Galois Theory

Konstantin Ardakov

October 2023

1. Solving polynomial equations by radicals

1.1. **Quadratic equations.** Everyone knows how to solve a quadratic equation

$$ax^2 + bx + c = 0.$$

You complete the square, writing

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

so that $(x + \frac{b}{2a})^2 = \frac{b^2-4ac}{4a^2}$ and deduce the quadratic formula

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

1.2. **Cubic equations.** In the 16th century, Ferro and Tartaglia found a way to similarly solve the cubic equation

$$ax^3 + bx^2 + cx + d = 0. \tag{1.1}$$

After making the change of variable $y = x + \frac{b}{3a}$, we obtain an equation of the form

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

Now we make the inspired substitution

$$\boxed{y = z - \frac{p}{3z}}.$$

Then we obtain

$$\left(z - \frac{p}{3z}\right)^3 + p\left(z - \frac{p}{3z}\right) + q = 0.$$

Expanding out the left hand side gives

$$z^3 - 3z^2 \cdot \frac{p}{3z} + 3z \cdot \frac{p^2}{9z^2} - \frac{p^3}{27z^3} + pz - \frac{p^2}{3z} + q = 0$$

and this miraculously simplifies down to a quadratic equation in z^3, namely

$$z^6 + qz^3 - \frac{p^3}{27} = 0.$$

Hence[1] $z^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ and we obtain the *Ferro-Tartaglia*[2] *formula*

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}} \quad .$$

Thanks go to Keyang Li for spotting many typos in these notes.

[1] making the other choice of sign in the quadratic formula leads to the same solutions

[2] popularised by Cardano in a book called *The Great Art, 1545*

1.3. **Quartic equations.** At around the same time (1540?) Cardano's student Ferrari discovered a method for solving quartic equations

$$ax^4 + bx^3 + cx^2 + dx + e = 0. \tag{1.2}$$

The substitution $y = x + \frac{b}{4a}$ reduces this to the equation

$$x^4 + px^2 + qx + r = 0.$$

We introduce a new variable θ, and try rewrite the above equation in the form

$$\boxed{(x^2 + \theta)^2 = (\tau x + \sigma)^2}$$

for certain τ, σ depending only on θ, p, q and r. Now, if $x^4 + px^2 + qx + r = 0$, then

$$(x^2 + \theta)^2 = x^4 + 2x^2\theta + \theta^2 = 2\theta x^2 + \theta^2 - px^2 - qx - r = (2\theta - p)x^2 - qx + (\theta^2 - r).$$

The right hand side equals $(\tau x + \sigma)^2 = \tau^2 x^2 + 2\tau\sigma x + \sigma^2$ if and only if

$$\tau^2 = 2\theta - p, \quad 2\tau\sigma = -q, \quad \text{and} \quad \sigma^2 = \theta^2 - r.$$

Using the first and third of these equations to define τ and σ, we deduce that

$$4(2\theta - p)(\theta^2 - r) = 4\tau^2\sigma^2 = (2\tau\sigma)^2 = q^2.$$

Dividing through by 8, we see that this holds if and only if

$$\theta^3 - \frac{p}{2}\theta^2 - r\theta + \frac{pr}{2} - \frac{q^2}{8} = 0.$$

This equation is called the *resolvent cubic* of the quartic, and can be solved using the Ferro-Tartaglia formula. Given θ, we can then form $\tau := \sqrt{2\theta - p}$ and $\sigma := -\frac{q}{2\sqrt{2\theta - p}} = -\frac{q}{2\tau}$, and then factorise our original quartic in the form

$$(x^2 + \tau x + \theta + \sigma)(x^2 - \tau x + \theta - \sigma) = 0. \tag{1.3}$$

The two quadratics can now be solved separately.

1.4. **Quintic equations.** Since the middle of the 16th century, for over two hundred years mathematicians have tried to extend the methods of the Italians to solve polynomial equations of higher degree, starting with the quintic

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0.$$

Everyone failed. Eventually, by the end of the 18th century, people became convinced that this is impossible. And indeed, in around 1800 Ruffini and then Abel proved that it is *impossible* to solve this equation, in full generality, using radical expressions similar to the quartic and the cubic. But what does this mean?

Definition 1.1. Given $y \in \mathbb{C}$, let $\mathbb{Q}(y)$ be the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and y. Similarly, given $y_1, \cdots, y_m \in \mathbb{C}$ and a subfield F of $\mathbb{C}$, then $F(y_1, \cdots, y_m)$ denotes the smallest subfield of $\mathbb{C}$ containing both F and $\{y_1, \cdots, y_m\}$.

Definition 1.2. Let F be a subfield of $\mathbb{C}$ and $y \in \mathbb{C}$. We say that y is *algebraic over* F if there exist $a_0, a_1, \cdots, a_d \in F$ with $a_d \neq 0$, such that

$$a_d y^d + a_{d-1} y^{d-1} + \cdots + a_1 y + a_0 = 0.$$

If no such equation exists, then we say that y is *transcendental over* F.

Explicitly: if y is transcendental over $\mathbb{Q}$, then $\mathbb{Q}(y)$ consists of rational functions $f(y)/g(y)$ for polynomials $f(y), g(y) \in \mathbb{Q}[y]$ with $g(y) \neq 0$; and if y is algebraic over $\mathbb{Q}$, with, say d being the least possible degree of a monic polynomial equation satisfied by y with coefficients in $\mathbb{Q}$, then

$$\mathbb{Q}(y) = \{\lambda_0 + \lambda_1 y + \cdots + \lambda_{d-1} y^{d-1} : \lambda_0, \cdots, \lambda_{d-1} \in \mathbb{Q}\}.$$

In the case of the cubic (1.1), let's assume for simplicity that the coefficients p, q of the cubic equation are rational numbers. Then we can form the chain of fields

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(\sqrt{\Delta}, z) \subset \mathbb{C}$$

where $\Delta := \frac{q^2}{4} + \frac{p^3}{27}$ and $z^3 = -\frac{q}{2} + \sqrt{\Delta} \in \mathbb{Q}(\sqrt{\Delta})$. Then by what we did above,

$$\mathbb{Q}(\sqrt{\Delta}, z)$$

contains at least one [3] of the complex roots of (1.1). Similarly in the case of the quartic (1.2), starting with rational coefficients p, q, r, we form the chain of subfields

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(\sqrt{\Delta}, z) \subset \mathbb{Q}(\sqrt{\Delta}, z, \tau) \subset \mathbb{Q}(\sqrt{\Delta}, z, \tau, \sqrt{\Delta_1}) \subset \mathbb{Q}(\sqrt{\Delta}, z, \tau, \sqrt{\Delta_1}, \sqrt{\Delta_2}) \subset \mathbb{C}$$

where Δ and z are the radicals in the Ferro-Tartaglia formula for θ, $\tau := \sqrt{2\theta - p}$, $\Delta_1 := \tau^2 - 4(\theta - \frac{q}{2\tau})$ and $\Delta_2 := \tau^2 - 4(\theta + \frac{q}{2\tau})$ are the discriminants of the quadratic factors of the quartic visible in (1.3). Then we can say that

$$\mathbb{Q}(\sqrt{\Delta}, z, \tau, \sqrt{\Delta_1}, \sqrt{\Delta_2}).$$

contains at least one of the roots of the quartic (1.2).

Definition 1.3. Let F be a subfield of $\mathbb{C}$ and let $\alpha \in \mathbb{C}$ be algebraic over F. We say that α *is solvable by radicals over* F if there exists a chain of subfields

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n$$

such that $\alpha \in F_n$, and

- for all $i = 1, \cdots, n$, there exists an element $\alpha_i \in F_i$ and a positive integer d_i, such that

$$F_i = F_{i-1}(\alpha_i) \quad \text{and} \quad \alpha_i^{d_i} \in F_{i-1}.$$

[3] Recall from the Fundamental Theorem of Algebra (a theorem from the Complex Analysis course A2) that *any* polynomial with complex coefficients splits into a product of linear factors over $\mathbb{C}$

Clearly, to determine whether or not α is solvable over F, we have to understand the *intermediate subfields* $F \subset L \subset F(\alpha)$. Recall that a field extension K/F is said to be *finite* if K is a finite dimensional F-vector space; in this case $[K : F] := \dim_F K$ is called the *degree* of the field extension.

Problem 1.4. Let K/F be a finite field extension. How can we effectively classify the intermediate subfields $F \subseteq L \subseteq K$?

