extension is separable.

b) A finite field K contains p^n elements for some prime p and integer n. By Lagrange's Theorem/Fermat's Little Theorem, every element $a \in K$ satisfies

$$a^{p^n} = a$$

and so

$$a = \left(a^{p^{n-1}}\right)^p$$

which implies the Frobenius map is surjective, and so every irreducible polynomial is separable, and so every finite extension of a finite field is separable

c) Every finite extension of a finite field is separable, so every algebraic extension is separable, so the field is perfect.

□

5 Galois groups and Galois extensions

Definition 5.1. *Let K be a field. We denote by $\mathrm{Aut}(K)$ the group of field automorphism of K.*

Let L/K be a field extension. The subgroup of all K-automorphisms of L (previously denoted by $\mathrm{Aut}_K(L)$) is called the Galois group of L over K and is denoted by one of

$$\mathrm{Gal}(L:K) \quad \text{or} \quad \mathrm{Gal}(L/K).$$

If $K = \mathbb{Q}$, we sometimes just write $\mathrm{Gal}(L)$.

Example 5.2.

- $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$*, as any field automorphism fixes* 0 *and* 1*, and hence* $\mathbb{N}$*,* $\mathbb{Z}$*, and* $\mathbb{Q}$ *itself.*
- $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$*. As before, any field automorphism $\varphi : \mathbb{R} \to \mathbb{R}$ fixes $\mathbb{Q}$. Furthermore, if $a > b$, then there is some non-zero $c \in \mathbb{R}$ such that*

  $$a - b = c^2 \quad \Rightarrow \varphi(a) - \varphi(b) = \varphi(c)^2$$

  and so $\varphi(a) > \varphi(b)$. It is then an easy exercise to show that an order preserving map that fixes $\mathbb{Q}$ preserves supremums of bounded sets

  $$\varphi(\sup(S)) = \sup(\varphi(S))$$

  and a sup*-preserving map fixing $\mathbb{Q}$ must fix $\mathbb{R}$, as every real is the supremum of a set of rationals.*
- $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}), \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$*, as a map fixing $\mathbb{Q}$ is determined by where it sends $\sqrt{2}$. The only options are*

  $$\sqrt{2} \mapsto \sqrt{2} \quad \text{and} \quad \sqrt{2} \mapsto -\sqrt{2}$$

  both of which give valid field automorphisms (Theorem 3.26)
- $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}) = \{\mathrm{id}\}$*, as any $\mathbb{Q}$-automorphism must send $\sqrt[3]{2}$ to a solution of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$, of which there is only $\sqrt[3]{2}$.*

Our next goal is to prove a central result in Galois theory, relation the size of a field extension to that of its Galois group

Theorem 5.3. *Let L/K be a finite extension. Then*

$$|\mathrm{Gal}(L/K)| \leq [L:K]$$

with equality if and only if L is a normal and separable extension.

We will note prove this directly, but it will be an immediate consequence of the following, more general, result.

Theorem 5.4. *Let L/K and M/K be two extensions of a field K, such that L/K is finite. Then, the number of K-homomorphisms $\phi : L \to M$ is less than or equal to $[L : K]$ with equality if and only if every irreducible polynomial $f(x) \in K[x]$ with a root in L splits as a product of distinct linear factors in $M[x]$.*

Proof. We will prove the bound by induction on $[L : K]$. First suppose we have some $\alpha \in L \setminus K$ and consider the extension $K(\alpha)$. Suppose that $m_\alpha(x) \in K[x]$ is the minimal polynomial of α over K, of degree n. Then any K-homomorphism $\phi : L \to M$ restricts to a K-homomorphism $K(\alpha) \to M$.

The set of such K-homomorphisms is in bijection with the set of roots of $m_\alpha(x)$ in M. In particular, there are at most

$$\deg m_\alpha = n = [K(\alpha) : K]$$

such homomorphisms.

Fixing a K-homomorphism $\tau : K(\alpha) \to M$, we can view M and an extension of $K(\alpha)$, and hence any K-homomorphism $\phi : L \to M$ restricting to τ can be viewed as a $K(\alpha)$-homomorphism. As

$$[L : K(\alpha) = \frac{[L : K]}{[K(\alpha) : K]} < [L : K]$$

we can assume, by induction, that there are at most $[L : K(\alpha)]$ such $K(alpha)$-homomorphisms restricting to a given K-homomorphism $K(\alpha) \to M$.

As every K-homomorphism $L \to M$ corresponds to one of these pairs of a K-homomorphism $K(\alpha) \to M$ and a $K(\alpha)$-homomorphism $L \to M$, we conclude that there are at most

$$[L : K(\alpha)][K(\alpha) : K] = [L : K]$$

K-homomorphisms $L \to M$.

Now suppose there are exactly $[L : K]$ such maps. The same argument as above shows that this implies that we must have exactly $[L : K(\alpha)]$ $K(\alpha)$-homomorphisms $L \to M$ and exactly $[K(\alpha) : K]$ K-homomorphisms $K(\alpha) \to M$. This latter condition implies that $m_\alpha(x)$ has exactly

$$\deg m_\alpha = [K(\alpha) : K]$$

distinct roots in M, i.e. it splits as a product of distinct linear factors in M. As α was generic, other than $\alpha \notin K$, this must hold for every irreducible polynomial with a root in L (even the linear ones, trivially).

Conversely, suppose that every irreducible polynomial with a root in L splits as a product of distinct linear factors in M. Take some $\alpha \in L \setminus K$, and consider the extension $K(\alpha)$. Choose some $\beta \in L$ and let

$$m_\beta(x) \in K[x]$$

be the minimal polynomial over K and

$$\tilde{m}_\beta(x) \in K(\alpha)[x]$$

be the minimal polynomial over $K(\alpha)$. Clearly, we must have that $\tilde{m}_\beta(x)$ divides $m_\beta(x)$ in $K(\alpha)[x]$.

As $m_\beta(x)$ has a root (β) in L, it splits as a product of distinct linear factors in M, and so $\tilde{m}_\beta(x)$ splits as a product of distinct linear factors in M.

Hence, by induction, we can assume that we get exactly $[L : K(\alpha)]$ $K(\alpha)$-homomorphisms $L \to M$ for any given K-homomorphism $K(\alpha) \to M$, and there are exactly $[K(\alpha) : K] = \deg m_\alpha$ such maps (as $m_\alpha(x)$ splits as a product of distinct linear factors in M). Thus, there are exactly

$$[L : K(\alpha)][K(\alpha) : K] = [L : K]$$

K-homomorphisms $L \to M$. □

Theorem 5.3 follows directly from Theorem 5.4 on taking $L = M$. The set of K-homomorphisms $L \to L$ is $\mathrm{Gal}(L/K)$, as every K-homomorphism $L \to L$ is an automorphism. The condition that

$$f(x) \text{ has a root in} L \quad \Rightarrow \quad f(x) \text{ splits in } L$$

is precisely what it means to be normal, and the distinctness of the linear factors is precisely what it means to be separable. As such, we make the following definition.

Definition 5.5. *A field extension L/K is called Galois if it is finite, normal, and separable.*

Corollary 5.6. $|\mathrm{Gal}(L/K)| = [L : K]$ *if and only if L/K is Galois*

As a side effect of our proof of Theorem 5.4, we also get

Corollary 5.7. *If L/K is Galois, and we have an intermediate field $K \subset F \subset L$, then L/F is Galois.*

Remark 5.8. *The extension F/K is not necessarily Galois! It will always be separable, but may not be normal. Take for example*

$$K = \mathbb{Q}, \quad F = \mathbb{Q}(\sqrt[3]{2}), \quad L = \mathbb{Q}(\sqrt[3]{2}, \omega)$$

where ω is a complex cube root of 1.

As a quick note: recall that a field extension is finite and normal iff it is the splitting field of a polynomial (Theorem 4.3), and so a Galois extension is a separable splitting field. In particular, over a field of characteristic 0, or over a finite field, a Galois extension is the same thing as a splitting field.

5.1 Fixed fields and the Galois correspondence

So, given a Galois extension L/K, what are the intermediate fields $K \subset F \subset L$ such that F/K is Galois? To classify these, we need to introduce the notion of a fixed field.

Definition 5.9. *Let K be a field and let G be a subgroup of $\mathrm{Aut}(K)$. We define the fixed subfield of G to be the set*

$$K^G = \{a \in K \mid \sigma(a) = a \text{ for all } \sigma \in G\}.$$

Lemma 5.10. *K^G is a subfield of K.*

Proof. We can check that if $a, b \in K^G$, then

$$\sigma(a+b) = \sigma(a) + \sigma(b) = a + b$$

for all $\sigma \in G$, and

$$\sigma(ab) = \sigma(a)\sigma(b) = ab$$

and so on. Thus K^G is a subfield. □

Fixed subfields are closely related to Galois groups. For a field extension L/K, K is precisely the subfield of L fixed by $\mathrm{Gal}(L/K)$.

Theorem 5.11. *A field extension L/K is Galois if and only if $K = L^G$ for some finite $G \subset \mathrm{Aut}(L)$. Moreover, in this case, $\mathrm{Gal}(L/K) = G$.*

Proof. We start by assuming that L/K is Galois, and let

$$G = \mathrm{Gal}(L/K) \subset \mathrm{Aut}(L).$$

By definition, $\mathrm{Gal}(L/K)$ fixes K, so

$$K \subset L^G \subset L$$

and so

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

By Theorem 5.3, we also have that

$$[L : L^G] \geq |\mathrm{Gal}(L/L^G)|.$$

As any element of G fixes L^G, we must therefore have

$$G \subset \mathrm{Gal}(L/L^G) \quad \Rightarrow |G| \leq |\mathrm{Gal}(L/L^G)|.$$

Putting all these inequalities together, we find

$$[L : L^G] \leq [L : K] = |G| \leq |\mathrm{Gal}(L/L^G)| \leq [L : L^G]$$

which implies these are all equalities. Hence

$$[L : L^G] = [L : K] \quad \Rightarrow \quad [L^G : K] = 1$$

and so $L^G = K$. Furthermore

$$|G| \leq |\operatorname{Gal}(L/L^G)| \quad \Rightarrow \quad G = \operatorname{Gal}(L/L^G)$$

Now we will prove the converge. Let $G \subset \operatorname{Aut}(L)$ be some finite subgroup of automorphisms. We want to show that L/L^G is a Galois extension, and will start by showing that

$$[L : L^G] \leq |G|.$$

Suppose that

$$G = \{g_1, g_2, \ldots, g_n\}.$$

To show this inequality, we want to show that no set of $(n+1)$ elements if L are linearly independent over L^G, or equivalent that for any set $\{x_1, \ldots, x_{n+1}\}$ of $(n+1)$ elements of L are linearly dependent over L^G. Thus, we want to find $u_1, \ldots, u_{n+1} \in L^G$, not all 0, such that

$$x_1 u_1 + \cdots + x_{n+1} u_{n+1} = 0$$

Lets start by supposing such a dependency exists. We can then act on it by $g_1, g_2, \ldots, g_n$ to get n linear equations

$$0 = g_j \left(\sum_{i=1}^{n+1} x_i u_i \right) = \sum_{i=1}^{n+1} g_j(x_i) g_j(u_i) = \sum_{i=1}^{n+1} g_j(x_i) u_i$$

assuming $u_i \in L^G$. If such u_i exist, they must give a solution to this set of n linear equation in $(n+1)$ unknowns $u_1, \ldots, u_{n+1}$.

Any such system of equations has a non-trivial solution in L^{n+1}, but possibly not in L^G. Let us choose a non-trivial solution $(u_1, \ldots, u_{n+1}) \in L^{n+1}$ with as few non-zero coordinates as possible. We can assume that

$$u_1, u_2, \ldots, u_r \neq 0, \quad u_{r+1} = u_{r+2} = \cdots = u_{n+1}$$

by reordering the coordinates if needed. We can also assume that $u_1 = 1$.

Taking some $\sigma \in G$, we can apply this to our equations and solution to find that

$$\sum_{i=1}^{n+1} \sigma g_j(x_i) \sigma(u_i) = 0$$

for each $1 \leq j \leq n$. As

$$\{\sigma g_1, \sigma g_2, \ldots, \sigma g_n\} = \{g_1, \ldots, g_n\}$$

this is just a permutation of our equations, so

$$(\sigma(u_1), \ldots, \sigma(u_{n+1})) = (1, \sigma(u_2), \ldots, \sigma(u_r), 0, \ldots, 0)$$

is another solution. The space of solutions is closed under addition, so

$$(1, u_2, \ldots, u_r, 0, \ldots, 0) - (1, \sigma(u_2), \ldots, \sigma(u_r), 0, \ldots, 0)$$

is another solution. But this is

$$(0, u_2 - \sigma(u_2), \ldots, u_r - \sigma(u_r), 0, \ldots, 0)$$

which has fewer non-zero coordinates. Thus it must be trivial, and so

$$u_j = \sigma(u_j)$$

for all j. Since σ was arbitrary, $u_1, \ldots, u_{n+1}$ are elements of L^G, giving the desired L^G dependence. Thus

$$[L : L^G] \leq |G|$$

Clearly $G \subset \mathrm{Gal}(L/L^G)$, so

$$|G| \leq |\,\mathrm{Gal}(L/L^G)| \leq [L : L^G].$$

Combining these inequalities, we see that we must have

$$|\,\mathrm{Gal}(L/L^G)| = [L : L^G] \quad \text{and} \quad |G| = |\,\mathrm{Gal}(L/L^G)|.$$

Thus L/L^G is Galois and $G = \mathrm{Gal}(L/L^G)$. □

Remark 5.12. *We could also use a trick that you would likely see in a group representations course to give a different argument. As in the argument above, we can find $u_1, \ldots, u_{n+1} \in L$ such that*

$$\sum_{i=1}^{n+1} g_j(x_i) u_i = 0$$

for each $1 \leq j \leq n$. As in the proof, we can apply $\sigma \in G$ to this system of equations to find another solution

$$(\sigma(u_1), \sigma(u_2), \ldots, \sigma(u_{n+1})$$

for each $\sigma \in G$. Adding these solutions together, we get a solution

$$\left(\sum_{\sigma \in G} \sigma(u_1), \ldots, \sum_{\sigma \in G} \sigma(u_{n+1}) \right)$$

which is fixed by G. For any $g \in G$

$$g \left(\sum_{\sigma \in G} \sigma(u_i) \right) = \sum_{\sigma \in G} g\sigma(u_i) = \sum_{\sigma \in G} \sigma(u_i)$$

as g permutes the elements of G. Thus, we get a solution in L^G. We need to do a bit of work to show that this is a non-trivial solution, but it is possible.