1.5. **An overview of Galois theory.** The fundamental insight of Galois is that the solution to Problem 1.4 is controlled, at least in all favourable cases, by the *group of symmetries* of the larger field. More precisely:

Definition 1.5. Let $F \subset \mathbb{C}$ be a subfield, and let $f \in F[x]$ be a non-constant polynomial.

(a) The *splitting field of f over F* is the subfield of $\mathbb{C}$ generated by F together with all the roots of f in $\mathbb{C}$.

(b) A finite field extension K of F is said *Galois* if there exists some non-constant polynomial $f \in F[x]$ such that K is the splitting field of f.

(c) Let K/F be a Galois extension. The *Galois group* of K/F, written

$$\mathrm{Gal}(K/F)$$

is the group of all F-linear field automorphisms[4] of K. The group operation is composition of automorphisms.

(d) The *Galois group of the polynomial f over F* is defined to be

$$\mathrm{Gal}_F(f) := \mathrm{Gal}(K/F)$$

where K is the splitting field of f over F.

Remark 1.6. Let K be a field extension of F and let $\varphi : K \to K$ be a field automorphism. Then φ is F-linear if and only if φ fixes F pointwise.

Example 1.7. (a) $\mathrm{Gal}_{\mathbb{Q}}(x^2 - 2)$ is cyclic of order 2..

(b) Let $F := \mathbb{Q}$ and let $f = x^3 - 2$. Let $\alpha := \sqrt[3]{2} \in \mathbb{R} \subset \mathbb{C}$ and let $\omega := e^{2\pi i/3} \in \mathbb{C}$. Then f factors in $\mathbb{C}[x]$ as

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

so the splitting field of f is $K = \mathbb{Q}(\alpha, \omega)$. If $\sigma : K \to K$ is an F-linear automorphism, then $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$ shows that $\sigma(\alpha) \in \{\alpha, \omega\alpha, \omega^2\alpha\}$. This shows that every $\sigma \in G := \mathrm{Gal}(K/F)$ *induces a permutation $\underline{\sigma}$ of the roots of f*. Since the roots of f, together with F, generate K as a field, we see that if $\underline{\sigma}$ is the identity permutation, then σ is the identity automorphism. Thus, the map $\sigma \mapsto \underline{\sigma}$ gives an injective group homomorphism

$$G \hookrightarrow S_3.$$

[4]That is, the bijective ring homomorphisms $\sigma : K \to K$ that fix F pointwise

In fact, in this example we will see later that this map is also surjective.

Using the language of groups acting on sets, we will prove the following easy

Proposition 1.8. Let K/F be a finite Galois extension. Then $\mathrm{Gal}(K/F)$ is a finite group.

What do intermediate fields have to do with symmetries of the roots? Well, if $f \in F[x]$ and K is the splitting field of f over F, and if $F \subseteq L \subseteq K$ is an intermediate field, then K is still the splitting field of f over L. In other words, if K/F is Galois, then so is K/L.

Lemma 1.9. Let $F \subseteq L \subseteq K$ be an intermediate field in a Galois extension K/F.
(a) $\mathrm{Gal}(K/L)$ is a subgroup of $\mathrm{Gal}(K/F)$.
(b) If $F \subseteq L_1 \subseteq L_2 \subseteq K$ are two intermediate fields, then

$$\mathrm{Gal}(K/L_2) \leqslant \mathrm{Gal}(K/L_1).$$

In this way, we obtain a rule which associates with each intermediate field L the subgroup $\mathrm{Gal}(K/L)$ of the Galois group:

$$\left\{ \begin{array}{c} \text{intermediate fields} \\ F \subseteq L \subseteq K \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{subgroups} \\ H \leqslant \mathrm{Gal}(K/F) \end{array} \right\}$$

and this function *reverses inclusions*: the larger the intermediate field L, the smaller the associated Galois group.

Definition 1.10. Let H be a subgroup of $\mathrm{Gal}(K/F)$. The *fixed field* of H is

$$K^H := \{x \in K : \sigma(x) = x \quad \text{for all} \quad \sigma \in H\}.$$

It is easy to see that K^H is indeed a subfield of K containing F.

Theorem 1.11. [Main Theorem of Galois Theory 1] Let $F \subseteq L \subseteq K$ be an intermediate field in a Galois extension K/F. Then we have $L = K^{\mathrm{Gal}(K/L)}$, so the map $L \mapsto \mathrm{Gal}(K/L)$ is *injective*.

In other words, the subgroup $\mathrm{Gal}(K/L)$ of $\mathrm{Gal}(K/F)$ *completely determines* the intermediate field L. Combining Theorem 1.11 with Proposition 1.8, we obtain the interesting

Corollary 1.12. A finite Galois extension K/F has *only finitely many* intermediate subfields L.

In fact, the map $L \mapsto \mathrm{Gal}(K/L)$ also turns out to be surjective!

Theorem 1.13. [Main Theorem of Galois Theory 2] Let K/F be a Galois extension and let $H \leqslant \mathrm{Gal}(K/F)$. Let $L := K^H$. Then $F \subseteq L \subseteq K$, and $\mathrm{Gal}(K/L) = H$.

In other words, at least for Galois extensions, the intermediate subfields correspond *bijectively* with the subgroups of the Galois group.

But what does this have to do with understanding whether some $\alpha \in \mathbb{C}$ which is algebraic over a subfield F is solvable over F? Recall that a group G is said to be *solvable* if there exists a chain

$$\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_m = G$$

for some subgroups $G_0, G_1, \cdots, G_m$ of G such that:

- G_{i-1} is *normal* in G_i for all $i = 1, \cdots, m$, and
- the factor group G_i/G_{i-1} is abelian for all $i = 1, \cdots, m$.

Example 1.14. (a) S_3 is solvable: we have the chain

$$\{1\} \triangleleft A_3 \triangleleft S_3$$

with A_3 cyclic of order 3, and S_3/A_3 cyclic of order 2.

(b) S_4 is solvable: we have the chain

$$\{1\} \triangleleft \langle (12)(34) \rangle \triangleleft V_4 \triangleleft A_4 \triangleleft S_4.$$

(c) A_n and S_n are *not* solvable for any $n \geq 5$.

(d) Let q be a prime power and let $\mathbb{F}_q$ be a finite field of order q. The group of upper-triangular invertible matrices

$$B_n(\mathbb{F}_q) = \{g \in \mathrm{GL}_n(\mathbb{F}_q) : g_{ij} = 0 \quad \text{for all} \quad i > j\}$$

is solvable for all $n \geq 1$.

Using Theorems 1.11 and 1.13, we will prove the following group-theoretic characterisation of solvability.

Theorem 1.15. Let F be a subfield of $\mathbb{C}$ and let α be algebraic over F, with minimal polynomial $m_{F,\alpha}(t)$ over F. Then the following are equivalent:

(1) α is solvable by radicals over F,
(2) the Galois group $\mathrm{Gal}_F(f)$ is a solvable group.

Theorem 1.15 explains why certain quintic equations do not admit solutions by radicals. In fact, we will later on see an explicit example of a polynomial $f \in \mathbb{Q}[x]$ whose Galois group over $\mathbb{Q}$ is S_5.

2. Background from algebra

Definition 2.1. Let K/F be a field and let $\alpha \in K$ be algebraic over F. The *minimal polynomial of α over F* is the monic polynomial $m_{F,\alpha} \in F[t]$ of least degree such that $m_{F,\alpha} = 0$.

Remark 2.2. We always have the *evaluation map* $\mathrm{ev}_\alpha : F[t] \to K$, given by $\mathrm{ev}_\alpha(g) = g(\alpha)$ for each $g \in F[t]$. The condition that α is algebraic over F is equivalent to $\ker \mathrm{ev}_\alpha$ being non-zero. But $\ker \mathrm{ev}_\alpha$ is an ideal of $F[t]$, which is a principal ideal domain. In this way, we see that $\ker \mathrm{ev}_\alpha = \langle m_{F,\alpha} \rangle$ and in fact $m_{F,\alpha}$ is the unique monic generator of $\ker \mathrm{ev}_\alpha$.

This viewpoint on the minimal polynomial implies the following important

Corollary 2.3. Let $h \in F[t]$. Then $h(\alpha) = 0 \Leftrightarrow m_{F,\alpha}$ divides h.

The following is fundamental.

Lemma 2.4. Let K/F be a finite extension and let $\alpha \in K$. Then α is algebraic over F.