Example 5.13. *Consider the field extension $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, we can compute the degree of the extension to be*

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 2 \times 2 = 4.$$

This extension is Galois, as it is the splitting field of $(x^2 - 2)(x^2 - 3)$, but we will show this using Theorem 5.11. Theorem 5.11 says that if we can find a finite subgroup $G \subset \mathrm{Aut}(K)$ such that

$$\mathbb{Q} = K^G$$

is the fixed subfield, then $K/\mathbb{Q}$ is Galois with Galois group G.

If it were Galois, then the Galois group would have order $[K : \mathbb{Q}] = 4$, so we are looking for a group of order 4, of which there are two:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \text{and} \quad \mathbb{Z}/4\mathbb{Z}$$

A basis of K is $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Any field automorphism of K fixes $\mathbb{Q}$ if and only if it fixes 1. Thus, any field automorphism of K fixing $\mathbb{Q}$ is completely determined by its action of $\sqrt{2}$ and $\sqrt{3}$, and must take these to roots of their minimal polynomials. Two such automorphisms are

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}, \quad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}.$$

It is an easy check to see that these generate a group G isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, as $\sigma^2 = \tau^2 = e$ and $\sigma\tau = \tau\sigma$. Furthermore, this group G fixes $\mathbb{Q}$ and only $\mathbb{Q}$: we find that

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = \sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

and

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = \tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$

if and only if $b = c = d = 0$.

Thus $K/\mathbb{Q}$ is Galois with Galois group G.

Remark 5.14. *If we didn't want to manually check that G fixes $\mathbb{Q}$ and only $\mathbb{Q}$, we could note that K/K^G is Galois with Galois group G, so*

$$[K^G/\mathbb{Q}] = \frac{[K : \mathbb{Q}]}{[K : K^G]} = \frac{4}{|G|} = \frac{4}{4} = 1$$

and hence $K^G = \mathbb{Q}$.

Recall that Corollary 4.5, there exists an element of $\mathrm{Gal}(L/K)$ taking $\alpha \in L$ to any other root β of the minimal polynomial of α $m_\alpha(x) \in K[x]$. A short corollary of Theorem 5.11 follows neatly with this observation.

Corollary 5.15. *A finite extension L/K is Galois if and only if, for every $\alpha \in L$, the minimal polynomial of α over K is*

$$M_\alpha(x) = \prod_{\beta \in \mathrm{Gal}(L/K)\cdot\alpha} (x - \beta)$$

where

$$\mathrm{Gal}(L/K) \cdot \alpha = \{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L/K)\}$$

is the set of images of α under the Galois group, without multiplicity.

Proof. Suppose L/K is Galois. Since $\mathrm{Gal}(L/K)$ permutes the elements of $\mathrm{Gal}(L/K)\cdot\alpha$, it fixes any symmetric polynomial in the elements of $\mathrm{Gal}(L/K)\cdot\alpha$. In particular, it fixes the coefficients of $M_\alpha(x)$. The elements of L fixed by $\mathrm{Gal}(L/K)$ are exactly the elements of $L^{\mathrm{Gal}(L/K)} = K$, and so $M_\alpha(x) \in K[x]$. Thus, the minimal polynomial of α $m_\alpha(x) \in K[x]$ divides $M_\alpha(x)$ in $K[x]$. Corollary 4.5 tells us that $\mathrm{Gal}(L/K)$ acts transitively on the roots of $m_\alpha(x)$, and so every root of $m_\alpha(x)$ is an element of $\mathrm{Gal}(L/K)\cdot(\alpha)$, which implies that $M_\alpha(x)$ divides $m_\alpha(x)$. They must therefore be equal.

Conversely, suppose that $M_\alpha(x)$ is the minimal polynomial of $\alpha \in L$ for every $\alpha \in L$. Clearly $M_\alpha(x)$ has no repeated roots, so α is separable over K and so L is separable over K. Now suppose $f(x) \in K[x]$ is irreducible, with a root $\alpha \in L$. Then, (up to multiplication by a constant)

$$f(x) = M_\alpha(x).$$

Since $\sigma(\alpha) \in L$ for all $\sigma \in \mathrm{Gal}(L/K)$, every root of $M_\alpha(x)$ is in L, and so $f(x) = M_\alpha(x)$ splits as a product of linear factors in $L[x]$. Thus L/K is normal and hence Galois. □

5.2 Some Galois group computations

We will later see a semi-systematic way of computing Galois groups of various extensions, but for now we will demonstrate slightly ad-hoc methods in a number of examples.

Example 5.16. *Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a complex root of $x^3 - 1$. We know this is a normal extension of $\mathbb{Q}$ (as it is the splitting field of $x^3 - 2$) and hence a Galois extension of $\mathbb{Q}$. We must have that $\mathrm{Gal}(L/\mathbb{Q})$ permutes the roots of $x^3 - 2$ (since it is irreducible over $\mathbb{Q}$), and its action is completely determined by its action on the roots (since L is obtained by adjoining the roots to $\mathbb{Q}$). Thus, $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to a subgroup of S_3. As this is a Galois extension*

$$|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{3})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \times 3 = 6 = |S_3|.$$

Hence, we must have $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$.

Example 5.17. *Let $\alpha = \sqrt{5+\sqrt{21}}$ and let $L = \mathbb{Q}(\alpha)$. We will show that it is Galois and compute its Galois group. First note that*

$$(\alpha^2 - 5)^2 - 21 = 0$$

so α is algebraic of degree at most 4. Thus

$$[L : \mathbb{Q}] \leq 4.$$

Next we note that

$$\sqrt{21} = \alpha^2 - 5 \in L \quad \Rightarrow \quad \mathbb{Q}(\sqrt{21}) \subset L.$$

Thus

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{21})][\mathbb{Q}(\sqrt{21}) : \mathbb{Q}] = 2[L : \mathbb{Q}(\sqrt{21})]$$

is even. If it is equal to 2, then $\sqrt{5+\sqrt{21}} \in \mathbb{Q}(\sqrt{21}$. Assuming this, we can show this implies

$$21x^4 - x^2 + \frac{1}{4} = 0$$

has a rational root, when this in fact has no real roots. Thus $[L : \mathbb{Q}] = 4$.

It is not too difficult to show that

$$(x^2 - 5)^2 - 21$$

splits in L, with roots

$$\alpha, -\alpha, \beta = \sqrt{5-\sqrt{21}} = \frac{2}{\alpha}, -\beta$$

and so $L/\mathbb{Q}$ is a splitting field and therefore Galois. Thus $|\operatorname{Gal}(L/\mathbb{Q})| = 4$.

An element of $\operatorname{Gal}(L/\mathbb{Q})$ is completely determined by its action on α, and since $\operatorname{Gal}(L/QQ)$ acts transitively on the roots of $(x^2-5)^2-21$, we get the four automorphisms in the Galois group for free

$$\sigma_0 : \alpha \mapsto \alpha,\ \sigma_1 : \alpha \mapsto -\alpha,\ \sigma_2 : \alpha \mapsto \beta,\ \sigma_3 : \alpha \mapsto -\beta.$$

It is easy to check that $\sigma_i^2 = \sigma_0$, so every element has order 2. Thus

$$\operatorname{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Note that every element of the Galois preserves relations among the roots! If two roots add to 0, this relation holds after applying an element of the Galois group. If two roots multiply to 2, this relation holds after applying an element of the Galois group.

A very helpful notion to keep in mind when thinking about the Galois group of the splitting field of a polynomial is the following: the Galois group permutes the roots of the polynomial, so can be viewed as a subgroup of the symmetric group. This is made precise below

Lemma 5.18. *Let $f(x) \in K[x]$ be a polynomial of degree n with splitting field L/K. Suppose that $f(x)$ has distinct roots in L. Then* $\mathrm{Gal}(L/K)$ *can be identified with a subgroup of the symmetric group S_n.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the n distinct roots of $f(x)$ in L, and let $\sigma \in \mathrm{Gal}(L/K)$. As $L = K(\alpha_1, \ldots, \alpha_n)$ is the splitting field, the action of σ on L is uniquely determined by its action on the set

$$\{\alpha_1, \alpha_2, \ldots, \alpha_n\}.$$

Furthermore, since

$$f(\sigma(\alpha_k)) = \sigma(f(\alpha_k)) = \sigma(0) = 0$$

for each $1 \leq k \leq n$, we must have that σ is determined by a map

$$\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \to \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

As σ is an automorphism, this map must be injective, and hence bijective. Thus, σ is uniquely identified by a permutation of the set $\{\alpha_1, \ldots, \alpha_n\}$. This holds true for every element of $\mathrm{Gal}(L/K)$, which lets us identify it with a subgroup of the permutation group S_n. □

5.3 The Galois correspondence

The Galois correspondence, or the fundamental group of Galois theory, is the following collection of results. It lets us relate the subgroup structure of a Galois group with the subfield structure of a field extension.

Theorem 5.19. *Let L/K be a Galois extension, with Galois group $G = \mathrm{Gal}(L/K)$. Let*

$$\mathcal{F} = \{K \subset F \subset L \mid F \text{ is a field}\}$$

be the set of intermediate fields, and let

$$\mathcal{G} = \{H \subset G \mid H \text{ a subgroup}\}$$

be the set of subgroups. Define maps

$$\gamma : \mathcal{F} \to \mathcal{G}, \quad \varphi : \mathcal{G} \to \mathcal{F}$$

by

$$\gamma(F) = \mathrm{Gal}(L/F), \quad \varphi(H) = L^H.$$

Then:

1. *If $F_1 \subset F_2$, then $\gamma(F_1) \supset \gamma(F_2)$,*
2. *If $H_1 \subset H_2$, then $\varphi(H_1) \supset \varphi(H_2)$,*
3. *$\varphi(\gamma(F)) = F$, and $\gamma(\varphi(H)) = H$,*

4. $[K : F] = |\gamma(F)|$ *and*
$$[F : K] = |G|/|\gamma(F)|,$$

5. F/K *is a normal extension (and hence a Galois extension) if and only if* $\gamma(F)$ *is a normal subgroup of* G*. In this case the Galois group is isomorphic to the quotient group*
$$\mathrm{Gal}(F/K) \cong G/\gamma(F).$$

Proof. 1. If $F_1 \subset F_2$, then any automorphism of L that fixes F_2 also fixes F_1, and so $\mathrm{Gal}(L/F_2) \subset \mathrm{Gal}(L/F_1)$, i.e. $\gamma(F_2) \subset \gamma(F_1)$.

2. If $H_1 \subset H_2$, then any element of L fixed by H_2 is fixed by H_1, and so $L^{H_2} \subset L^{H_1}$, i.e. $\varphi(H_2) \subset \varphi(H_1)$.

3. Recall that, since L/K is Galois, L/F is Galois. Thus
$$F = L^{\mathrm{Gal}(L/F)} = L^{\gamma(F)} = \varphi(\gamma(F)).$$
Similarly, for any subgroup H, L/L^H is Galois with Galois group $\mathrm{Gal}(L/L^H) = H$. That is
$$\gamma(\varphi(H)) = \mathrm{Gal}(L/\varphi(H)) = \mathrm{Gal}(L/L^H) = H.$$

4. Since L/F is Galois, $[L : F] = |\mathrm{Gal}(L/F)| = |\gamma(F)|$. By Tower Law
$$[F : K] = \frac{[L : K]}{[L : F]} = |G|/|\gamma(F)|.$$

5. We first show a property of conjugate Galois groups. Specifically, we will show that
$$\text{If } g \in G \text{ and } F \in \mathcal{F}, \text{ then } g(F) \subset \mathcal{F} \text{ and } \gamma(g(F)) = g\gamma(F)g^{-1}.$$
To prove this, we first note that
$$K \subset F \subset L$$
implies that
$$K = g(K) \subset g(F) \subset g(L) = L$$
so $g(F) \in \mathcal{F}$. Now take $h \in G$. We have $h \in \gamma(g(F))$ if and only if h fixes elements of $g(F)$, i.e.
$$\begin{aligned} & h(g(a)) = g(a) \text{ for all } a \in F \\ \Leftrightarrow\ & g^{-1}hg(a) = a \text{ for all } a \in F \\ \Leftrightarrow\ & g^{-1}hg \in \mathrm{Gal}(L/F) = \gamma(F) \end{aligned}$$

and so $h \in g\gamma(F)g^{-1}$.

Thus $\gamma(F)$ is a normal subgroup of G if and only if $\gamma(g(F)) = \gamma(F)$ for all $g \in G$. By part 3, this is equivalent to $g(F) = F$ for all $g \in G$.

So now suppose F/K is a normal extension, and let $\alpha \in F$ have minimal polynomial $m_\alpha(x) \in K[x]$. For each $g \in G$, $g(\alpha)$ is a root of $m_\alpha(x)$. Since F/K is normal and has a root of $m_\alpha(x)$, $m_\alpha(x)$ splits as a product of linear factors in $F[x]$, and so F contains all the roots of $m_\alpha(x)$. Thus $g(\alpha) \in F$ for all $g \in G$ and $\alpha \in F$. Hence $g(F) = F$ for all $g \in G$. Therefore $\gamma(F)$ is a normal subgroup of G.

Conversely, suppose $\gamma(F)$ is a normal subgroup. If $\alpha \in F$ has minimal polynomial $m_\alpha(x) \in K[x]$, then $m_\alpha(x)$ splits as a product of linear factors in $L[x]$. If $\beta \in L$ is another root, there exists $g \in G$ such that $g(\alpha) = \beta$. But $g(F) = F$, so $\beta \in F$. This holds for all roots of $m_\alpha(x)$, so $m_\alpha(x)$ splits as a product of linear factors in $F[x]$. This holds for every irreducible polynomial with a root in F, and so F/K is normal.

Finally, note that if $\gamma(F)$ is a normal subgroup, then $g(F) = F$. Hence every K-automorphism of L restricts to a K-automorphism of F. Thus, we have a map

$$\lambda : G \to \mathrm{Gal}(F/K).$$

By Corollary 4.5, every K-automorphism of F extends to one of L, so this map is surjective. The kernel of this map is, by definition,

$$\{g \in G \mid g|_F = \mathrm{id}\} = \mathrm{Gal}(L/F) = \gamma(F).$$

Thus, by the first isomorphism theorem

$$G/\gamma(F) = G/\ker\lambda \cong \mathrm{im}\ \lambda = \mathrm{Gal}(F/K).$$

□

Remark 5.20. *We could also prove the final statement by noting that*

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

and so the image of λ a subgroup of $\mathrm{Gal}(F/K)$ of the same size as $\mathrm{Gal}(F/K)$, so must be equal to it.