Proof. Let $n = [K : F]$. Then $\{1, \alpha, \alpha^2, \cdots, \alpha^n\}$ is linearly dependent over F. So we can find $\lambda_n, \lambda_{n-1}, \cdots, \lambda_0 \in F$ such that $\lambda_n \alpha^n + \cdots + \lambda_1 \alpha + \lambda_0 = 0$. □

Let $F[\alpha]$ be the subring of K generated by F and α. In other words, this is just the image of $\mathrm{ev}_\alpha : F[t] \to K$.

Lemma 2.5. $F[\alpha] \cong F[t]/\langle m_{F,\alpha} \rangle$ as rings.

Proof. This follows from the First Isomorphism Theorem for rings. □

Lemma 2.6. Let $d := \deg m_{F,\alpha}$. Then $\{1, \alpha, \cdots, \alpha^{d-1}\}$ is basis for $F[\alpha]$ over F, so $\dim_F F[\alpha] = d$.

Proof. By the division algorithm, for every $f \in F[t]$, there are unique $q, r \in F[t]$ with $\deg r < d := \deg m_{F,\alpha}$ such that $f = q\, m_{F,\alpha} + r$. So, the image of $\{1, t, \cdots, t^{d-1}\}$ in $F[t]/\langle m_{F,\alpha} \rangle$ is an F-basis. Now use Lemma 2.5. □

Lemma 2.7. If $\alpha \in K$ is algebraic over F, then $F(\alpha) = F[\alpha]$.

Proof. $F[\alpha]$ is an integral domain, being a subring of the field K. Let $0 \neq x \in F[\alpha]$; then the multiplication-by-x map $L_x : F[\alpha] \to F[\alpha]$ is injective. Now, $\dim_F F[\alpha]$ is finite by Lemma 2.6, so L_x is also surjective by Rank-Nullity. So, there exists $y \in F[\alpha]$ such that $L_x(y) = 1$. But $L_x(y) = xy$, so x is invertible in $F[\alpha]$. So, $F[\alpha]$ is already a field, and hence is the subfield $F(\alpha)$ of K generated by F and α. □

Corollary 2.8. If $\alpha \in K$ is algebraic over F, then $m_{F,\alpha}$ is irreducible over F.

Proof. Since $F(\alpha) \cong F[t]/\ker \mathrm{ev}_\alpha$ is field, $\ker \mathrm{ev}_\alpha = \langle m_{F,\alpha} \rangle$ is a maximal ideal. Hence $m_{F,\alpha}$ is irreducible. □

Remark 2.9. You may wonder why the minimal polynomials m_T of linear transformations $T : V \to V$ that you encountered in Part A Linear Algebra were in general not irreducible. The reason is that whilst it is still the case that m_T is

the monic generator of the ideal $\ker \mathrm{ev}_T$ of $F[t]$, where $\mathrm{ev}_T : F[t] \to \mathrm{End}(V)$ is the evaluation at T map, the codomain of ev_T is the ring $\mathrm{End}(V)$ of linear maps from $V \to V$, which is isomorphic to a matrix ring $M_n(F)$ (after choosing a basis for V), and which *has zero-divisors* as soon as $n \geq 2$.

Definition 2.10. Let K/F be a field extension. Then the *degree* of K over F is

$$[K : F] := \dim_F K.$$

Corollary 2.11. For all α algebraic over F, we have $[F(\alpha) : F] = \deg m_{F,\alpha}(t)$.

Proof. Use Lemma 2.6 and Lemma 2.7. □

It is important to be able to compute minimal polynomials of algebraic numbers.

Example 2.12. (a) Let $\alpha = \sqrt{2}$. Then $f = x^2 - 2 \in \mathbb{Q}[x]$ vanishes at α, so $m_{\mathbb{Q},\alpha} \mid f$. If f was reducible over $\mathbb{Q}$ then it would have a linear factor, and then $\sqrt{2} \in \mathbb{Q}$ which is not the case. So, f is irreducible over $\mathbb{Q}$ and hence $m_{\mathbb{Q},\alpha} = f$.

(b) Let $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C}$. Then $\omega^3 = 1$ but $\omega \neq 1$, so $\omega^2 + \omega + 1 = \frac{\omega^3 - 1}{\omega - 1} = 0$. Hence $m_{\mathbb{Q},\omega} \mid x^2 + x + 1$. If $\deg m_{\mathbb{Q},\omega} = 1$, then $\omega \in \mathbb{Q}$, but of course $\omega = \frac{-1+i\sqrt{3}}{2} \notin \mathbb{R}$. So $\deg m_{\mathbb{Q},\omega} = 2$ and $m_{\mathbb{Q},\omega} = x^2 + x + 1$.

(c) Let $\alpha = \sqrt[3]{2}$. The polynomial $f = x^3 - 2$ is irreducible over $\mathbb{Z}$ by Eisenstein's Criterion at $p = 2$. Hence it is also irreducible over $\mathbb{Q}$ by Gauss's Lemma [5]. Since $m_{\mathbb{Q},\alpha} \mid f$ we must have equality.

We now come to a very important result.

Theorem 2.13 (Tower Law)**.** Let $K/L/F$ be finite field extensions. Then

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

Proof. Let $\{x_1, \ldots, x_m\}$ be a basis for L as an F-vector space, and let $\{y_1, \cdots, y_n\}$ be a basis for K as an L-vector space. It will be enough to show that

$$\{x_i y_j : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$$

is a basis for K as an F-vector space. This set spans K, because

$$K = \sum_{j=1}^{m} L y_j = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} F x_i \right) y_j = \sum_{i=1}^{n} \sum_{j=1}^{n} F x_i y_j.$$

Suppose now that $\sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_{ij} x_i y_j = 0$ for some $\lambda_{ij} \in F$. Then since $\{y_1, \cdots, y_m\}$ is linearly independent over L, for each $j = 1, \cdots, m$ we have $\sum_{i=1}^{n} \lambda_{ij} x_i = 0$. Since $\{x_1, \cdots, x_n\}$ is linearly independent over F, we deduce $\lambda_{ij} = 0$ for all i, j. □

[5] see Problem Sheet 1 for a refresher on these two results from Part A Rings and Modules

3. Upper bounds on the size of the Galois group

We briefly recall some facts about group actions on sets from Prelims.

Definition 3.1. Let G be a group. A *G-action on a set X* is a function

$$a : G \times X \to X, \quad (g, x) \mapsto a(g, x)$$

such that

(1) $a(1, x) = x$ for all $x \in X$,
(2) $a(g, a(h, x)) = a(gh, x)$ for all $g, h \in G$ and all $x \in X$.

Given a group G and a set X, there will in general be several different actions of G on X. Nevertheless, it is very standard to omit the letter a specifying the particular action from the notation, so we will write

$$g \cdot x = a(g, x)$$

whenever the group action $a : G \times X \to X$ is understood. In this language, the two axioms for a group action become

$$1 \cdot x = x \quad \text{and} \quad g \cdot (h \cdot x) = (gh) \cdot x \quad \text{for all} \quad g, h \in G, x \in X.$$

Let G act on X. We say that a subset Y of X is *G-stable* if $g \cdot y \in Y$ for all $y \in Y$. In this case, G also acts on Y. We recall the following two constructions.

Definition 3.2. Let G act on a set X.

(1) If H is a subgroup of G, then H also acts on X by *restriction*:

$$h \cdot x := g \cdot x \quad \text{for all} \quad h \in H, x \in X.$$

(2) Suppose that G acts also acts on Y. Then G also acts on $X \times Y$ via

$$g \cdot (x, y) := (g \cdot x, g \cdot y) \quad \text{for all} \quad g \in G, (x, y) \in X \times Y.$$

This is called the *diagonal action*.

The key example of a group action in Galois Theory is the following

Lemma 3.3. Let K/F be a field extension and let $G = \mathrm{Gal}(K/F)$, so that G acts on K. Let $f \in F[t]$ and let

$$V(f) := \{\alpha \in K : f(\alpha) = 0\}.$$

Then $V(f)$ is a G-stable subset of K and hence G also acts on $V(f)$.

Proof. Let $\sigma \in G$ and $\alpha \in V(f)$. Write $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$. Then

$$f(\sigma(\alpha)) = \sum_{i=0}^{n} a_i \sigma(\alpha)^i = \sum_{i=0}^{n} a_i \sigma(\alpha^i) = \sigma\left(\sum_{i=0}^{n} a_i \alpha^i\right) = \sigma(f(\alpha)) = \sigma(0) = 0$$

using the fact that σ is an F-linear ring homomorphism. Hence $\sigma(\alpha) \in V(f)$ for all $\alpha \in V(f)$, so $V(f)$ is G-stable. $\square$

There is really only one main theorem about group actions - Theorem 3.7.