5.4 Examples of the Galois correspondence

We collect here some more examples of Galois group computations and applications of the Galois correspondence.

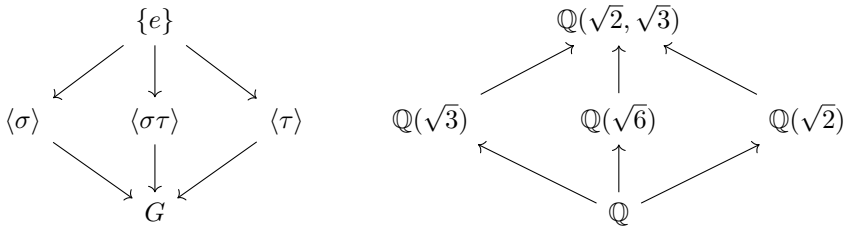
Example 5.21. *Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Recall that $G = \mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to*

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

and is generated by

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad , \quad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} .$$

Since G is abelian, every subgroup is normal, so $F/\mathbb{Q}$ is Galois for every intermediate subfield $\mathbb{Q} \subset F \subset L$. The Galois group G has subgroup diagram below, and the intermediate fields have the following inclusion diagram



We can easily compute that

$$\begin{aligned} \varphi(\{e\}) &= \mathbb{Q}(\sqrt{2}\sqrt{3})^{\{e\}} = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ \varphi(\langle\sigma\rangle) &= \mathbb{Q}(\sqrt{2}\sqrt{3})^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{3}) \\ \varphi(\langle\tau\rangle) &= \mathbb{Q}(\sqrt{2}\sqrt{3})^{\langle\tau\rangle} = \mathbb{Q}(\sqrt{2}) \\ \varphi(\langle\sigma\tau\rangle) &= \mathbb{Q}(\sqrt{2}\sqrt{3})^{\langle\sigma\tau\rangle} = \mathbb{Q}(\sqrt{6}) \\ \varphi(G) &= \mathbb{Q}(\sqrt{2}\sqrt{3})^{G} = \mathbb{Q}. \end{aligned}$$

Notably, the Galois correspondence tells us that this is a complete list of intermediate fields. As such, if we have any other intermediate field, such as $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, must be one of the above list, and we can figure this out by looking at the action of G on the given subfield. In this case, it is easy to see that $\sqrt{2}+\sqrt{3}$ is not fixed by σ, τ, or $\sigma\tau$. Hence, we must have $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Example 5.22. *Consider the product P over all possible expressions of the form*

$$1 \pm \sqrt{2} \pm \sqrt{3} \pm \cdots \pm \sqrt{99} + \pm\sqrt{100}.$$

This product is an element of

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{99})$$

which is the splitting field of $\prod_{k=2}^{99}(x^2 - k)$, and so $K/\mathbb{Q}$ is a Galois extension. Every $\mathbb{Q}$-automorphism of K must send a square root to itself or its negative, and so permutes the factors of P. Thus P is fixed by every element of $\mathrm{Gal}(K/\mathbb{Q})$ and is therefore an element of $\mathbb{Q}$. In fact, as P is an algebraic integer, $P \in \mathbb{Z}$.

Example 5.23. *Lets compute the Galois group of the splitting field of $x^4 - 3$ over $\mathbb{Q}$. The splitting field is $K = \mathbb{Q}(\sqrt[4]{3}, i)$, which is an extension of degree*

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[4]{3})][\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 2 \times 4 = 8.$$

The extension is Galois, so $|\operatorname{Gal}(K/\mathbb{Q})| = 8$ *and so it is one of*

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ (\mathbb{Z}/2\mathbb{Z})^3,\ D_4,\ Q_8$$

where

$$D_4 = \langle r, s \mid r^4 = s^2 = (sr)^2 = e \rangle$$

is the dihedral group of symmetries of the square, and Q_8 *is the quaternion group.*

A $\mathbb{Q}$*-automorphism is determined by the image of* $\sqrt[4]{3}$ *and* i*, and we must have that*

$$\begin{aligned} \sqrt[4]{3} &\mapsto \sqrt[4]{3}, i\sqrt[4]{3}, -\sqrt[4]{3}, -i\sqrt[4]{3} \\ i &\mapsto i, -i. \end{aligned}$$

To determine the Galois group, we can either try to write down every automorphism, or to find a generating set. We define two $\mathbb{Q}$*-automorphisms by*

$$\sigma : \begin{cases} \sqrt[4]{3} \mapsto i\sqrt[4]{3} \\ i \mapsto i \end{cases}, \quad \tau : \begin{cases} \sqrt[4]{3} \mapsto \sqrt[4]{3} \\ i \mapsto -i \end{cases}.$$

We can check that

$$\sigma^4 = \tau^2 = (\tau\sigma)^2 = e$$

so the subgroup of $\operatorname{Gal}(K/\mathbb{Q})$ *generated by* σ *and* τ *is isomorphic to* D_4*. Since both of these are groups of order* 8*, we therefore have*

$$\operatorname{Gal}(K/\mathbb{Q}) \cong D_4.$$

What are the fixed subfields? We have normal subgroups $\{e\}$*,* $\langle\sigma\rangle$*,* $\langle\sigma^2\rangle$*, and* $\langle\sigma, \tau\rangle$*, and*

$$\langle\tau, \sigma^2\rangle,\ \langle\sigma\tau, \sigma^2\rangle,$$

and the non-normal subgroups

$$\{e, \tau\},\ \{e, \sigma\tau\},\ \{e, \sigma^2\tau\},\ \{e, \sigma^3\tau\}$$

The fixed fields corresponding to the interesting normal subgroups are

$$\begin{aligned} \varphi(\langle\sigma\rangle) &= \mathbb{Q}(i) \\ \varphi(\langle\sigma^2\rangle) &= \mathbb{Q}(\sqrt{3}, i) \varphi(\langle\tau, \sigma^2\rangle) && = \mathbb{Q}(\sqrt{3}) \\ \varphi(\langle\sigma\tau, \sigma^2 & \\ \text{rangle}) &= \mathbb{Q}(i\sqrt{3}) \end{aligned}$$

which are the only four intermediate subfields that are Galois extensions of $\mathbb{Q}$*. Everything else is not normal, corresponding to adding a single root of* $x^4 - 3$ *to* $\mathbb{Q}$*:*

$$\varphi(\langle\tau\rangle) = \mathbb{Q}(\sqrt[4]{3}).$$

Example 5.24. *Lets determine the Galois group of the splitting field of* $x^4 - 3$ *over* $\mathbb{F}_5$*. As* $a^4 = 1$ *for all* $a \in \mathbb{F}_5$*,* $x^4 - 3$ *has no roots in* $\mathbb{F}_5$*. If we suppose*

$$x^4 - 3 = (x^2 + ax + b)(x^2 + cx + d)$$

in $\mathbb{F}_5[x]$*, we find that* $b^2 = 2$*, which has no solutions in* $\mathbb{F}_5$*, so* $x^4 - 3$ *is irreducible in* $\mathbb{F}_5[x]$*.*

We claim that

$$\mathbb{F}_{5^4} \cong \mathbb{F}_5[x]/(x^4 - 3)$$

is the splitting field. Let α *denote the image of* x *in the quotient. As* $1^4 = 2^4 = 3^4 = 4^4 = 1$ *in* $\mathbb{F}5^4$*, we have that*

$$(k\alpha)^4 = 3$$

for each $k = 1, 2, 3, 4$*. Thus* $\alpha, 2\alpha, 3\alpha, 4\alpha$ *are the roots of* $x^4 - 3$*, and so* $x^4 - 3$ *splits of* $\mathbb{F}_{5^4}$*.*

As this is a splitting field, it is a Galois extension of $\mathbb{F}_5$*. Thus, the Galois group*

$$G = \mathrm{Gal}(\mathbb{F}_{5^4}/\mathbb{F}_5)$$

has order $|G| = |\mathbb{F}_{5^4} : \mathbb{F}_5] = 4$*.*

Any $\mathbb{F}_5$*-automorphism is determined by the image of* α*, and we have at least 4 distinct automorphisms*

$$\sigma_k : \alpha \mapsto k\alpha$$

for $k = 1, 2, 3, 4$*. These must form the Galois group, and we can check that*

$$\sigma_2^2 = \sigma_4,\ \sigma_2^3 = \sigma_4,\ \sigma_2^4 = \sigma_1 = e$$

so $G \cong \mathbb{Z}/4\mathbb{Z}$*.*

This has exactly one interesting subgroup $\langle \sigma_2^2 \rangle$*, with corresponding fixed subfield spanned by elements*

$$a + b\alpha + c\alpha^2 + c\alpha^3$$

such that

$$a + b\alpha + c\alpha^2 + c\alpha^3 = a + 4b\alpha + 16c\alpha^2 + 64d\alpha^3 = a - b\alpha + c\alpha^2 - d\alpha^3.$$

Thus $b = d = 0$*, and so*

$$\varphi(\langle \sigma_2^2 \rangle) - \mathbb{F}_5(\alpha^2) \cong \mathbb{F}_{5^2}.$$

Example 5.25. *Let us find the Galois group of the splitting field of* $x^4 - 3$ *over* $\mathbb{F}_7$*. We first check if it is irreducible. It has no roots over* $\mathbb{F}_7$*, as* $a^4 \in \{0, 1, 2, 4\}$ *in* $\mathbb{F}_7$*. It does, however, split as a product of quadratic factors. If*

$$x^4 - 3 = (x^2 + ax + b)(x^2 + cx + d)$$

we must have that

$$a + c = 0,\ ac + b + d = 0,\ ad + bc = 0,\ bc = -3 = 4$$

which as solution

$$a = 2,\ b = 2,\ c = -2,\ d = 2$$

and so

$$x^4 - 3 = (x^2 + 2x + 2)(x^2 - 2x + 2).$$

Lets first adjoint a root α of $x^2 + 2x + 2$ to obtain

$$\mathbb{F}_{49} \cong \mathbb{F}_7[x]/(x^2 + 2x + 2).$$

The quadratic $x^2 + 2x + 2$ splits in this field. Does $x^2 - 2x + 2$ split in this field?

We can be clever and note that

$$x^2 - 2x + 2 = (-x)^2 + 2(-x) + 2$$

and so $-\alpha$ is a root. Otherwise, we suppose we have a root $a + b\alpha \in \mathbb{F}_{49}$ and compute

$$\begin{aligned}(a + b\alpha)^2 - 2(a + b\alpha) + 2 &= a^2 + 2ab\alpha + b^2\alpha^2 - 2a - 2b\alpha + 2 \\ &= a^2 + 2ab\alpha + b^2(-2\alpha - 2) - 2a - 2b\alpha + 2 = 0\end{aligned}$$

which implies that

$$a^2 - 2b^2 - 2a + 2 = 0, \quad 2ab - 2b^2 - 2b = 0.$$

We know there is no root with $b = 0$, so we can divide out by $2b$ in the second equation to find

$$a = b + 1.$$

Filling this into the first equation, we get

$$-b^2 + 1 = 0 \quad \Rightarrow \quad b^2 = 1 \quad \Rightarrow \quad b = \pm 1.$$

Thus we have $(a, b) = (2, 1)$ or $(a, b) = (0, -1)$. Checking these, we find that $-\alpha$ is a root!. Thus $\mathbb{F}_{49}$ is the splitting field. Thus

$$|\operatorname{Gal}(\mathbb{F}_{49}/\mathbb{F}_7)| = [\mathbb{F}_{49} : \mathbb{F}_7] = 2 \quad \Rightarrow \quad \operatorname{Gal}(\mathbb{F}_{49}, \mathbb{F}_7) \cong \mathbb{Z}/2\mathbb{Z}.$$

6 Applications of the Galois correspondence

6.1 Cyclotomic fields and regular polygons

6.1.1 Constructing a pentagon

Given points $0, 1 \in \mathbb{C}$, to construct a pentagon inscribed in the unit circle, it suffices to construct the point $\zeta = e^{2\pi i/5}$, we can then copy the distance from 1 to ζ around the circle to find all the vertices of the pentagon. So how do we construct ζ?

This root of unity is a root of

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1).$$

The polynomial $x^4+x^3+x^2+x+1$ is irreducible over $\mathbb{Q}$ (apply Eisenstein after setting $x = y + 1$), and so we can identify

$$\mathbb{Q}(\zeta) \cong \mathbb{Q}[x]/(x^4 + x^3 + x^2 + x + 1).$$

Note that the other roots of this polynomial are ζ^2, ζ^3, and ζ^4, so $\mathbb{Q}(\zeta)$ is the splitting field of $x^5 - 1$, and is a degree 4 extension. As $4 = 2^2$, there is hope that elements in this field are constructable. Specifically, ζ is constructable if we can find an intermediate field F such that

$$[\mathbb{Q}(\zeta) : F)] = [F : \mathbb{Q}] = 2.$$

Since $\mathbb{Q}(\zeta)$ is a splitting field, it is a normal extension of $\mathbb{Q}$, so the Galois correspondence tells us that intermediate fields are in bijection with subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

An element of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is completely determined by the image of ζ, which can be any of the four roots of $x^4 + x^3 + x^2 + x + 1$. If we take the automorphism σ determined by $\sigma(\zeta) = \zeta^2$, we find

$$\sigma^2(\zeta) = \zeta^4,\ \sigma^3(\zeta) = \zeta^3,\ \sigma^4(\zeta) = \zeta$$

and so σ generates a copy of $\mathbb{Z}/4\mathbb{Z}$ in $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Since

$$|\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$$

the Galois group must be isomorphic to $\mathbb{Z}/4\mathbb{Z}$. This has exactly one non-trivial subgroup, generated by σ^2, and so there is one intermediate subfield

$$F = \mathbb{Q}(\zeta)^{\langle\sigma^2\rangle}.$$

The Galois correspondence tells us that

$$[\mathbb{Q}(\zeta) : F)] = [F : \mathbb{Q}] = 2$$

so we can indeed construct ζ.