Definition 3.4. Let G be a group acting on a set X, and let $x \in X$.

(1) The *stabiliser* of x is the set $\mathrm{Stab}_G(x) := \{g \in G : g \cdot x = x\} \subset G$.
(2) The *orbit* of x is the set $G \cdot x := \{g \cdot x : g \in G\} \subset X$.

Recall from Prelims that $\mathrm{Stab}_G(x)$ is always subgroup of G. Since X carries no structure, the orbit $G \cdot x$ is just a set. However, we always have the *orbit map*

$$\pi_x : G \to G \cdot x$$

given by $\pi_x(g) = g \cdot x$ for all $g \in G$. This map is always surjective, and $\pi_x^{-1}(x)$ is just the stabiliser $\mathrm{Stab}_G(x)$ of x.

Proposition 3.5. Let G be a group acting on a set X and let $x \in X$. Then

$$\pi_x^{-1}(g \cdot x) = g\,\mathrm{Stab}_G(x) \quad \text{for all} \quad g \in G.$$

Proof. We have $\pi_x(g) = g \cdot x$. Now for $h \in G$, we have

$$h \in \pi_x^{-1}(g \cdot x) \Leftrightarrow h \cdot x = g \cdot x \Leftrightarrow g^{-1}h \in \mathrm{Stab}_G(x) \Leftrightarrow h \in g\,\mathrm{Stab}_G(x).$$

So, $\pi_x^{-1}(g \cdot x) = g\,\mathrm{Stab}_G(x)$. □

Corollary 3.6. Suppose that G is a possibly infinite group acting on a finite set X. Suppose that there exists $x \in X$ such that $\mathrm{Stab}_G(x)$ is finite. Then G is finite.

Proof. The orbit $G \cdot x$ is finite because X is finite. Write $G \cdot x = \{g_1 \cdot x, \cdots, g_n \cdot x\}$. By Proposition 3.5, for all $i = 1, \cdots, n$, we have $\pi_x^{-1}(g_i \cdot x) = g_i\,\mathrm{Stab}_G(x)$, which is a finite set. Considering fibres of the surjective orbit map $\pi_x : G \twoheadrightarrow G \cdot x$, we have

$$G = \pi_x^{-1}(g_1 \cdot x) \cup \cdots \cup \pi_x^{-1}(g_n \cdot x).$$

This is a finite union of finite sets and is therefore finite. □

Theorem 3.7 (Orbit-Stabiliser)**.** Let G be a finite group acting on a finite set X. Then for all $x \in X$, we have

$$|G \cdot x| \,|\, |\mathrm{Stab}_G(x)| = |G|.$$

Proof. Let $n = |G \cdot x|$ and $G \cdot x = \{g_1 \cdot x, \cdots, g_n \cdot x\}$. By Proposition 3.5,

$$|G| = \sum_{i=1}^{n} |\pi_x^{-1}(g_i \cdot x)| = n|\,\mathrm{Stab}_G(x)| = |G \cdot x| \,|\, |\mathrm{Stab}_G(x)|.$$ □

Proposition 3.8. Let K/F be a finite extension. Then $G := \mathrm{Gal}(K/F)$ is finite.

Proof. Let $\{\alpha_1, \cdots, \alpha_n\}$ be a basis for K as an F-vector space. Each α_i is algebraic over F by Lemma 2.4. Let $m_i := m_{F,\alpha_i}$ be the minimal polynomial of α_i over F. Let $V(m_i) := \{\beta \in K : m_i(\beta) = 0\}$ be the set of zeroes of m_i in K: note that this is always a *finite set*.

By Lemma 3.3, G acts on $V(m_i)$ for each i. Using Example 3.2(2) repeatedly, we can now define an action of G on the product set $X = V(m_1) \times \cdots \times V(m_n)$ by

$$\sigma \cdot (\beta_1, \ldots, \beta_n) := (\sigma(\beta_1), \cdots, \sigma(\beta_n))$$

for all $\sigma \in G$ and $(\beta_1, \cdots, \beta_n) \in X$. We claim that

$$\mathrm{Stab}_G((\alpha_1, \cdots, \alpha_n)) = \{1\}.$$

Indeed, suppose that $\sigma \in G$ fixes each α_i. Then since σ is an F-linear automorphism of K and since $\{\alpha_1, \cdots, \alpha_n\}$ is an F-vector space basis for K, we see that σ fixes every other element of K. But then σ must be the identity map $1 : K \to K$. Since $V(m_1) \times \cdots \times V(m_n)$ is finite, Corollary 3.6 implies that G is finite. □

It would be nicer if K was a simple extension of the form $K = F(z)$:

Lemma 3.9. If $z \in K$ has $\mathrm{Stab}_G(z) = \{1\}$, then $|G| \leqslant [F(z) : F]$.

Proof. The group G acts on $V(m_{F,z}) := \{\beta \in K : m_{F,z}(\beta) = 0\}$ by Lemma 3.3. Now $|V(m_{F,z})| \leqslant \deg m_{F,z}(t) = [F(z) : F]$ by Corollary 2.11. On the other hand, Theorem 3.7 shows that $|G| = |G \cdot z| \, |\mathrm{Stab}_G(z)| = |G \cdot z|$ since $\mathrm{Stab}_G(z) = \{1\}$. Therefore $|G| = |G \cdot z| \leqslant |V(m_{F,z})| \leqslant [F(z) : F]$. □

This motivates trying to find some $z \in K$ with trivial stabiliser.

Proposition 3.10. Suppose that F is infinite. Let $K_1, \cdots, K_m$ be finitely many *proper* subfields of K containing F. Then

$$K_1 \cup \cdots \cup K_m < K.$$

Proof. Suppose for a contradiction that $K = K_1 \cup \cdots \cup K_m$. We can assume that $m \geq 2$, and that m is minimal with this property. Choose and fix some $y \in K \backslash K_1$. We will now show that $K_1 \subseteq K_2 \cup \cdots \cup K_m$. This implies that $K = K_2 \cup \cdots \cup K_m$, which contradicts the minimality of m.

Let $x \in K_1$. Since F is infinite, we can choose a subset $S \subset F$ of size $m + 1$. For each $\alpha \in S$, we can find some $i(\alpha) \in \{1, \cdots, m\}$ such that $x + \alpha y \in K_{i(\alpha)}$, because $K = K_1 \cup \cdots \cup K_m$. The function $i : S \to \{1, \cdots, m\}$ cannot be injective. So we can find $\alpha \neq \beta$ in S such that $x + \alpha y$ and $x + \beta y$ both lie in $K_{i(\alpha)}$. But then $y = \frac{(x+\alpha y)-(x+\beta y)}{\alpha-\beta} \in K_{i(\alpha)}$. Since $y \notin K_1$ by assumption, we conclude that $i(\alpha) > 1$. Then $x = (x + \alpha y) - \alpha y \in K_{i(\alpha)} \subseteq K_2 \cup \cdots \cup K_m$ for every $x \in K_1$. □

Of course the proof Proposition 3.10 fails when F is finite.

Corollary 3.11. Let K/F be a finite extension. Then $\mathrm{Stab}_G(z) = \{1\}$ for at least one $z \in K$.

Proof. By Proposition 3.8, G is finite. Suppose first that F is infinite. Write $G\backslash\{1\} := \{g_1, \cdots, g_m\}$. Since each g_i is non-trivial, each fixed field $K^{\langle g_i \rangle}$ is a *proper* subfield of K containing F. Since F is infinite, we can find some $z \in$

$K \setminus \left(K^{\langle g_1 \rangle} \cup \cdots \cup K^{\langle g_m \rangle}\right)$ by Proposition 3.10. Clearly z is not fixed by any g_i. So, the only element of G fixing z is 1.

We leave the case where F is finite as an exercise. □

Theorem 3.12. Let K/F be a finite extension. Then $|G| \leqslant [K : F]$.

Proof. Choose $z \in K$ with $\mathrm{Stab}_G(z) = \{1\}$ using Corollary 3.11. Then Lemma 3.9 implies that $|G| \leqslant [F(z) : F] \leqslant [K : F]$. □

4. Galois extensions

We fix a ground field F throughout §4. The definition of *Galois extensions* involves a discussion of *splitting fields* and *separability*.

Definition 4.1. Let F be a field and let $f \in F[t]$. A field extension K of F is said to be a *splitting field* of f if

(a) f splits completely in $K[t]$, and
(b) K is generated as a field by F together with the roots of f.