We can make this construction explicit via the Galois correspondence too. Since

$$\sigma^2(a+b\zeta+c\zeta^2+d\zeta^3) = a+b\zeta^4+c\zeta^3+d\zeta^2 = a+b(-1-\zeta-\zeta^2-\zeta^3)+c\zeta^3+d\zeta^2,$$

an element of $\mathbb{Q}(\zeta)$ is fixed by $\langle\sigma^2\rangle$ if and only if $b = 0$ and $c = d$. Hence

$$F = \mathbb{Q}(\zeta^2 + \zeta^3).$$

We can simplify this further: let

$$A = \zeta^2 + \zeta^3, \quad B = \zeta + \zeta^4.$$

Then

$$A + B = -1, \quad AB = -1$$

and so A and B are roots of

$$t^2 + t - 1, \quad \Rightarrow \quad A, B = \frac{-1 \pm \sqrt{5}}{2}.$$

Thus $F = \mathbb{Q}(\sqrt{5})$, and we can easily construct ζ from this.

We use the square root construction to construct B as the positive solution to

$$t^2 + t - 1 = \left(t + \frac{1}{2}\right)^2 - \frac{5}{4} = 0$$

and then ζ is obtained by drawing a vertical line through B, and finding the intersection with the unit circle.

To generalise this to an arbitrary polygon, we need to understand cyclotomic fields.

6.1.2 Cyclotomic fields

Let $n \in \mathbb{N}$ and denote by $\zeta_n^{\frac{2\pi i}{n}}$ a primitive n^{th} root of unity.

Definition 6.1. *The field $\mathbb{Q}(\zeta_n)$ is called the n^{th} cyclotomic field. The n^{th} cyclotomic polynomial is defined to be*

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(x - e^{\frac{2\pi i k}{n}}\right)$$

Consider the polynomial

$$x^n - 1 = \prod_{k=1}^{n} \left(x - \zeta_n^k\right) = \prod_{j=1}^{n} \left(x - e^{\frac{2\pi i k}{n}}\right).$$

For every $d|n$, we find a factor for every primitive $\left(\frac{n}{d}\right)^{\text{th}}$ root of unity, and so we can group these together to find that

$$x^n - 1 = \prod_{d|n} \Phi_{n/d}(x) = \prod_{d|n} \Phi_d(x)$$

This is a very useful way to recursively compute the cyclotomic polynomials via division, and also helps us establish the following.

Proposition 6.2. *The cyclotomic polynomials $\Phi_n(x)$ are elements of $\mathbb{Z}[x]$ and are irreducible over $\mathbb{Q}$.*

Proof. It is easy to check that $\Phi_1(x) = x - 1$ is an element of $\mathbb{Z}[x]$. Since if

$$f(x) = g(x)h(x)$$

for some non-constant polynomials $f(x), g(x) \in \mathbb{Z}[x]$ and $h(x)$, then $h(x) \in \mathbb{Z}[x]$. Thus, by induction on n, it is easy to see that

$$\Phi_n = \frac{x^n - 1}{\prod_{d|n,\, d \neq n} \Phi_d(x)}$$

must be an element of $\mathbb{Z}[x]$.

To prove that it is irreducible, we have to do a bit more work. Suppose otherwise, that

$$\Phi_n(x) = g(x)h(x)$$

for some monic polynomials with integer coefficients (Gauss Lemma lets us assume integer coefficients). Without loss of generality, we can assume $g(x)$ is irreducible over $\mathbb{Q}$. Let ξ be a root of $g(x)$ and take some prime p not dividing n. Since p does not divide n, ξ^p is also a primitive root of unity, and hence a root of $\Phi_n(x)$. If ξ^p is a root of $h(x)$, then ξ is a root of $h(x^p)$, and so $g(x)|h(x^p)$:

$$h(x^p) = g(x)\tilde{h}(x).$$

Since these all have integer coefficients, we can consider this modulo p to obtain a factorisation of $h(x^p)$ in $\mathbb{F}_p[x]$. Thus

$$h(x)^p \cong h(x^p) \cong g(x)\tilde{h}(x) \pmod{p}$$

and so $g(x)$ and $h(x)$ have a common factor mod p. This implies that $\Phi_n(x)$ has a repeated factor mod p, and so $x^n - 1$ has a repeated factor mod p. This means it has a common factor with its derivative nx^{n-1}. Since p does not divide n, the only irreducible factor of nx^{n-1} is x, which is not a factor of $x^n - 1$, a contradiction.

Therefore ξ^p is a root of $g(x)$. Iterating this argument, we see that ξ^k is a root of $g(x)$ for any k such that $\gcd(k, n) = 1$, and so every primitive root of unity is a root of $g(x)$. Therefore $g(x) = \Phi_n(x)$ must be irreducible. □

Corollary 6.3. *The Galois group of a cyclotomic field is cyclic:*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/\phi(n)\mathbb{Z}.$$

Proof. It is evident that $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$, and so it is a Galois extension of $\mathbb{Q}$. Thus

$$|\,\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

Since $\Phi_n(x)$ is the minimal polynomial of ζ_n, we have that

$$\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n(x))$$

is an extension of degree $\deg \Phi_n(x) = \phi(n)$.

Elements of the Galois group must send ζ_n to one of the roots of $\Phi_n(x)$, so every element of the Galois group is one of

$$\sigma_k : zeta_n \mapsto \zeta_n^k$$

for $\gcd(k, n) = 1$. Since

$$\sigma_k(\sigma_\ell(\zeta_n))(\zeta_n^k)^\ell = \sigma_{k\ell}(\zeta_n)$$

we see that

$$\sigma_k \circ \sigma_e ll = \sigma_{k\ell}$$

which is precisely the multiplicative group structure of $(\mathbb{Z}/n\mathbb{Z})^\times$. Thus, we have a surjective homomorphism

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma_k &\mapsto \overline{k} \end{aligned}$$

between two groups of the same order, and hence an isomorphism. □

6.1.3 Constructing regular polygons

Corollary 3.23 tells us that if a complex α is constructable, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$ for some m. Suppose

$$n = p_1^{a_1} \dots p_r^{a_r}$$

is the prime decomposition of n. Then, we know that

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) = p_1^{a_1 - 1} \dots p_r^{a_r - 1}(p_1 - 1) \dots (p_r - 1).$$

In order for this to be a power of two we need that $a_i = 1$ for any odd p_i, and furthermore that for any odd prime factor must be of the form

$$p_i = 2^{b_i} + 1$$

for some b_i.

Furthermore, as

$$x^{2k+1} + 1 = (x + 1)(x^{2k} - x^{2k-1} + x^{2k-2} - \dots - x + 1)$$

for any $k \geq 1$, we have that

$$(2^t + 1) | (2^{t(2k+1)} + 1).$$

As such, $2^b + 1$ cannot be prime if b has any odd prime factors. Thus, the odd prime factors of n must be Fermat primes.

Definition 6.4. *A number $2^{2^k} + 1$ is called a Fermat number. It is called a Fermat prime if it is prime.*

Example 6.5. *The first 5 Fermat numbers*

$$3,\ 5,\ 17,\ 257,\ 65537$$

are prime. For $k = 5$, we do not obtain a prime

$$641 | 2^{2^5} + 1 = 4294967297.$$

There are no more known examples of Fermat prime!

Theorem 6.6. *A regular n-gon (equivalently ζ_n) can be constructed using a ruler and compass if and only if*

$$n = 2^a p_1 \dots p_r$$

where $p_1, \dots, p_r$ are distinct Fermat primes.

Proof. The earlier discussion shows that no other n-gon can be constructed, so suppose we have such an n.

If we can construct the angle $\frac{2\pi}{m}$ (equivalently ζ_m) for some m, we can easily construct ζ_{2m} by bisecting the angle $\frac{2\pi}{m}$. If we can construct the angle $\frac{2\pi}{m_1}$ and $\frac{2\pi}{m_2}$ for some m_1 and m_2, we can construct the angle

$$\frac{2\pi(am_1 + bm_2)}{m_1 m_2}$$

for any integers a, b. In particular, if $\gcd(m_1, m_2) = 1$, we can find a, b such that

$$am_1 + bm_2 = 1$$

and so we can construct the angle $\frac{2\pi}{m_1 m_2}$.

Thus, it suffices to consider $n = p = 2^{2^k} + 1$ for a single Fermat prime p. By Corollary 6.3, the Galois group is

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/\phi(p)\mathbb{Z} = \mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}/2^{2^k}\mathbb{Z}.$$

Let σ be a generator of the Galois group. Then we get a sequence of subgroups

$$\{e\} \subset \langle \sigma^{2^{2^k-1}} \rangle \subset \langle \sigma^{2^{2^k-2}} \rangle \subset \cdots \langle \sigma^{2^2} \rangle \subset \langle \sigma^{2^1} \rangle \subset \mathbb{Z}/2^{2^k}/\mathbb{Z}$$

each of which is index 2 in the next. By the Galois correspondence, this corresponds to a sequence of subfields

$$\mathbb{Q}(\zeta_p) \supset \mathbb{Q}(\zeta_p)^{\langle \sigma^2 \rangle} \supset \mathbb{Q}(\zeta_p)^{\langle \sigma^{2^2} \rangle} \supset \cdots \subset \mathbb{Q}(\zeta_p)^{\langle \sigma^{2^{2^k-1}} \rangle} \supset \mathbb{Q}$$

where the degree of each extension is 2. Hence, ζ_p is constructable. □

Example 6.7. *Let us reduce constructing a 17-gon to solving a bunch of quadratics. Let $\zeta = \zeta_{17}$ and we choose the generator of $(\mathbb{Z}/17\mathbb{Z})^\times$ given by*

$$\sigma : \zeta \mapsto \zeta^3.$$

We start with the first quadratic extension of $\mathbb{Q}$, which corresponds to the subfield F_2 of $\mathbb{Q}(\zeta)$ fixed by σ^2. This has $\mathbb{Q}$-basis consisting of 1 and one of the fixed elements

$$A_3 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6$$
$$A_1 = \zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^{16} + \zeta^{15} + \zeta^{13} + \zeta^9.$$

These satisfy

$$A_3 + A_1 = \sum_{k=1}^{16} \zeta^k = -1.$$

As $\sigma(A_3) = A_1$ *and* $\sigma(A_1) = A_3$, A_3A_1 *is fixed by the Galois group and is therefore an integer. In fact, in the product,* 1 *does not appear, and each primitive root appears exactly* 4 *times, so* $A_3A_1 = -4$. *Thus, they are roots of*

$$t^2 + t - 4 = 0.$$

Next we consider the subfield F_4 *fixed by* σ^4. *This has* F_2 *basis* 1 *and one of the four fixed elements*

$$\begin{aligned} B_1 &= \zeta + \zeta^4 + \zeta^{16} + \zeta^{13} \\ B_2 &= \zeta^2 + \zeta^8 + \zeta^{15} + \zeta^9 \\ B_3 &= \zeta^3 + \zeta^{12} + \zeta^{14} + \zeta^5 \\ B_6 &= \zeta^6 + \zeta^7 + \zeta^{11} + \zeta^{10}. \end{aligned}$$

It is easy to see/check that

$$B_1 + B_2 = A_1,\ B_1B_2 = -1,\ B_3 + B_6 = A_3,\ B_3B_6 = -1$$

so we can easily construct quadratic equations for each of the B *quantities.*

Finally, we consider the subfield F_8 *fixed by* σ^8. *This has* F_4*-basis* 1 *and one of the* 8 *fixed elements*

$$\begin{aligned} C_1 &= \zeta + \zeta^{16} \\ C_2 &= \zeta^2 + \zeta^{15} \\ C_3 &= \zeta^3 + \zeta^{14} \\ C_4 &= \zeta^4 + \zeta^{13} \\ C_5 &= \zeta^5 + \zeta^{12} \\ C_6 &= \zeta^6 + \zeta^{11} \\ C_7 &= \zeta^7 + \zeta^{10} \\ C_8 &= \zeta^8 + \zeta^9. \end{aligned}$$

We have that

$$C_1 + C_4 = B_1,\ C_2 + C_8 = B_2,\ C_3 + C_5 = B_3,\ C_6 + C_7 = B_6$$

and

$$C_1C_4 = B_3,\ C_2C_8 = B_6,\ C_3C_5 = B_2,\ C_6C_7 = B_1$$

so we can construct quadratic equations for each of these. Finally, ζ *satisfies*

$$t^2 - C_0 + 1 = 0$$

so we can find ζ.

6.2 Solvability in radicals

Next we will resolve the question of whether a quartic equation can be solved in terms of radicals, as well as to motivate the formula we derived for the cubic and quartic equations. As a side effect, we will develop some useful tools for determining Galois groups of splitting fields of low degree polynomials.

Definition 6.8. *A field extension L/K is called a radical extension if there exists a tower of field extensions*

$$L = K_m \subset K_m \subset K_{m-1} \subset \cdots \subset K_1 \subset K_0 = K$$

such that for each $1 \leq i \leq m$, there exists a prime number p_i and an element $a_i \in K_i$ such that $a_i^{p_i} \in K_{i-1}$ and $K_i = K_{i-1}(a_i)$. We call each extension K_i/K_{i-1} a simple radical extension.

Remark 6.9. *We could allow non-prime powers here, but taking the n^{th} root is the same as taking several p^{th} roots for varying primes p. The definition also captures adjoining roots of unity, which is essentially the case when a_i^p is a ${p_i}^{th}$ power in K_{i-1}, but a_i is not an element of K_{i-1}.*

We want to describe when a specific element is contained within a radical extension, and so it is more convenient to discuss solvable extensions.

Definition 6.10. *A field extension L/K is called solvable (or soluable) if there is an extension M/L such that M/K is radical.*

Example 6.11. *The extension $\mathbb{Q}(\sqrt{2}, \omega)/\mathbb{Q}$, where $\omega = e^{\frac{2\pi i}{3}}$ is a radical extension, since $\omega^3 = 1$, so*

$$\mathbb{Q}(\sqrt{2}, \omega) \supset \mathbb{Q}(\omega) \supset \mathbb{Q}$$

is a sequence of simple radical extensions.

Since we know, from an earlier discussion, that

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

we have that $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$ is a radical extension.

Since we know we can solve a cubic in terms of radicals, the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is solvable, where α is a root of $x^3 - 9x + 9$. However, this is not a radical extension. To see that it is not radical, note that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

and so if this were a radical extension, it would have to be a simple radical extension:

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{b})$$

for some $b \in \mathbb{Q}$. Such an extension is not normal, and so not a splitting field. In contrast, we can show that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is the splitting field of $x^3 - 9x + 9$, and so cannot be radical.

Our goal is essentially now to describe radical and solvable fields in terms of their Galois groups, which means it is time for a bit of group theory

6.2.1 Solvable groups

Definition 6.12. *Let G be a group and define the derived subgroup of G, written $G' = [G, G]$ to be the subgroup of G generated by all commutators $ghg^{-1}h^{-1}$, where $g, h \in G$.*

The derived series of H is the sequence of subgroups

$$G^{(0)} := G, \quad G^{(k+1)} = [G^{(k)}, G^{(k)}]$$

We call G solvable (or soluable) if $G^{(m)} = \{e\}$ for some $m \geq 0$.

Example 6.13.

- *If G is abelian, $ghg^{-1}h^{-1} = e$ for all $g, h \in G$, so $G^{(1)} = \{e\}$. Hence every abelian group is solvable.*
- *If $G = S_3$, then $G^{(1)}$ is generated by $ghg^{-1}h^{-1}$ for $g, h \in S_3$.*

  i) If g and h are 3-cycles, they commute, as the only 3-cycles are (123) and $(132) = (123)^{-1}$.

  ii) If g, h are distinct 2-cycles, their commutator is a 3-cycle

  $$(12)(23)(12)(23) = (132)$$

  iii) If g, h are a 3-cycle and a 2-cycle, the commutator is again a 3-cycle

  $$(12)(123)(12)(132) = (123)$$

  Hence $G^{(1)}$ consists of the identity and the 3-cycles, i.e. the alternating group:

  $$G^{(1)} = A_3 \cong \mathbb{Z}/3\mathbb{Z}.$$

  This is abelian, so $G^{(2)} = \{e\}$ and S_3 is solvable.

Solvable groups have a number of useful properties with regards to taking quotients and subgroups, that let us more easily generate examples/non-examples

Proposition 6.14. *i) If G is solvable, and $H \subset G$ is a subgroup, then H is solvable.*

ii) If G is solvable, and $H \subset G$ is a normal subgroup, then the quotient G/H is solvable.

iii) If G is a group, with a normal subgroup $H \subset G$ such that both H and G/H are solvable, then G is solvable.

Proof. i) If $H \subset G$, it is quick to check that $H^{(1)} \subset G^{(1)}$, and so $H^{(2)} \subset G^{(2)}, \dots H^{(k)} \subset G^{(k)}$. In particular, if G is solvable, with $G^{(m)} = \{e\}$, we must have $H^{(m)} = \{e\}$, and so H is solvable.

ii) Let $\pi : G \to G/H$ be the natural projection, and note that the commutator subgroup $(G/H)^{(1)}$ is generated by elements of the form

$$(gH)(hH)(g^{-1}H)(h^{-1}H) = ghg^{-1}h^{-1}H,$$

and so $(G/H)^{(1)} \subset \pi\left(G^{(1)}\right)$. As π must take commutators to commutators, we must also have $\pi\left(G^{(1)}\right) \subset (G/H)^{(1)}$, and hence they are equal. Similarly, we must have

$$\pi\left(G^{(k)}\right) = (G/H)^{(k)}$$

and so if $G^{(m)} = \{e\}$, $(G/H)^{(m)} = \{eH\}$. Thus G/H is solvable if G is.

iii) Suppose G/H is solvable, with $(G/H)^{(m)} = \{eH\}$ for some m. Then, as in part (ii), we have that $\pi(G^{(m)}) = \{eH\}$, which means that every element of $G^{(m)}$ is contained in H:

$$G^{(m)} \subset H.$$

But then $G^{(m+1)} \subset H^{(1)}$, $G^{(m+2)} \subset H^{(2)}$, and so on, as in part (i). Thus, if H is solvable, and $H^{(k)} = \{e\}$, $G^{(m+k)} = \{e\}$, so G is solvable.

□

Corollary 6.15. *The symmetric group S_n is not solvable for any $n \geq 5$.*

Proof. As the alternating group A_5 is a subgroup of S_n for all $n \geq 5$, the previous proposition implies it is sufficient to show A_5 is not solvable. Every non-identity element of A_5 is of the form

$$(ijk) \quad \text{or} \quad (ij)(kl)$$

for distinct $1 \leq i, j, k, l \leq 5$. Since

$$\begin{aligned}(ijl)(ikm)(ijl)^{-1}(ikm)^{-1} &= (ijl)(ikm)(ilj)(imk) \\ &= (ijk)\end{aligned}$$

and

$$\begin{aligned}(ijk)(ijl)(ijk)^{-1}(ijl)^{-1} &= (ijk)(ijl)(ikj)(ilj) \\ &= (ij)(kl),\end{aligned}$$

every element of A_5 is a commutator, and so $A_5^{(1)} = A_5$. In particular, the derived series of A_5 is constant, so A_5 cannot be solvable. □

In order to related solvable groups to radical extensions, we need a more Galois-friendly reformulation, given by the following theorem.

Theorem 6.16. *For a finite group G, the following are equivalent:*

1. *G is solvable.*

2. *There exists a sequence of subgroups*

$$G = G_0 \supset G_1 \subset G_2 \supset \cdots \supset G_m = \{e\}$$

such that G_{i+1} is a normal subgroup of G_i, and the quotient G_i/G_{i+1} is abelian.

3. *There exists a sequence of subgroups*

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m = \{e\}$$

such that G_{i+1} is a normal subgroup of G_i, and the quotient G_i/G_{i+1} is cyclic of prime order.

Proof. To see that (1) $\Rightarrow$ (2), note that, for any group H, the commutator subgroup $H^{(1)} = [H, H]$ is a normal subgroup of H. If $h \in [H, H]$, then

$$ghg^{-1} = (ghg^{-1}h^{-1})h$$

is a product of two elements of h, and is therefore in H. Essentially by definition, the quotient group $H/[H, H]$ is abelian, as all commutators project to the identity. Thus, taking $G_i = G^{(i)}$, we obtain a sequence of subgroups with G_{i+1} a normal subgroup of G_i such that G_i/G_{i+1} is abelian. If G is solvable, this gives the desired sequence.

Next we assume (2). We can assume that all the inclusions in our sequence

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m = \{e\}$$

are strict. Consider one such inclusion $G_i \supset G_{i+1}$, and let $H_{i,1}$ be the maximal proper normal subgroup of G_i containing G_{i+1}. Then define a sequence of proper normal subgroups by taking $H_{i,j+1}$ to be the maximal proper normal subgroup of $H_{i,j}$ containing G_{i+1}. We must eventually find a k such that $H_{i,k} = G_{i+1}$, as the subgroups are decreasing in order, and we stop once we find this k.

As $H_{i,j+1}$ is maximal, the quotient $H_{i,j}/H_{i,j+1}$ is a simple group (that is to say, it contains no subgroups other than itself and the trivial group). Furthermore, it must be abelian: let $g, h \in H_{i,j} \subset G_i$. Since G_i/G_{i+1} is abelian, we must have that

$$ghg^{-1}h^{-1} \subset G_{i+1} \subset H_{i,j+1}.$$

As such, this commutator is also trivial in the quotient $H_{i,j}/H_{i,j+1}$, and so it is abelian. Finally, we note that every simple abelian group is cyclic of prime order. Thus, gluing the sequences

$$G_i = H_{i,0} \supset H_{i,1} \supset \cdots \supset H_{i,k} = G_{i+1}$$

together, we obtain the necessary sequence of subgroups for condition (3)

Finally to see that (3) implies (1), suppose we have such a sequence. Note that $\{e\}$ is solvable, and $G_{m-1} \cong G_{m-1}/\{e\}$ is abelian, and hence solvable. As G_{m-2}/G_{m-1} is abelian, and hence solvable, Proposition 6.14 tells us that G_{m-2} is solvable. We can repeat this argument all the way up the chain: G_i/G_{i+1} is abelian, and therefore solvable, so if G_{i+1} is solvable, so if G_i. Thus G is solvable. □

6.3 The Galois theory of radical extensions

We are now almost equipped to describe when an algebraic number is an element of a radical extension. We first need a few technical lemmas. Some are to handle roots of unity, which are necessary to have radical Galois extensions, while the others will enable us to always consider a Galois extension, even when adjoining our desired algebraic number doesn't necessarily produce one.

6.3.1 Some technical lemmas

We start with a group theory lemma, followed by a lemma that applies broadly to abelian groups, but we only need it for the multiplicative subgroups of fields.

Lemma 6.17. *Let G be an abelian group and let a be an element of maximal order m. Then, for every $g \in G$ of order r, we must have that $r|m$.*

Proof. Suppose we have an element g of order r not dividing m. Then there exists some prime p such that p^a is the maximal power of p dividing r, p^b is the maximal power of p dividing m and $a > b$. Consider the elements

$$\tilde{a} = a^{p^b} \quad \text{and} \quad \tilde{g} = g^{\frac{r}{p^a}}.$$

These have orders $\frac{m}{p^b}$ and p^a respectively. As $\gcd\left(p^a, \frac{m}{p^b}\right) = 1$, their product $\tilde{a}\tilde{g}$ must have order

$$p^a \frac{m}{p^b} = mp^{a-b} > m$$

contradicting the maximality of m. Thus $r|m$. □

Lemma 6.18. *Let E and F be two fields, and suppose we have k distinct group homomorphisms*

$$\sigma_1, \ldots, \sigma_k : E^\times \to F^\times.$$

Then there homomorphisms are linearly independent over F, which is to say that if

$$c_1\sigma_1(s) + c_2\sigma_2(s) + \cdots + c_k(\sigma_k(s) = 0$$

for every $s \in E^\times$, then $c_1 = c_2 = \cdots = c_k = 0$.

Proof. We proceed by induction on k. The case of $k = 1$ is obvious, as $\sigma(1) = 1$. Suppose it holds true for $k - 1$ distinct homomorphisms, and suppose we have k distinct homomorphisms $E^\times \to F^\times$ and $c_1, \ldots, c_k \in F$ such that

$$c_1\sigma_1(s) + \cdots + c_k\sigma_k(s) = 0$$

for all $s \in E^\times$. We can assume that none of $c_1, \ldots, c_k$ are 0, as otherwise we could apply the induction hypothesis. As this holds for all $s \in E^\times$, we must also have that

$$c_1\sigma_1(s)\sigma_1(t)+c_2\sigma_2(s)\sigma_2(t)+\cdots+c_k\sigma_k(s)\sigma_k(t) = c_1\sigma_1(st)+c_2\sigma_2(st)+\cdots+c_k\sigma_k(st) = 0$$

for all $s, t \in E^\times$. Therefore, the sum

$$c_1\sigma_1(s)\sigma_1(t)+c_2\sigma_2(s)\sigma_2(t)+\cdots+c_k\sigma_k(s)\sigma_k(t)-(c_1\sigma_1(s)+\cdots+c_k\sigma_k(s))\,\sigma_k(t)=0$$

as each major summand vanishes. This rearranges to

$$c_1(\sigma_1(t)-\sigma_k(t)\sigma_1(s)+c_2(\sigma_2(t)-\sigma_k(t))\sigma_2(s)+\cdots+c_{k-1}(\sigma_{k-1}(t)-\sigma_k(t))\sigma_{k-1}(s)=0$$

for all s and t in $E^\times$. Bu our induction hypothesis, we must therefore have

$$c_i(\sigma_1(h)-\sigma_k(t))=0$$

for each $1 \leq i \leq k-1$ and every $t \in E^\times$. But since our homomorphisms were distinct, this can only hold if $c_1 = c_2 = \cdots = c_{k-1} = 0$. This gives the desired contradiction. □

Finally, we will use these two lemmas to prove the following important proposition, relating simple radical extensions with cyclic Galois groups.

Proposition 6.19. *Suppose that a field K contains n distinct roots of unity of order n, for some $n \geq 2$. Then a Galois extension L/K with $[L:K]=n$ has Galois group $\mathbb{Z}/n\mathbb{Z}$ if and only if there exists $a \in L$ such that $L = K(a)$ and $a^n \in K$*

Proof. Suppose such an a exists. Then, $x^n - a^n$ must be irreducible over K, as otherwise we would have

$$n = [L:K] = [K(a):K] < n$$

as the minimal polynomial of a would have lower degree. Since the elements of $G = \mathrm{Gal}(K(a)/K)$ are completely determined by their action on a, and must send a root of $x^n - a^n$ to another root in $K(a)$, G is in bijection with the set of roots in L. As K contains n distinct roots of unity, these roots are

$$a,\, a\zeta_2,\, a\zeta_3, \ldots,\, a\zeta_n$$

where ζ_k is a root of unity of order n in K. It is easy to see that G must be abelian, with automorphisms given by multiplying a by the corresponding root of unity.

Let $\sigma_k : a \mapsto a\zeta_k$ be an element of maximal order m in G. If $m = n$, then σ generates G and so G is cyclic. If $m < n$, then

$$a = \sigma_k^m(a) = a\zeta_k^m \quad \Rightarrow \quad \zeta_k^m = 1.$$

For any other element $\sigma_\ell \in G$ of order r, we can similarly conclude that

$$a = \sigma_\ell^r(a) = a\zeta_\ell^r \quad \Rightarrow \quad \zeta_\ell^r = 1$$

Lemma 6.17 tells us that $r|m$, and so $\zeta_\ell^m = 1$. But this holds for every $\sigma_\ell \in G$ and hence for every ζ_ℓ, $1 \leq \ell \leq n$. This gives n solutions to a degree $m < n$ equation, giving a contradiction. Thus $m = n$ and so G is cyclic.

Conversely, suppose that $G = \mathrm{Gal}(L/K) = \langle \sigma \rangle$ is cyclic with generator σ. Choose $\zeta \in K$ a primitive root of unity, and for each $b \in L^\times$ consider the element

$$a := b + \zeta^{-1}\sigma(b) + \zeta^{-2}\sigma^2(b) + \cdots + \zeta^{1-n}\sigma^{n-1}(b).$$

As $e, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are distinct homomorphisms $L^\times \to L^\times$, Lemma 6.18 tells us that they are linearly independent. In particular, there exists a b for which a is non-zero, as the coefficients of this linear combination are non-zero.