Lemma 4.2. Let K/F be a field extension and let $\alpha_1, \cdots, \alpha_n \in K$ be algebraic over F. Then $[F(\alpha_1, \cdots, \alpha_n) : F] < \infty$.

Proof. Proceed by induction on n. When $n = 1$, this follows from Corollary 2.11. Assume $n \geq 2$ and let $L := F(\alpha_1, \cdots, \alpha_{n-1})$; then $[L : F] < \infty$ by induction. Since α_n is algebraic over F, it is also algebraic over L. Hence Theorem 2.13 implies that

$$[F(\alpha_1, \cdots, \alpha_n) : F] = [L(\alpha_n) : F] = [L(\alpha_n) : L]\,[L : F] < \infty. \qquad \square$$

Corollary 4.3. Let $f \in F[t]$ and let K be a splitting field of f. Then $[K : F] < \infty$.

Proof. $K = F(\alpha_1, \cdots, \alpha_n)$ where $\alpha_1, \cdots, \alpha_n$ are the roots of f in K. Now apply Lemma 4.2. □

Lemma 4.4. Let $g \in F[t]$ be irreducible. Then there exists a simple extension $L = F(\alpha)$ generated by a root α of g.

Proof. Since g is an irreducible polynomial in the principal ideal domain $F[t]$, it generates a maximal ideal $\langle g \rangle$ in $F[t]$. Hence $L := F[t]/\langle g \rangle$ is a field, containing a copy of F, $\alpha := t + \langle g \rangle \in L$ is a root of g in L. Since α generates L as a ring together with F, we see that $L = F[\alpha]$. Since α is algebraic over F, we deduce that $F(\alpha) = F[\alpha] = L$ by Lemma 2.7. □

This basic construction is called *adjoining a root of an irreducible polynomial*.

Corollary 4.5. Let $f \in F[t]$. Then there exists a splitting field K of f.

Proof. Proceed by induction on the degree d of f, the case $d = 1$ being clear. Let g be an irreducible factor of f. Using Lemma 4.4, we can adjoin a root α of g to form the field extension $L := F(\alpha)$. Since $g \mid f$, we see that $f(\alpha) = 0$, so $(t - \alpha) \mid f$. Let $h = f/(t - \alpha) \in L[t]$. Since $\deg h < d$, by induction we can find a splitting field K of h. Since $\alpha \in L \subset K$, $f = (t - \alpha) \cdot h$ splits completely in $K[t]$. Since the roots of f in K generate K together with F, we see that K is also a splitting field of f. □

Example 4.6. Let $f = x^3 - 2$ and $F = \mathbb{Q}$. Adjoin a root α of f to $\mathbb{Q}$ to form $\mathbb{Q}(\alpha)$; then $f = (x - \alpha)(x^2 + \alpha x + \alpha^2 x)$ but the quadratic does not split over $\mathbb{Q}(\alpha)$ (exercise). Hence $x^2 + \alpha x + \alpha^2$ is irreducible over $\mathbb{Q}(\alpha)$, and we can adjoin a root β of this quadratic to form $K = \mathbb{Q}(\alpha)(\beta)$. If γ is the other root, then $\gamma = -\alpha - \beta$ already lies in K, so K is the splitting field of f. Then by Corollary 2.11 we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(x^3 - 2) = 3$ and $[K : \mathbb{Q}(\alpha)] = \deg(x^2 + \alpha x + \alpha^2) = 2$, so

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \times 3 = 6$$

by the Tower Law, Theorem 2.13.

You will see other interesting examples of splitting fields on Problem Sheet 1. We now turn to the more subtle notion of *separability*.

Definition 4.7. Let $f = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0 \in F[t]$.

(a) The *formal derivative* of f is

$$D(f) := n a_n t^{n-1} + (n-1) a_{n-1} t^{n-2} + \cdots + a_1 \in F[t].$$

(b) Suppose that f is irreducible. Then f is *separable* if $D(f) \neq 0$.

(c) We say that f is *separable* if each of its irreducible factors in $F[t]$ is separable.

Definition 4.8. We say that the finite extension K/F is *Galois* if it is the splitting field of some separable polynomial in $F[t]$.

Remark 4.9. Suppose that F is a **field of characteristic zero**. Then *every* polynomial $f \in F[t]$ is separable.

Lemma 4.10. Let $f \in F[t]$ be a separable irreducible polynomial. Then there exist $p, q \in F[t]$ such that $pf + qD(f) = 1$.

Proof. Since f is separable, $D(f)$ is a non-zero polynomial of strictly smaller degree than f. Since f is irreducible, the ideal $\langle f \rangle$ of the principal ideal domain $F[t]$ is maximal. Hence either $\langle f, D(f) \rangle = \langle f \rangle$, or $\langle f, D(f) \rangle = \langle 1 \rangle$. In the first case, $D(f) \in \langle f \rangle$, so there exists $g \in F[t]$ such that $fg = D(f)$. Since $D(f)$ is non-zero by assumption and since $F[t]$ is a domain, g must also be nonzero. Hence $D(f)$ has a non-zero term of degree $\geq \deg f$, which is impossible. So in fact $\langle f, D(f) \rangle = \langle 1 \rangle$ and we can find p and q in $F[t]$ such that $pf + qD(f) = 1$ as claimed. □

Proposition 4.11. Let $f \in F[t]$ be a separable irreducible polynomial, and let K be any field extension of F over which f splits completely. Then f has exactly $\deg f$ distinct roots in K.

Proof. By Lemma 4.10, there exist $p, q \in F[t]$ such that $pf + qD(f) = 1$. Suppose that α is a repeated root of f in K. Then $f = (t-\alpha)^2 g$ for some $g \in K[t]$ and hence $D(f) = 2(t-\alpha)g + (t-\alpha)^2 D(g)$, so $f(\alpha) = D(f)(\alpha) = 0$. Substituting $t = \alpha$ into $pf + qD(f) = 1$ then gives $0 = 1$, a contradiction. □

You will see an example of an inseparable polynomial over a field of positive characteristic in the first Problem Sheet.

We now start working towards showing that Galois extensions have a sufficiently large Galois group.

Lemma 4.12. Let $\varphi : F \to \tilde{F}$ be an isomorphism and let K/F and $\tilde{K}/\tilde{F}$ be finite extensions. Let $\alpha \in K$ and $\tilde{\alpha} \in \tilde{K}$, and suppose that $\varphi(m_{F,\alpha})(\tilde{\alpha}) = 0$. Then there is a unique extension $\tilde{\varphi} : F(\alpha) \to \tilde{F}(\tilde{\alpha})$ of $\varphi : F \to \tilde{F}$ such that $\tilde{\varphi}(\alpha) = \tilde{\alpha}$:

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & \tilde{F} \\ \big| & & \big| \\ F(\alpha) & \xrightarrow[\tilde{\varphi}]{} & \tilde{F}(\tilde{\alpha}). \end{array}$$

Proof. Let $g = m_{F,\alpha}$, an irreducible polynomial over F by Corollary 2.8. Since $\varphi(g)(\tilde{\alpha}) = 0$, Corollary 2.3 implies that $m_{\tilde{F},\tilde{\alpha}}$ divides $\tilde{g} := \varphi(g)$. But $\tilde{g}$ is irreducible over $\tilde{F}$, so in fact $\tilde{g} = m_{\tilde{F},\tilde{\alpha}}$. Applying Lemma 2.5 and Lemma 2.7 twice gives us isomorphisms

$$\theta : F[t]/\langle g \rangle \xrightarrow{\cong} F(\alpha) \quad \text{and} \quad \tilde{\theta} : \tilde{F}[t]/\langle \tilde{g} \rangle \xrightarrow{\cong} \tilde{F}(\tilde{\alpha}).$$

The isomorphism $\varphi : F \to \tilde{F}$ extends to an isomorphism $\varphi : F[t] \to \tilde{F}[t]$ which sends t to t. It sends the ideal $\langle g \rangle$ onto $\langle \tilde{g} \rangle$, and hence descends to give an isomorphism

$$\overline{\varphi} : F[t]/\langle g \rangle \xrightarrow{\cong} \tilde{F}[t]/\langle \tilde{g} \rangle.$$

These fit into the following diagram of fields and ring homomorphisms:

$$\begin{array}{ccccccc} & & F & \xrightarrow{\varphi} & \tilde{F} & & \\ & \swarrow & \big| & & \big| & \searrow & \\ K & - & F(\alpha) & \xrightarrow[\tilde{\varphi}]{} & \tilde{F}(\tilde{\alpha}) & - & \tilde{K} \\ & & \theta \uparrow \cong & & \cong \uparrow \tilde{\theta} & & \\ & & \frac{F[t]}{\langle g \rangle} & \xrightarrow[\overline{\varphi}]{\cong} & \frac{\tilde{F}[t]}{\langle \tilde{g} \rangle} & & \end{array}$$

Then $\tilde{\varphi} := \tilde{\theta} \circ \overline{\varphi} \circ \theta^{-1} : F(\alpha) \to \tilde{F}(\tilde{\alpha})$ is the required isomorphism.