We then see that

$$\begin{aligned}\sigma(a) &= \sigma(b) + \zeta^{-1}\sigma^2(b) + \cdots + \zeta^{1-n}\sigma^n(b) \\ &= \zeta\zeta^{-1}\sigma(b) + \zeta\zeta^{-2}\sigma^2(b) + \cdots + \zeta\zeta^{1-n}\sigma^{n-1}(b) + \zeta b \\ &= \zeta a\end{aligned}$$

and so $\sigma(a^n) = \sigma(a)^n = a^n$. Thus a^n is fixed by G and is therefore an element of K. Finally, as $\sigma^k(a) = \zeta^k a$ are all distinct, the minimal polynomial of a over K is

$$(x - a)(x - \zeta a)(x - \zeta^2 a) \cdots (x - \zeta^{n-1} a)$$

which is of degree n. Hence

$$[K(a) : K] = n = [L : K]$$

and so $L = K(a)$. □

6.3.2 Galois groups of radical extensions

Combining the results from previous section, we obtain the following

Theorem 6.20. *Suppose that L/K is a Galois extension with Galois group G, and that K contains all the p^{th} roots of unity for every prime $p \mid |G|$. Then G is solvable if and only if L/K is radical.*

Proof. By Theorem 6.16, G is solvable if and only if there exists a chain of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{e\}$$

such that $G_{i+1} \subset G_i$ is a normal subgroup, and G_i/G_{i+1} is cyclic of prime order, dividing the order of G.

By the Galois correspondence, G is therefore solvable if and only if there exists a chain of subfields

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L$$

such that K_{i+1}/K_i is normal (and therefore Galois) with cyclic Galois group of prime order dividing the order of G. As K contains all roots of unity of prime order dividing $|G|$, Proposition 6.19 tells us that this occurs if and only if K_{i+1}/K_i is a simple radical extension, which occurs if and only if L/K is radical. □

This gives us a very straightforward classification of radical extensions in terms of Galois groups, but with two major restrictions: the extension L/K must be Galois, and K must contain many roots of unity. The first of these is not too much of an issue, as the following proposition tells us that, at least in characteristic 0, freely pass to the Galois closure without losing the property of being radical, and so we can always working the a Galois extension containing the extension we are interested in.

Proposition 6.21. *Let L/K be a radical extension, and denote by L^{norm}/K the normal closure of this extension. Then L^{norm}/K is radical.*

Proof. If L/K is radical, then we can write

$$L = K(a_1, \dots, a_n)$$

with a prime p_i such that $a_i^{p_i} \in K(a_1, \dots, a_{i-1})$ for each $1 \leq i \leq n$. Let $m_i(x)$ be the minimal polynomial of a_i over K. Then the normal closure of L/K is the splitting field of $f(x) = m_1(x)m_2(x)\dots m_n(x)$. Let $\{b_i^{(j)}\}$ be the roots of $m_i(x)$, with $1 \leq j \leq d_i = \deg m_i(x)$, and let

$$K_i = K(b_s^{(j)} \mid s \leq i\} \supset K(a_1, \dots, a_i).$$

Since $b_i^{(j)}$ and a_i have the same minimal polynomial over K, there exists a K-automorphism $\tau_i^{(j)} : L^{norm} \to L^{norm}$ such that $\tau_i^{(j)}(a_i) = b_i^{(j)}$, by Corollary 4.5.

Since $a_i^{p_i} \in K(a_1, \dots, a_{i-1}) \subset K_{i-1}$, we must have that

$$\left(b_i^{(j)}\right)^{p_i} = \left(\tau_i^{(j)}(a_i)\right)^{p_i} = \tau_i^{(j)}\left(a_i^{p_i}\right) \in \tau_i^{(j)} K_{i-1}.$$

But K_{i-1} is the splitting field of $m_1(x)\dots m_{i-1}(x)$ over K, so it is a normal extension of K. From the proof of the Galois correspondence, we know that any K-automorphism of L^{norm} must map normal subextensions to themselves, so $\tau_i^{(j)} K_{i-1} = K_{i-1}$. Thus

$$\left(b_i^{(j)}\right)^{p_i} \in K_{i-1}$$

Hence K_i is a radical extension of K_{i-1}, and so K_i/K is radical. Thus L^{norm}/K is radical. □

Thus we can always moved to a normal extension, and to a Galois where our extensions are guaranteed to be separable (e.g. characteristic 0). Next, we need to address the issue of roots of unity. In order to do so, we need to work in characteristic 0, as this is where we best understand cyclotomic fields.

Proposition 6.22. *Let L/K be a Galois extension of a characteristic 0 field K, and let $n \geq 2$ be an integer. Let K'/K and L'/L be the splitting fields of $x^n - 1$ over K and L respectively. Then*

1. *If one of* $H = \mathrm{Gal}(L'/K)$, $G = \mathrm{Gal}(L/K)$, *or* $\Gamma = \mathrm{Gal}(L'/K')$ *is solvable, then all three are solvable.*

2. *The degree* $[L' : K']$ *divides* $[L : K]$.

Proof. We first note that we have a restriction map

$$\begin{aligned} \mathrm{Gal}(L'/L) &\to \mathrm{Gal}(K'/K) \\ \sigma &\mapsto \sigma|_{K'} \end{aligned}$$

This is a well defined homomorphism since

a) If $\sigma|_L = e$, then $\sigma|_K = e$, as $K \subset L$,

b) Since K'/K is a normal extension, any K-automorphism of L' must map $K' \to K$.

c) Composition is compatible with restriction.

Furthermore, this is an injective map. We can write

$$L' = L(\zeta_n), \quad K' = K(\zeta_n),$$

so any element of either Galois group is completely determined by where it sends ζ_n, which will not change upon restriction. Thus $\mathrm{Gal}(L'/L)$ is isomorphic to a subgroup of $\mathrm{Gal}(K'/K)$.

Now, since L'/L is Galois and L/K is Galois, L'/K is Galois, with Galois group H. By the Galois correspondence, Γ is a normal subgroup of H, as is $\mathrm{Gal}(L'/L)$, and we have that

$$\begin{aligned} G = \mathrm{Gal}(L/K) &\cong H/\mathrm{Gal}(L'/L) \\ \mathrm{Gal}(K'/K) &\cong H/\Gamma. \end{aligned}$$

Finally, we note that

$$\mathrm{Gal}(L'/L) \subset \mathrm{Gal}(K'/K) = \mathrm{Gal}(K(\zeta_n)/K) \subset \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

and so both $\mathrm{Gal}(L'/L)$ and $\mathrm{Gal}(K'/K)$ are abelian and hence solvable. Then, by Proposition 6.14m we have that

- H solvable implies the subgroup Γ and the quotient G are solvable,
- Γ solvable implies H is solvable, as the quotient $\mathrm{Gal}(K'/K)$ is, and hence G is solvable,
- G solvable implies that H is solvable, as the normal subgroup $\mathrm{Gal}(L'/L)$ is, and hence Γ is solvable.

To see that $[L' : K']$ divides $[L : K]$, we first note that the order a subgroup divides the order of the group, so

$$[L' : L] = |\operatorname{Gal}(L'/L)| \mid |\operatorname{Gal}(K'/K) = [K' : K].$$

Tower law tells us that

$$[L' : L][L : L] = [L' : K'][K' : K]$$

and so

$$[L : K] = \frac{[K' : K]}{[L' : L]}[L' : K']$$

is an integer multiple of $[L' : K']$. □

Using this, we can circumvent needing the roots of unity in K.

Theorem 6.23. *Suppose K is a field of characteristic 0, and let L/K be a finite field extension. This extension is solvable if and only if the normal closure L^{norm} has solvable Galois group over K.*

Proof. First suppose $\operatorname{Gal}(L^{norm}/K)$ is solvable. Let L' and K' be the splitting fields of

$$x^{[L^{norm}:K]} - 1$$

over L^{norm} and K respectively. By Proposition 6.22, L'/K' is a Galois extension with solvable Galois group. Since

$$|\operatorname{Gal}(L'/K')| = [L' : K'] \mid [L^{norm} : K]$$

K' contains all p^{th} root of unity for p dividing the order of the Galois group, and so Theorem 6.20 tells us that L'/K' is radical. Clearly K'/K is radical, so L'/K is radical, and therefore L/K is solvable.

Conversely, suppose that L/K is solvable. This means we can extend this to a radical extension M/K. Let M^{norm} be the normal closure of M. Propositions 6.21 tells us this is a radical extension of K. Now let M' and K' be the splitting fields of

$$x^{[M^{norm}:K]} - 1$$

over M^{norm} and K respectively. Then M'/K is radical.

Since $[M' : K'] \mid [M^{norm} : K]$, we have all the necessary roots of unity to conclude that $\operatorname{Gal}(M'/K')$ is solvable, and hence $\operatorname{Gal}(M^{norm}/K)$ is solvable. Thus

$$\operatorname{Gal}(L^{norm}/K) \cong \operatorname{Gal}(M^{norm}/K)/\operatorname{Gal}(M^{norm}/L^{norm})$$

is solvable. □

Corollary 6.24. *Suppose K is a field of characteristic 0, and $f(x) \in K[x]$ is a polynomial. The roots of $f(x)$ can be expressed in terms of nested radicals, roots of unity, and arithmetic operations if and only if the Galois group of the splitting field is solvable.*

6.4 Soluability of polynomials

6.4.1 The quintic case

Theorem 6.25. *Let $K = \mathbb{Q}$, and let $n \geq 5$ be an integer. Let $x_1, \ldots, x_n$ be formal variables, so that*

$$f(x) = (x - x_1)(x - x_2)\cdots(x - x_n) = x^n - e_1 x^{n-1} + e_2 x^{n-2} + \cdots \pm e_n$$

has coefficients in elementary symmetric polynomials. Then there is no formula using arithmetic operations and extractions of roots expressing $x_1, x_2, \ldots, x_n$ in terms of $e_1, \ldots, e_n$.

Proof. Consider the field $\mathbb{Q}(e_1, \ldots, e_n)$. The splitting field of $f(x)$ over $\mathbb{Q}(e_1, \ldots, e_n 0$ is $\mathbb{Q}(x_1, \ldots, x_n)$. Since this is an algebraic extension, every element of this extension can be written in the form

$$\frac{g(x_1, \ldots, x_n)}{h(e_1, \ldots, e_n)}$$

where $g(x_1, \ldots, x_n)$ is a polynomial, and $h(e_1, \ldots, e_n) \in \mathbb{Q}(e_1, \ldots, e_n)$. From Theorem 2.19, we can see that such an element is invariant under the action of S_n permuting the variables if and only if it is expressible in terms of elementary symmetric polynomials:

$$\mathbb{Q}(x_1, \ldots, x_n)^{S_n} = \mathbb{Q}(e_1, \ldots, e_n).$$

Thus

$$\mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(e_1, \ldots, e_n)) = S_n$$

which is not solvable for $n \geq 5$. The claim then follows. □

The situation is even worse than this: it is not just that there is no formula that works for arbitrary quintics, but we can write down specific quintics whose roots cannot be expressed in terms of radicals. For example, we will show $x^5 - 6x + 3$ has no roots expressible over $\mathbb{Q}$ via radicals. First, we need a useful lemma.

Lemma 6.26. *A transitive subgroup of S_5 containing a transposition is equal to S_5.*

Proof. Let G be a transitive subgroup of S_5 containing a transposition $(a\, b)$. By transitivity, we can find $\sigma_k \in G$ such that $\sigma(a) = k$ for each $k = 1, 2, 3, 4, 5$. Hence

$$\sigma(a,\ b)\sigma^{-1} = (\sigma(b)\, k) \in G.$$

Thus, every $1, 2, 3, 4, 5$ is involved in at least one transposition in G. This means that G contains at least 3 transpositions, and one number appears in 2 of them. Since the transpositions $(i\, k)$ and $(j\, k)$ generate all permutations of i, j, k G contains a copy of S_3. Relabelling if necessary, we can assume that this copy permutes $1, 2, 3$.

By transitivity, there is a $\sigma \in G$ such that $\sigma(1) = 4$. The element $\tau = \sigma(2\,3)$ also maps 1 to 4, and so

$$\sigma(1\,2)\sigma^{-1} = (4\,\sigma(2)) \quad \text{and} \quad \tau(1\,2)\tau^{-1} = (4\,\tau(2))$$

give two transpositions involving a 4. One of them must therefore not be $(4\,5)$, and so this transposition, alongside the copy of S_3, generates a copy of S_4. Finally, we know that 5 is involved in some transposition, so this, along with S_4 generates all of S_5. □

Example 6.27. *We claim the roots of $f(x) = x^5 - 6x + 3$ cannot be expressed in terms of radicals. Let L be the splitting field of $f(x)$ over $\mathbb{Q}$. It then suffices to show that $G = \mathrm{Gal}(L/\mathbb{Q})$ is not solvable. To determine this group, we need to do a bit of work. We first note that*

$$3 \mid 6,\ 3 \mid 3,\ 9 \nmid 3,$$

so $f(x)$ is irreducible by Eisenstein's criterion. Thus, G is a transitive subgroup of S_5. Based on the previous lemma, if G contains a transposition, it must equal S_5, which is not solvable.

Complex conjugation is always an automorphism of any extension of $\mathbb{Q}$, of order at most 2. As such, it is a good candidate for a transposition. However, there is no guarantee that is is a transposition. For example, it acts as the identity on the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, and as a product of a pair of disjoint transpositions on $\mathbb{Q}(\sqrt{-2}, \sqrt{-3})/\mathbb{Q}$. To show that it must be a transposition in our case, it would suffice to show that $f(x)$ has exactly 2 complex roots.

We can check that

$$\begin{aligned} f(-2) &= -17 < 0, \\ f(-1) &= 8 > 0, \\ f(1) &= -2 < 0, \\ f(2) &= 23 > 0. \end{aligned}$$

Thus, $f(x)$ has at least 3 real roots. As $f'(x) = 5x^4 - 6$ has exactly 2 real roots, $f(x)$ has exactly 2 turning points, and so $f(x)$ has exactly 3 real roots.

Thus it has exactly two non-trivial complex conjugate roots, which are swapped by complex conjugation, giving a transposition in G. Thus $G = S_5$, so the roots cannot be expressed in terms of radicals.

Remark 6.28. *Rather than having to constantly define the splitting field of a polynomial, we introduce the notation*

$$\mathrm{Gal}(f) := \mathrm{Gal}(L/K)$$

for the Galois group of the splitting field of a polynomial over K. The base field will usually be obvious from context.

6.4.2 The cubic case

We know that S_3 is solvable, as we have a sequence

$$S_3 \supset A_3 \supset \{e\}$$

of normal subgroups, for which the quotient is cyclic of prime order. This informs how we can solve a cubic in terms of radicals.