If $\psi : F(\alpha) \to \tilde{F}(\tilde{\alpha})$ is another extension of φ such that $\psi(\alpha) = \tilde{\alpha}$, then ψ agrees with $\tilde{\varphi}$ on F and α. Since these generate $F(\alpha)$ as a ring by Lemma 2.7, $\psi = \tilde{\varphi}$. $\square$

We now use the separability assumption to prove that the Galois group of a Galois extension is sufficiently large.

Theorem 4.13. Let $\varphi : F \to \tilde{F}$ be an isomorphism. Suppose that K is a splitting field of the separable polynomial $f \in F[t]$, and let $\tilde{K}$ be a splitting field of $\tilde{f} := \varphi(f) \in \tilde{F}[t]$. Then there are at least $[K : F]$ distinct isomorphisms $K \to \tilde{K}$ extending φ.

Proof. We proceed by induction on $[K : F]$, the case $[K : F] = 1$ being clear.

Let g be a monic irreducible factor of f in $F[t]$ with $\deg g \geq 2$; then g is separable by Definition 4.7(c). Since φ is an isomorphism, $\tilde{g} := \varphi(g) \in \tilde{F}[t]$ is also separable. Since $\tilde{K}$ is a splitting field of $\tilde{f}$ and $\tilde{g} \mid \tilde{f}$, $\tilde{g}$ has exactly $\boxed{n := \deg \tilde{g}}$ distinct roots $\beta_1, \cdots, \beta_n \in \tilde{K}$, say, by Proposition 4.11.

Choose a root $\alpha \in K$ of g. Since $g(\alpha) = 0$ and since g is monic and irreducible over F, Corollary 2.3 implies that $m_{F,\alpha} = g$. Fix $i = 1, \cdots, n$. Then $\varphi(m_{F,\alpha})(\beta_i) = \varphi(g)(\beta_i) = \tilde{g}(\beta_i) = 0$, so Lemma 4.12 gives us an isomorphism $\varphi_i : F(\alpha) \to \tilde{F}(\beta_i)$ which extends $\varphi : F \to \tilde{F}$ and which sends α to β_i.

Since $\boxed{m := [K : F(\alpha)]} < [K : F]$, we can apply induction to the field extensions $K/F(\alpha)$ and $\tilde{K}/\tilde{F}(\beta_i)$ and the isomorphism $\varphi_i : F(\alpha) \to \tilde{F}(\beta_i)$ to find at least m different extensions $\varphi_i^{(j)} : K \to \tilde{K}$, $j = 1, \cdots, m$, of $\varphi_i : F(\alpha) \to \tilde{F}(\beta_i)$. Suppose that $\varphi_i^{(j)} = \varphi_{i'}^{(j')}$ for some $1 \leqslant i, i' \leqslant n$ and $1 \leqslant j, j' \leqslant m$. Then $\beta_i = \varphi_i^{(j)}(\alpha) = \varphi_{i'}^{(j')}(\alpha) = \beta_{i'}$ so $i = i'$, and then by induction we have $j = j'$. Thus we have constructed at least nm different extensions of $\varphi : F \xrightarrow{\cong} \tilde{F}$ to $K \to \tilde{K}$.

$$\begin{array}{ccccc} F & \text{———} & F(\alpha) & \text{———} & K \\ {\scriptstyle\varphi}\downarrow & & {\scriptstyle\varphi_i}\downarrow & & \vdots\,{\scriptstyle\varphi_i^{(j)}} \\ \tilde{F} & \text{———} & \tilde{F}(\beta_i) & \text{———} & \tilde{K} \end{array}$$

Finally, using Corollary 2.11 we have $[F(\alpha) : F] = \deg m_{F,\alpha} = \deg g = \deg \tilde{g} = n$. Applying Theorem 2.13, we find $[K : F] = [K : F(\alpha)][F(\alpha) : F] = mn$. $\square$

Corollary 4.14. Let K/F be a Galois extension. Then

$$|\operatorname{Gal}(K/F)| \geq [K : F].$$

Proof. Since K/F is Galois, we may assume that K is a splitting field of some separable polynomial $f \in F[t]$. Take $\tilde{F} := F$, let $\varphi : F \to F$ be the identity map and let $\tilde{K} = K$. Then Theorem 4.13 implies that there are at least $[K : F]$ distinct automorphisms of K extending $1 : F \to F$. $\square$

Corollary 4.15. Let $f \in F[t]$ be a separable polynonomial, and let K be a splitting field for f. Suppose that L is another extension of F such that f splits completely in $L[t]$. Then

(a) there exists at least one monomorphism $K \hookrightarrow L$,
(b) if L is also a splitting field of f, then this monomorphism is an isomorphism,
(c) any two splitting fields of f are (non-canonically!) isomorphic.

Proof. (a) Let $\tilde{K}$ be the subfield of L generated by F together with the roots of f. Then by Theorem 4.13 we can find at least one isomorphism $\varphi : K \to \tilde{K}$ extending the identity map on F. If $i : \tilde{K} \hookrightarrow L$ is the inclusion, then $i \circ \varphi : K \to L$ is the required monomorphism.

(b) In this case, $\tilde{K} = L$. The image of $i \circ \varphi$ equals $\tilde{K}$, so it is an isomorphism.

(c) Follows from (b). □

Example 4.16. Let $F = \mathbb{Q}$ and let K be the splitting field of $f = x^3 - 2$. As we saw in Example 4.6, $K = \mathbb{Q}(\alpha)(\beta)$ where α is a root of $x^3 - 2$ and β is a root of $x^2 + \alpha x + \alpha^2$. The three distinct roots of f in K are α, β and $\gamma := -\alpha - \beta$.

For each $\delta \in \{\alpha, \beta, \gamma\}$, by Lemma 4.12 we have an extension $\varphi_\delta : \mathbb{Q}(\alpha) \to \mathbb{Q}(\delta)$ of the identity map $1_\mathbb{Q} : \mathbb{Q} \to \mathbb{Q}$ that sends α to δ. Then φ_α has two extensions $\varphi_\alpha^{(1)}, \varphi_\alpha^{(2)}$ to an automorphism of K, characterised by $\varphi_\alpha^{(1)}(\beta) = \beta$ and $\varphi_\alpha^{(2)}(\beta) = \gamma$. Now φ_β sends $m_{\mathbb{Q}(\alpha),\beta} = t^2 + \alpha t + \alpha^2$ to $t^2 + \beta t + \beta^2 \in \mathbb{Q}(\beta)[t]$, which factorises as $(t-\alpha)(t-\gamma)$ over K. Hence there are two extensions $\varphi_\beta^{(1)}, \varphi_\beta^{(2)}$ of φ_β, characterised by $\varphi_\beta^{(1)}(\beta) = \alpha$ and $\varphi_\beta^{(2)}(\beta) = \gamma$. Similarly, there are two extensions $\varphi_\gamma^{(1)}, \varphi_\gamma^{(2)}$ of $\varphi_\gamma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\gamma)$, characterised by $\varphi_\gamma^{(1)}(\beta) = \alpha$ and $\varphi_\gamma^{(2)}(\beta) = \beta$.

Using Corollary 4.14 and Theorem 3.12, we conclude that

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\varphi_\alpha^{(1)}, \varphi_\alpha^{(2)}, \varphi_\beta^{(1)}, \varphi_\beta^{(2)}, \varphi_\gamma^{(1)}, \varphi_\gamma^{(2)}\}$$

where the effect of these automorphisms on $V(f) = \{\alpha, \beta, \gamma\}$ is given as follows:

	$\varphi_\alpha^{(1)}$	$\varphi_\alpha^{(2)}$	$\varphi_\beta^{(1)}$	$\varphi_\beta^{(2)}$	$\varphi_\gamma^{(1)}$	$\varphi_\gamma^{(2)}$
α	α	α	β	β	γ	γ
β	β	γ	α	γ	α	β
γ	γ	β	γ	α	β	α

Because all possible permutations of $\{\alpha, \beta, \gamma\}$ occur, this Galois group has to be isomorphic to S_3.