Consider an irreducible cubic $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$, with roots x_1, x_2, x_3 and Galois group $G = \mathrm{Gal}(f)$. Since $f(x)$ is irreducible, G is transitive, and hence $G = A_3$ or S_3.

If $G = A_3$, then the proof of Proposition 6.19 tells us that

$$X = x_1 + \zeta_3 x_2 + \zeta_3^2 x_3$$

generates L. Since $(123)X = \zeta_3^2 X$ and $(132)X = \omega X$, we have that X^3 is invariant under G, and so $X^3 \in \mathbb{Q}$. Similarly

$$Y = x_1 + \zeta_3^2 x_2 + \zeta_3 x_3$$

must have $Y^3 \in \mathbb{Q}$. Knowing that

$$x_1 + x_2 + x_3 = -a$$

we find

$$x_1 = \frac{X + Y - a}{3}$$

so it suffices to find X and Y.

If $G = S_3$, then X^3 and Y^3 are still invariant under A_3, but are swapped by the transpositions. Hence $X^3 + Y^3$ and $X^3 Y^3$ are elements of $\mathbb{Q}$, and so we can construct a quadratic equation for them, as we did in the very beginning! Indeed, some calculations with symmetric polynomials shows that, if

$$f(x) = x^3 + px + q$$

then

$$\left(\frac{X}{3}\right)^3 + \left(\frac{Y}{3}\right) s = -q, \quad \left(\frac{XY}{9}\right)^3 = -\frac{p}{27}$$

which gives exactly the quadratic we derived earlier!

Remark 6.29. *The expression in terms of radicals is pretty much useless in real life. For example, if we solve*

$$f(x) = x^3 - 7x + 6 = (x-1)(x-2)(x+3)$$

using the formula, we get that

$$\sqrt[3]{-3 + \frac{10}{9}\sqrt{-3}} + \sqrt[3]{-3 - \frac{10}{9}\sqrt{-3}}$$

is a root of $f(x)$. I leave you to figure out which one it is!

6.4.3 The quartic case

Let

$$V_4 = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

denote the Klein-4 normal subgroup of S_4. We can show that S_4 is solvable, as

$$S_4 \supset A_4 \supset V_4 \supset \{e\}$$

is a sequence of normal subgroups with abelian quotients.

Suppose we have an irreducible quartic

$$f(x) = x^4 + ax^3 + bx^2 + cx + d$$

with roots x_1, x_2, x_3, x_4, and let L be the splitting field of f over $\mathbb{Q}$. It is easy to check that

$$L^{V_4} = \mathbb{Q}(x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3)$$

is the fixed subfield associated to V_4. The generators of this field are permuted by the action of S_4, and so we have that

$$R(x) = (x - x_1x_2 - x_3x_4)(x - x_1x_3 - x_2x_4)(x - x_1x_4 - x_2x_3) \in \mathbb{Q}[x].$$

This is exactly (at least when $a = 0$) the auxiliary cubic we constructed in the first lecture. We can solve a cubic, so we can compute the roots $\alpha_1, \alpha_2, \alpha_3$ of $R(x)$. Then by solving

$$x^2 - \alpha_i x + d = x^2 - \alpha_i x + x_1x_2x_3x_4$$

we can find

$$x_1x_2,\ x_1x_3,\ x_1x_4$$

in terms of radicals. The product of these is

$$x_1^2(x_1x_2x_3x_4) = x_1^2 d$$

and so we can determine x_1.

6.4.4 Distinguishing Galois groups

In the above discussion, we looked at the worst case scenario, but as we saw with the cubic, knowing the Galois group can let us skip some steps and product a simpler formula for the roots. We will provide a complete description of how to identify transitive subgroups of S_3 and S_4. The first check is to compute the discriminant.

Proposition 6.30. *Let $f(x) \in K[x]$ have degree n. Then* $\mathrm{Gal}(f) \subset A_n$ *if and only if* $\mathrm{disc}(f)$ *is a square in K.*

Proof. Recall that, if $f(x)$ has roots $\alpha_1, \ldots, \alpha_n$ in the splitting field, then

$$\operatorname{disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

This is clearly invariant under the permutation action of S_n on the roots, and so is an element of K. Its square root

$$\sqrt{\operatorname{disc}(f)} = \prod_{i<j} (\alpha_i - \alpha_j)$$

is usually not. It is easy to check that

$$\sigma(\sqrt{\operatorname{disc}(f)}) = \pm\sqrt{\operatorname{disc}(f)}$$

with $\sqrt{\operatorname{disc}(f)}$ being invariant under σ if and only if $\sigma \in A_n$. Thus $\operatorname{disc}(f)$ is a square in L if and only if $\sqrt{\operatorname{disc}(f)} \in K$ if and only if $\operatorname{Gal}(f) \subset A_n$. □

This immediately separates the transitive subgroups of S_3, and provides a useful step in distinguishing transitive subgroups of S_4. The transitive subgroups of S_4, up to conjugation, are

$$S_4,\ A_4,\ D_4,\ \mathbb{Z}/4\mathbb{Z},\ V_4 \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

We have the following result.

Proposition 6.31. *Let*

$$f(x) = x^4 + ax^3 + bx^2 + cx + d \in K[x]$$

be an irreducible quartic polynomial, and let $G = \operatorname{Gal}(f)$. *Let* $R(x)$ *be the cubic defined earlier. Then:*

- *if* $\operatorname{disc}(f)$ *is not a square in* K *and* $R(x)$ *is irreducible, then* $G = S_4$,
- *if* $\operatorname{disc}(f)$ *is a square in* K *and* $R(x)$ *is irreducible, then* $G = A_4$,
- *if* $\operatorname{disc}(f)$ *is a square in* K *and* $R(x)$ *is reducible, then* $G = V_4$,
- *if* $\operatorname{disc}(f)$ *is not a square in* K, $R(x)$ *is reducible with root* $r \in K$, *and both* $x^2 + ax + b - r$ *and* $x^2 - rx + d$ *split over* $K(\sqrt{\operatorname{disc}(f)})$, *then* $G \cong \mathbb{Z}/4\mathbb{Z}$,
- *otherwise* $G \cong D_4$.

Proof. We will only consider the first three cases. If $R(x)$ is irreducible, then the splitting field contains an intermediate extension of order 3, so $3 \mid |G|$. Hence $G = S_4$ or $G = A_4$, which are distinguished by the discriminant.

If G contains a 3-cycle, this 3-cycle permutes the roots of $R(x)$, which means it must be irreducible. Thus, if $R(x)$ is not irreducible, G cannot contain a 3-cycle. If $\operatorname{disc}(f)$ is a square in K, and $R(x)$ is reducible, then G is a transitive subgroup of A_4 not containing a 3-cycle; V_4 is the only such group. □

6.5 The fundamental theorem of algebra

If you have seen a proof of the fundamental theorem of algebra, it probably made use of complex analysis in a fundamental way. Galois theory and group theory provide us with an entirely algebraic proof.

Theorem 6.32. *Every polynomial with complex coefficients has a complex root.*

Proof. We take a polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$$

and define

$$g(x) = f(x)(\overline{a}_n x^n + \overline{a}_{n-1}x^{n-1} + \cdots + \overline{a}_0)(x^2 + 1).$$

The coefficients this are invariant under complex conjugation, so $g(x) \in \mathbb{R}[x]$. Let K be the splitting field of $g(x)$ over $\mathbb{R}$. It suffices to show $K = \mathbb{C}$, as if $g(x)$ splits in $\mathbb{C}$, so does $f(x)$.

Let $G = \mathrm{Gal}(K/\mathbb{R})$, and write $|G| = 2^m q$ for some odd q. Sylow's first theorem tells us that, for any prime p, if p^k divides the order of G, G contains a subgroup of order p^k. In our case, G contains a subgroup H of order 2^m. By the Galois correspondence, K/K^H is a Galois extension of degree

$$[K : K^H] = |H| = 2^m$$

and so $K^H/\mathbb{R}$ is an extension of degree $[K^H : \mathbb{R}] = q$. We claim $q = 1$.

Suppose we have some $a \in K^H$ with minimal polynomial of degree d over $\mathbb{R}$. Since

$$d = [\mathbb{R}(a) : \mathbb{R}] \mid [K^H : \mathbb{R}] = q$$

we must have that d is odd. But every polynomial of odd degree has a real root, so if $d > 1$, the minimal polynomial of a would not be irreducible. Thus we must have $d = 1$, and so $a \in \mathbb{R}$ for all $a \in K^H$. Therefore $K^H = \mathbb{R}$ and $\mathrm{Gal}(K/\mathbb{R}) = H$.

If $m = 1$, we are done, as $K/\mathbb{R}$ is a quadratic extension of $\mathbb{R}$ containing the quadratic extension $\mathbb{C}$, and so $K = \mathbb{C}$. If $m > 1$, then we have $[K : \mathbb{C}] = 2^{m-1} > 1$. Hence $\mathrm{Gal}(K/\mathbb{C})$ is solvable by Lemma 6.33, and so we must have a sequence

$$\mathrm{Gal}(K/\mathbb{C}) = G_0 \supset G_1 \supset \cdots G_r = \{e\}$$

where $\mathrm{Gal}(K\mathbb{C})/G_1$ is cyclic of prime order, which must be 2. Thus, by the Galois correspondence, $[K^{G_1} : \mathbb{C}] = 2$. But as every element of $\mathbb{C}$ is a square in $\mathbb{C}$, every quadratic splits in $\mathbb{C}$, so $\mathbb{C}$ has no quadratic extensions. Thus, we must have $m = 1$ and $K = \mathbb{C}$. □

Lemma 6.33. *Every group of prime power order is solvable.*

Proof. Let p be prime, and suppose $|G| = p^k$. If $k = 1$, we are done, as G is cyclic. We proceed by induction.

Suppose it is true for groups of prime power order $p, p^2, \ldots, p^{k-1}$. If G has non-trivial centre $Z(G)$, this is an abelian (and solvable) normal subgroup, and the quotient $G/Z(G)$ has order $p^d < p^k$, which is solvable by the induction hypothesis. Thus, G is solvable.

So it suffices to show we have a non-trivial centre. Consider the action of G on itself by conjugation:

$$g \cdot x = gxg^{-1},$$

and let $\mathcal{C}$ be the set of conjugacy classes. For a given representative x of a conjugacy class $[x]$, we have that

$$|[x]| = \frac{|G|}{|S_x|}$$

where S_x is the stabliser of x. Hence

$$p^k = |G| = \sum_{[x]\in\mathcal{C}} |[x]| = \sum_{[x]\in\mathcal{C}} \frac{|G|}{|S_x|}.$$

We have that $\frac{|G|}{|S_x|}$ is a power of p, and that the term corresponding to $x = e$ is equal to 1. Since the sum is a power of p, this means that we must have at least one non-identity element x such that $|[x]| = 1$, and so $|G| = |S_x|$, and so $x \in Z(G)$ for some non-identity x. □

7 Some final results, and tricks for computation

7.1 Primitive element theorem

Definition 7.1. *Let L/K be a field extension. We call an element $a \in L$ a primitive element if $L = K(a)$.*

Example 7.2. *We know that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, so $\sqrt{2} + \sqrt{3}$ is a primitive element for the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$.*

We claim a primitive element always exists, though we will only show this for when the base field is infinite. For this we need a lemma.

Lemma 7.3. *Let F be an infinite field, and $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ be a non-zero polynomial. Then there exist $a_1, \ldots, a_n \in F$ such that $f(a_1, \ldots, a_n) \neq 0$.*

Proof. We induct on n. For $n = 1$, the polynomial $f(x_1)$ has only finitely many roots if it is non-zero. Thus, we can find a_1 such that $f(a_1) \neq 0$. For $n > 1$, we can write

$$f(x_1, \ldots, x_n) = f_k(x_1, \ldots, x_{n-1})x_n^k + f_{k-1}(x_1, \ldots, x_{n-1})x_n^{k-1} + \cdots + f_1(x_1, \ldots, x_{n-1})x_n + f_0(x_1, \ldots, x_{n-1}).$$

As $f(x_1, \ldots, x_n)$ is non-zero, at least one of $f_i(x_1, \ldots, x_{n-1})$ is non-zero, and so by induction there exists $(a_1, \ldots, a_{n-1}) \in F^{n-1}$ such that $f_i(a_!, \ldots, a_{n-1}) \neq 0$. Thus $f(a_1, \ldots, a_{n-1}, x_n)$ is a non-zero polynomial in 1 variable, so we can find $a_n \in F$ such that $f(a_1, \ldots, a_n) \neq 0$. □

Theorem 7.4. *A finite separable extension L of an infinite field K contains a primitive element.*

Proof. Suppose $[L : K] = n$. We first extend L/K to a Galois extension M/K, and let $G = \mathrm{Gal}(M/K)$. As this is finite, G has finitely many subgroups, and so there are finitely many intermediate subfields. In particular, there are finitely many fields

$$K \subset F \subset L.$$

Call those subfields strictly between K and L $F_1, F_2, \ldots, F_k$. Since each of these is a strict (K-vector) subspace of L, there exists a non-zero linear function

$$g_i(x_1, \ldots, x_n) : K^n \to K$$

that is 0 on every element of F_i (viewed as a vector subspace of $L \cong K^n$. These functions exist since, as K-vector spaces

$$\dim_K F_i^{\perp} = \dim_K L - \dim_K F_i > 0.$$

Let

$$f(x_1, \ldots, x_n) = g_1(x_1, \ldots, x_n) g_2(x_1, \ldots, x_n) \cdots g_k(x_1, \ldots, x_n).$$

This is a non-zero polynomial, so by Lemma 7.3 there exists $(a_1, \ldots, a_n) \in K^n \cong L$ such that $f(a_1, \ldots, a_n) \neq 0$. In particular, this gives an element $a \in L$ that is not contained in any of the $F_1, \ldots, F_k$. Thus, we have a field

$$K \subset K(a) \subset L$$

that is not equal to any of the subfield strictly contained in L. Therefore $K(a) = L$. □

7.2 Normal basis theorem

Definition 7.5. *Let L/K be a Galois extension. A K-basis of L is called normal if it is a single orbit of* $\mathrm{Gal}(L/K)$*, i.e.*

$$\{e_1, e_2, \ldots, e_n\} = \{\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)\}$$

for some $\alpha \in L$.

Example 7.6. *The $\mathbb{Q}$-basis $\{1, \sqrt{2}\}$ of $\mathbb{Q}(\sqrt{2})$ is not normal, as the Galois group does not permute the basis elements. The basis*

$$\left\{ \frac{1+\sqrt{2}}{2}, \frac{1-\sqrt{2}}{2} \right\}$$

is a normal basis.