We can now give a characterisation of Galois extensions. For the next four statements **we assume that K/F is a finite extension and that $G = \mathrm{Gal}(K/F)$.**

Theorem 4.17. If K is Galois over F then $|G| = [K : F]$.

Proof. Combine Corollary 4.14 with Theorem 3.12. □

Lemma 4.18. $\mathrm{Gal}(K/K^G) = G$.

Proof. This is a tautology, but an important one. We know that K^G is a subfield of K containing F. Hence every K^G-linear automorphism of K is also F-linear. On the other hand, if $\sigma : K \to K$ is F-linear, then $\sigma \in G$, so σ fixes K^G pointwise, so σ is also K^G-linear. □

Theorem 4.19. If $|G| = [K : F]$, then $F = K^G$.

Proof. By Lemma 4.18, we know that $G = \mathrm{Gal}(K/K^G)$. Applying Theorem 3.12 to the field extension K/K^G then shows that

$$|G| \leqslant [K : K^G].$$

Theorem 2.13 implies that $[K : K^G] \leqslant [K : F]$. Since $[K : F] = |G|$ by assumption, we get $[K : K^G] = [K : F]$. So $[K^G : F] = 1$ and $K^G = F$ as claimed. □

The following general Lemma will be useful.

Lemma 4.20. Let H be a finite group of automorphisms of a field L, let $X \subseteq L$ be a finite subset and define

$$f_X := \prod_{y \in X} (t - y) \in L[t]$$

(a) If X is H-stable, then f_X in fact has coefficients in L^H.
(b) f_X is always separable.

Proof. (a) The H-action on L extends to a coefficient-wise H-action on $L[t]$ by ring automorphisms, fixing t. Because X is H-stable, the set of linear polynomials $\{t - x : x \in X\}$ is H-stable. Since the H-action respects the multiplication in $L[t]$, we see that the product f_X of these linear polynomials is fixed by H:

$$f_X \in L[t]^H = L^H[t].$$

(b) Any factor g of f_X in $L[t]$ has the form f_Y for some subset Y of X, so we may assume without loss of generality that $Y = X$. We use the product rule:

$$D(f_X) = \sum_{y \in X} \prod_{z \in X \setminus \{y\}} (t - z).$$

Choose some $u \in X$; if $y \neq u$ then $\prod_{z \in X \setminus \{y\}} (u - z) = 0$ since the product includes the factor $u - z$ with $z = u$. Hence

$$D(f_X)(u) = \prod_{z \in X \setminus \{u\}} (u - z) \neq 0.$$

Hence f_X is separable. □

Theorem 4.21. If $F = K^G$, then K/F is Galois.

Proof. Let $\{z_1, \cdots, z_n\}$ be an F-basis for K. Since G is finite by Proposition 3.8, the set $X := \bigcup_{i=1}^{n} G \cdot z_i$ is also finite as well as G-stable. Then f_X is a separable polynomial with coefficients in K^G, by Lemma 4.20. Since $K^G = F$, we see that $f_X \in F[t]$. Since f_X splits completely over K and since K is generated by the roots of f_X in K, it is the splitting field of f_X over F. □

Combining Theorems 4.17, 4.19 and 4.21, we have proved the following

Corollary 4.22. Let K/F be a finite extension and let $G = \mathrm{Gal}(K/F)$. Then the following are equivalent:

(a) K/F is Galois (i.e. the splitting field of a separable polynomial in $F[t]$),
(b) $|G| = [K : F]$,
(c) $F = K^G$.

5. The Main Theorem of Galois Theory

We are now one technical Lemma away from the proof of Theorem 1.11.

Lemma 5.1. Let K/F be a Galois extension and let $F \subseteq L \subseteq K$ be an intermediate field. Then K/L is also Galois.

Proof. Since K/F is a Galois extension, it is a splitting field of some separable polynomial $f \in F[t]$. Since the roots of f in K still generate K as a field, we just need to show that f is separable when viewed as an element of $L[t]$. By Remark 4.9 this is clear when $\mathrm{char}\, F = 0$; we leave the general case as an exercise. □

Note that the extension L/F is *not* Galois in general, even when F has characteristic zero! We restate Theorem 1.11 here for the reader's convenience.

Theorem 5.2 (Main Theorem of Galois Theory 1)**.** Let K/F be a Galois extension and let $F \subseteq L \subseteq K$ be an intermediate field. Then

$$L = K^{\mathrm{Gal}(K/L)}.$$

Proof. The extension K/L is Galois by Lemma 5.1. Then $L = K^{\mathrm{Gal}(K/L)}$ by Corollary 4.22(a) ⇒ (c). □

Next, we will prove Theorem 1.13, but first we need an important

Proposition 5.3. Let K be a field, let H be a finite group of automorphisms of K and let $z \in K$. Then:

(a) z is algebraic over K^H,
(b) $m_{K^H,z} = f_{H\cdot z} = \prod_{y \in H\cdot z} (t - y)$,
(c) $\deg m_{K^H,z} = |H \cdot z|$.

Proof. (a) By Lemma 4.20, the polynomial $f_{H\cdot z}$ has coefficients in K^H. Since $f_{H\cdot z}(z) = 0$, z is algebraic over K^H.

(b) Since $f_{H\cdot z}(z) = 0$, Corollary 2.3 implies that $m_{K^H,z}$ divides $f_{H\cdot z}$.

On the other hand, $H \leqslant \mathrm{Gal}(K/K^H)$, so H acts on the roots of $m_{K^H,z}$ in K by Lemma 3.3. Since z is a root of $m_{K^H,z}$ in K, it follows that the entire H-orbit $H \cdot z$ is contained in the set of roots of $m_{K^H,z}$. Hence $f_{H\cdot z}$ divides $m_{K^H,z}$.

Since both $f_{H\cdot z}$ and $m_{K^H,z}$ are monic, we must have equality.

(c) This is now immediate from (b). □

Theorem 5.4 (Main Theorem of Galois Theory 2)**.** Let K/F be a Galois extension and let $H \leqslant \mathrm{Gal}(K/F)$. Then $\mathrm{Gal}(K/K^H) = H$.

Proof. Let $J := \mathrm{Gal}(K/K^H)$ — this is a finite group by Proposition 3.8 and $H \leqslant J$. Choose $z \in K$ such that $\mathrm{Stab}_J(z) = \{1\}$ using Corollary 3.11. Then applying Theorem 3.7 and Proposition 5.3 to H and J in turn, we deduce that

$$|H| = |H \cdot z| = \deg m_{K^H,z} \quad \text{and} \quad |J| = |J \cdot z| = \deg m_{K^J,z}.$$

Hence it is enough to show that $K^J = K^H$. However, since K/F is a Galois extension, the extension K/K^H is also Galois with Galois group $\mathrm{Gal}(K/K^H) = J$ by Lemma 5.1. Hence Corollary 4.22(a) ⇒ (c) implies that $K^J = K^H$. □

We will now describe the Galois correspondence in one particular example. The difficult bit is actually computing the Galois group!

Lemma 5.5. Let $F = \mathbb{Q}$ and let $f := t^4 - a$ for some positive square-free integer a. Let K be a splitting field of f and let $G = \mathrm{Gal}(K/F)$. Then

$$G \cong D_8,$$

the dihedral group of order 8.

Proof. Let $\xi := \sqrt[4]{a} \in \mathbb{R} \subset \mathbb{C}$. Then f factors over $\mathbb{C}$ as

$$f = (t - \xi)(t + \xi)(t - i\xi)(t + i\xi).$$

Using Corollary 4.15(c), we may assume that $K = \mathbb{Q}(\xi, i)$. We first calculate its degree. Pick a prime p dividing a; then by Eisenstein's criterion at p together with Gauss's Lemma, f is irreducible over $\mathbb{Q}$. Hence

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$$

by Corollary 2.11. Since $\mathbb{Q}(\xi)$ is wholly contained in $\mathbb{R}$, we know that $\boxed{i \notin \mathbb{Q}(\xi)}$. Hence $t^2 + 1$ is irreducible over $\mathbb{Q}(\xi)$, so applying Corollary 2.11 again gives

$$[K : \mathbb{Q}(\xi)] = 2.$$

Using Theorem 2.13 we now see that $[K : \mathbb{Q}] = 8$. Writing $G = \mathrm{Gal}(K/F)$, we then know by Theorem 4.17 that G is a group of order 8.