As with the primitive basis theorem, we claim a normal basis exists, but we will only prove this in the case of infinite K. We first need a lemma.

Lemma 7.7. *Let L/K be a Galois extension with Galois group*

$$\mathrm{Gal}(L/K) = \{e = \sigma_1, \sigma_2, \ldots, \sigma_n\}$$

and let $e_1, \ldots, e_n$ be a K-basis of L. Then the set of tuples

$$\{v_i = (\sigma_1(e_i), \sigma_2(e_i), \ldots, \sigma_n(e_i))\}$$

forms an L-basis of L^n.

Proof. Suppose $\{v_1, \ldots, v_n\}$ are not linearly independent over L. Then there exists $c_1, \ldots, c_n \in L$, not all 0, such that

$$c_1 v_1 + \cdots + c_n v_n = 0.$$

Taking the components of this, we therefore have

$$c_1\sigma_1(e_i) + \cdots + c_n\sigma_n(e_i) = 0$$

for each i. Since the σ_i are K-linear, this implies that

$$c_1\sigma_1(a) + \cdots + c_n\sigma_n(a) = 0$$

for all $a \in L$. By Lemma 6.18, this implies $c_1 = \cdots = c_n = 0$, a contradiction. □

Theorem 7.8. *A Galois extension L of an infinite field K has a normal basis.*

Proof. It suffices to show that we can find some $a \in L$ such that $\sigma_1(a), \ldots, \sigma_n(a)$ are linearly independent over K. If not, then for each $a \in L$, we can find $c_1, \ldots, c_n \in K$ (not all 0) such that

$$c_1\sigma_1(a) + \cdots + c_n\sigma_n(a) = 0.$$

Applying σ_i^{-1} to this, we see that, for each $a \in L$, we can find $c_1, \ldots, c_n \in K$ such that

$$c_1\sigma_i^{-1}\sigma_1(a) + \cdots + c_n\sigma_i^{-1}\sigma_n(a) = 0$$

for all $1 \le i \le n$. This says that, for each $a \in L$, the system of linear equations

$$A(a)\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} \sigma_1^{-1}\sigma_1(a) & \sigma_1^{-1}\sigma_2(a) & \cdots & \sigma_1^{-1}\sigma_n(a) \\ \sigma_2^{-1}\sigma_1(a) & \sigma_2^{-1}\sigma_2(a) & \cdots & \sigma_2^{-1}\sigma_n(a) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n^{-1}\sigma_1(a) & \sigma_n^{-1}\sigma_2(a) & \cdots & \sigma_n^{-1}\sigma_n(a) \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$$

has a non-trivial solution for each $a \in L$. Thus $\det(A(a)) = 0$ for each $a \in L$. Choosing a K-basis $e_1, \ldots, e_n$ of L and writing a generic element of L in the form

$$x = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n$$

we have that

$$A(x) = x_1 A(e_1) + \cdots + x_n A(e_n)$$

and $\det(A(x))$ is a polynomial in $x_1, \ldots, x_n$. If we can show this polynomial is non-zero, then by Lemma 7.3 there exists

$$a = a_1 e_1 + \cdots + a_n e_n \in L$$

such that $\det(A(a)) \neq 0$, giving an element such that

$$\{\sigma_1(a), \ldots, \sigma_n(a)\}$$

are linearly independent.

To show this polynomial is non-zero, we note that is is sufficient to show that it is non-zero for any $x_1, \ldots, x_n$, even if they are elements of L, not K. From Lemma 7.7, we know that we can find $c_1, \ldots, c_n \in L$ such that

$$c_1 \sigma_i(e_1) + \cdots + c_n \sigma_i(e_n) = \begin{cases} 1 \text{ if } i = 1, \\ 0 \text{ otherwise,} \end{cases}$$

and so

$$c_1 \sigma_i^{-1} \sigma_j(a) + \cdots + c_n \sigma_i^{-1} \sigma_j(a) = \begin{cases} 1 \text{ if } i = j, \\ 0 \text{ otherwise} \end{cases} .$$

as $\sigma_1 = e$. Thus

$$c_1 A(e_1) + \cdots + c_n A(e_n) = I_n$$

is the identity matrix. Therefore, when we evaluated $\det(A(x))$ at $(c_1, \ldots, c_n)$, we obtain 1, which means $\det(A(x))$ is non-zero. The claim then follows. □

7.3 A method for computing Galois groups

Most results in this section will be presented without proof, at least temporarily.

A useful, but impractical, result on the computation of Galois groups is due to Kronecker.

Theorem 7.9. *Let K be a field, and $f(x) \in K[x]$ be a separable polynomial with roots $a_1, \ldots, a_n$ in the splitting field. Introduce formal variables $t_1, \ldots, t_n$ and define*

$$F(x; t_1, \ldots, t_n) = \prod_{\sigma \in S_n} (x - t_{\sigma(1)} a_1 - \cdots - t_{\sigma(n)} a_n).$$

Then

$$F(x; t_1, \ldots, t_n) \in K[x, t_1, \ldots, t_n].$$

Let $\tilde{F}(x; t_1, \ldots, t_n)$ be the irreducible factor of F in $K[x, t_1, \ldots, t_n]$ divisible by $(x - t_1 a_1 - \cdots - t_n a_n)$ over the splitting field. Then

$$\mathrm{Gal}(f) = \{\sigma \in S_n \mid \tilde{F}(x; t_{\sigma(1)}, \cdots, t_{\sigma(n)}) = \tilde{F}(x; t_1, \ldots, t_n)\}$$

On one hand, this is an entirely explicit way of computing a Galois group knowing only the coefficients of $f(x)$. On the other hand, expressing F in terms of these coefficients involves substantial computation with symmetric polynomials, and factorising it is quite challenging. For something more doable by hand (and by computer), we introduce the following result.

Theorem 7.10. *Let $f(x) \in \mathbb{Z}[x]$ be monic and separable, and let p be a prime. Then:*

1. $\mathrm{disc}(f) \in \mathbb{Z}$ *and*

$$\mathrm{disc}\,(f(x) \pmod p) \equiv \mathrm{disc}(f) \pmod p,$$

2. *$f(x) \pmod p$ is separable for all but finitely many p,*
3. *if $f(x) \pmod p$ is separable and splits as a product of irreducible factors of degrees $d_1, d_2, \ldots, d_k$ in $\mathbb{F}_p[x]$, then $\mathrm{Gal}(f)$ contains a permutation whose decomposition into disjoint cycles consists of a product of cycles of length d_i for each $1 \leq i \leq k$.*

Thus, by picking various primes, we can deduce a good bit of information about the Galois group. In fact, Cebotarev's density theorem tells us that, by picking p at random, we "find" all elements of $\mathrm{Gal}(f)$ with equal probability.

Example 7.11. *Let $f(x) = x^4 - 8x^2 + 4x + 2$. This is irreducible by Eisenstein's criterion for $p = 2$, so $\mathrm{Gal}(f)$ is a transitive subgroup of S_4:*

$$S_4,\ A_4,\ D_4,\ V_4,\ \mathbb{Z}/4\mathbb{Z}.$$

We can compute $\mathrm{disc}(f) = 89344 = 2^3 \cdot 349$, which is not a square in $\mathbb{Q}$, so $\mathrm{Gal}(f)$ is one of $S_4, D_4, \mathbb{Z}/4\mathbb{Z}$.

Considering $f(x)$ modulo 2, we get

$$f(x) \equiv x^4 \pmod 2$$

so $\mathrm{Gal}(f)$ contains a product of 1-cycles...

Considering $f(x)$ modulo 3, we find that $f(x)$ has a root -1 in $\mathbb{F}_3$. We compute

$$f(x) \equiv (x + 1)(x^3 - x^2 - x + 2) \pmod 3.$$

By checking for roots, we find that this cubic is irreducible, and so $\mathrm{Gal}(f)$ contains a 3-cycle. Thus $\mathrm{Gal}(f) = S_4$.

Alongside this theorem, we can often use the following to quickly show a Galois group to be S_n.

Lemma 7.12. *Let $G \subset S_n$ be a transitive subgroup containing a transposition and an $(n-1)$-cycle. Then $G = S_n$.*

Proof. We can assume, without loss of generality, that the $(n-1)$-cycle is $\sigma = (1\,2\,\cdots\,n-1)$ and that the transposition is $(a\,b)$. Since G is transitive, there exists $\tau \in G$ such that $\tau(b) = n$, and so G contains the transposition

$$\tau(a\,b)\tau^{-1} = (\tau(a)\,n) = (k\,n).$$

Then G contains

$$\sigma^m(k\,n)\sigma^{-m} = (\sigma^m(k)\,n)$$

for each $1 \leq m \leq n-1$. Thus

$$(1\,n),\,(2\,n),\ldots,\,(n-1\,n) \in G$$

and

$$(i\,n)(j\,n)(i\,n) = (i\,j) \in G$$

for each $1 \leq i, j \leq n-1$. Thus G contains every transposition and hence $G = S_n$. □

Example 7.13. *Let $f(x) = x^5 + x^2 + 1$. We can show this is irreducible so* $\mathrm{Gal}(f)$ *is transitive and we can apply our theorem to compute* $\mathrm{Gal}(f)$*. We find that*

$$f(x) \equiv (x-1)(x^4 + x^3 + x^2 - x - 1) \pmod 3$$

is the complete factorisation in $\mathbb{F}_3[x]$, and so $\mathrm{Gal}(f)$ *contains a 4-cycle. Similarly, we find a complete factorisation*

$$f(x) \equiv (x^2 - x + 2)(x^3 + x^2 - x - 2) \pmod 5$$

in $\mathbb{F}_5[x]$, and so there is a σ that is a product of a disjoint transposition and 3-cycle. Hence σ^3 is a transposition. Thus $\mathrm{Gal}(f) = S_5$.

We can use this to construct monic $f_n(x) \in \mathbb{Z}[x]$ such that $\mathrm{Gal}(f) = S_n$ for every $n \geq 1$, as follows. We let

- $F_2(x) \in \mathbb{F}_2[x]$ be any monic irreducible polynomial of degree n,
- $F_3(x) \in \mathbb{F}_3[x]$ be any monic irreducible polynomial of degree $n-1$
- $F_5(x) \in \mathbb{F}_5[x]$ be any monic irreducible polynomial of degree $n-2$) if n is odd or $n-3$ if n is even.

We can lift these to monic polynomials $G_2(x), G_3(x), G_5(x) \in \mathbb{Z}[x]$, and define

$$f_n(x) := \begin{cases} -15G_2(x) + 10xG_3(x) + 6(x^2+2)G_5(x) \text{ if } n\text{is odd,} \\ -15G_2(x) + 10xG_3(x) + 6x(x^2+2)G_5(x) \text{ if } n\text{is even.} \end{cases}$$

Then $f_n(x)$ is monic (as $-15 + 10 + 6 = 1$) and irreducible (as it is irreducible modulo 2). It factorises as $xF_3(x)$ in $\mathbb{F}_3[x]$, so $\mathrm{Gal}(f)$ contains an $(n-1)$-cycle,

and factorises as $x^{\varepsilon_n}(x^2+2)F_5(x)$ in $\mathbb{F}_5[x]$, and so $\mathrm{Gal}(f)$ contains a product σ of a disjoin transposition and a cycle of odd length. Raising σ to the length of this odd cycle, we obtain a transposition in $\mathrm{Gal}(f)$. Hence $\mathrm{Gal}(f) = S_n$.

In fact, most irreducible polynomials of $\mathbb{Q}$ will have Galois group S_n. The probablity of a random monic $f(x) \in \mathbb{Z}[x]$ of degree n with coefficients of absolute value at most N having Galois group *not* equal to S_n decays like $\frac{C_n}{\sqrt[6]{N}}$ as $N \to \infty$. As such, the probability of a random polynomial having Galois group S_n is 1!

7.4 The inverse Galois problem

Most Galois groups are S_n, but what about the others? Do most groups appear as Galois groups? The answer, if we aren't too picky about our base field, is yes! In fact, every finite group appears as the Galois group of some extension $L/\mathbb{C}(t)$. But if we want to consider a more familiar ground field like $\mathbb{Q}$, then we have no idea. A result due to Kronecker-Weber tells us that every abelian group arises as the Galois group arises as $\mathrm{Gal}(L/\mathbb{Q})$ for L a subfield of a cyclotomic field. Shafarevich showed taht every solvable group is a Galois group over $\mathbb{Q}$. Serre gave us a surprising result which said that if all finite groups appears as Galois groups of extensions of $\mathbb{Q}$, then they appear as Galois groups of real extensions of $\mathbb{Q}$. Beyond this, little is known, and even to get all small groups, some effort is needed. We provide here an example for every finite group of order at most 8, and leave it to you to verify these. (Q_8 is particularly fun)

- $\mathbb{Z}/2\mathbb{Z}$ arises from $\mathbb{Q}(\sqrt{2})$,
- $\mathbb{Z}/3\mathbb{Z}$ arises from $\mathbb{Q}(\cos(2\pi/7))$,
- $\mathbb{Z}/4\mathbb{Z}$ arises from $\mathbb{Q}(\zeta_5)$,
- $(\mathbb{Z}/2\mathbb{Z})^2$ arises from $\mathbb{Q}(\sqrt{2}+\sqrt{3})$,
- $\mathbb{Z}/5\mathbb{Z}$ arises from $\mathbb{Q}(\cos(2\pi/11))$,
- $\mathbb{Z}/6\mathbb{Z}$ arises from $\mathbb{Q}(\zeta_7)$,
- S_3 arises from $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$,
- $\mathbb{Z}/7\mathbb{Z}$ arises from $\mathbb{Q}(\zeta_{29})^H$ where H is the subgroup of $(\mathbb{Z}/29\mathbb{Z})^\times \cong \mathbb{Z}/28\mathbb{Z}$ consisting of $H \cong \{0, 7, 14, 21\}$,
- $\mathbb{Z}/8\mathbb{Z}$ arises from $\mathbb{Q}(\cos(2\pi/17))$,
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ arises from $\mathbb{Q}(\zeta_{16})$,
- $(\mathbb{Z}/2\mathbb{Z})^3$ arises from $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$,
- D_4 arises from $\mathbb{Q}(\sqrt[4]{3}, i)$,
- Q_8 arises from
$$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{(2+\sqrt{2})(3+\sqrt{3})}).$$