Using Lemma 4.12 applied to $\mathbb{Q}(\xi) \subset K = \mathbb{Q}(\xi)(i)$, there is a $\mathbb{Q}(\xi)$-linear automorphism $\tau : K \to K$ such that

$$\tau(i) = -i \quad \text{and} \quad \tau(\xi) = \xi.$$

Of course, τ is the restriction to K of complex conjugation $\mathbb{C} \to \mathbb{C}$. Note that $K = \mathbb{Q}(i)(\xi)$ with $\boxed{[K : \mathbb{Q}(i)] = \dfrac{[K : \mathbb{Q}]}{[\mathbb{Q}(i) : \mathbb{Q}]} = 4}$ by Theorem 2.13. Hence by Corollary 2.11, $\deg m_{\mathbb{Q}(i),\xi} = 4$ so $t^4 - a$ remains irreducible over $\mathbb{Q}(i)$. Lemma 4.12, applied to $\mathbb{Q}(i) \subset K$, gives a $\mathbb{Q}(i)$-linear automorphism $\sigma : K \to K$ such that

$$\sigma(\xi) = i\xi \quad \text{and} \quad \sigma(i) = i.$$

Next, we compute the relations that σ and τ satisfy in G. Clearly

$$\sigma^4 = \tau^2 = 1$$

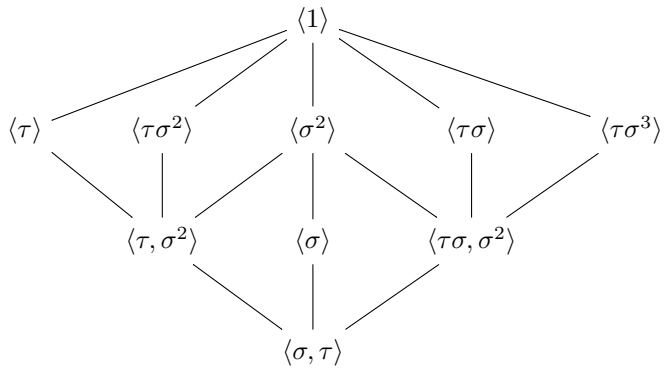
and $\sigma^2 \neq 1$ because $\sigma^2(\xi) = \sigma(i\xi) = i(i\xi) = -\xi \neq \xi$. So, σ has order 4 and τ has order 2. Next, $\tau\sigma\tau^{-1}(i) = -\tau\sigma(i) = -\tau(i) = i$ shows that $\tau\sigma\tau^{-1}$ fixes i, whereas $\tau\sigma\tau^{-1}(\xi) = \tau\sigma(\xi) = \tau(i\xi) = \tau(i)\tau(\xi) = -i\xi = i^3\xi = \sigma^{-1}(\xi)$. Hence

$$\tau\sigma\tau^{-1} = \sigma^{-1}.$$

Since $|G| = 8$, we conclude that $D_8 \to G$, $r \mapsto \sigma$ and $s \mapsto \tau$ is an isomorphism. $\square$

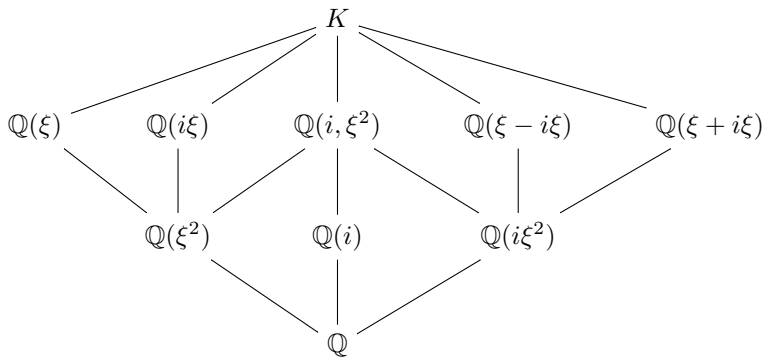
The next purely group-theoretical result is standard.

Lemma 5.6. The subgroups of $D_8 = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1} \rangle$ are:



Keep the notation of Lemma 5.5.

Corollary 5.7. The subfields of $K = \mathbb{Q}(\xi, i)$ are as follows:



Proof. It is routine to verify that the given generators *are* invariant under the appropriate subgroups of G. To see that they *do* generate the required fixed subfield, it's enough to compute the degree of K over the candidate subfield.

For example, in the case where $H = \langle \tau\sigma \rangle$, the element $\alpha := \xi - i\xi$ satisfies $\alpha^2 = \xi^2(1-i)^2 = -2i\xi^2$, so $\alpha^4 = -4a$ whence $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leqslant 4$. On the other hand, $i \notin \mathbb{Q}(\alpha)$ as otherwise $\xi = \frac{\alpha + \alpha i}{2}$ would lie in $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, i)$, leading to $K = \mathbb{Q}(\alpha)$ having degree $\leqslant 4$ over $\mathbb{Q}$. Hence $[K : \mathbb{Q}(\alpha)] = 2$. Therefore $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{[K:\mathbb{Q}]}{[K:\mathbb{Q}(\alpha)]} = 4$ by Theorem 2.13. □

We now work towards understanding the intermediate fields corresponding to the *normal* subgroups of G.

Lemma 5.8. Let K/F be a Galois extension and let L be an intermediate field. Suppose that L is $\mathrm{Gal}(K/F)$-stable. Then the restriction map

$$r : \mathrm{Gal}(K/F) \to \mathrm{Gal}(L/F)$$

is a well-defined surjective group homomorphism.

Proof. Let $\sigma \in \mathrm{Gal}(K/F)$; then $r(\sigma) = \sigma|_L : L \to K$ is only a well-defined element of $\mathrm{Gal}(L/F)$ because L is assumed to be $\mathrm{Gal}(K/F)$-stable. Hence r is well-defined, and it is clearly a group homomorphism. It is surjective by Theorem 4.13. □

Lemma 5.9. Let K/F be a Galois extension with $G = \mathrm{Gal}(K/F)$. Let L be an intermediate field. Then L/F is Galois if and only if L is G-stable.

Proof. Suppose that L/F is Galois. Then it is a splitting field of some separable polynomial $g \in F[t]$, so the roots $V(g)$ of g in L generate L. But $V(g)$ is G-stable by Lemma 3.3. Hence L is also G-stable.

Conversely, suppose that L is G-stable. By Theorem 4.21, it is enough to show that $L^{\mathrm{Gal}(L/F)} = F$. But $r(G) \leqslant \mathrm{Gal}(L/F)$ by Lemma 5.8, so $L^{\mathrm{Gal}(L/F)} \subseteq L^{r(G)} = L \cap K^G$. However $K^G = F$ by Corollary 4.22(a)⇒(c), so $L^{\mathrm{Gal}(L/F)} = F$. □

Lemma 5.10. Let K/F be a Galois extension with $G = \mathrm{Gal}(K/F)$ and let H be a subgroup of G. Then for all $\varphi \in G$, we have

$$K^{\varphi H \varphi^{-1}} = \varphi(K^H).$$

Proof. Let $x \in K$ and $\psi \in H$. Then $(\varphi\psi\varphi^{-1})\cdot x = x$ if and only if $\psi(\varphi^{-1}x) = \varphi^{-1}x$. So, $x \in K^{\varphi H \varphi^{-1}} \Leftrightarrow \varphi^{-1}(x) \in K^H \Leftrightarrow x \in \varphi(K^H)$. □

Theorem 5.11 (Main Theorem of Galois Theory 3)**.** Let K/F be a Galois extension with $G = \mathrm{Gal}(K/F)$ and let L be an intermediate subfield with $H := \mathrm{Gal}(K/L)$.

(1) H is normal in G if and only if L is Galois over F.
(2) If H is normal in G, the restriction map $\mathrm{Gal}(K/F) \to \mathrm{Gal}(L/F)$ induces a group isomorphism
$$G/H \cong \mathrm{Gal}(L/F).$$

Proof. (1) By Theorem 5.2 we have $L = K^H$. Now, H is normal in G if and only if $\varphi H \varphi^{-1} = H$ for all $\varphi \in G$. By Theorem 5.2 together with Theorem 5.4, this is equivalent to $K^H = K^{\varphi H \varphi^{-1}}$ for all $\varphi \in G$. Since $K^{\varphi H \varphi^{-1}} = \varphi(K^H)$ by Lemma 5.10, this is equivalent to K^H being G-stable. But Lemma 5.9 tells us that K^H is G-stable if and only if K^H/F is Galois.

(2) Suppose H is normal in G. Then L is Galois over F by (1), so L is G-stable by Lemma 5.9. Hence $r : G \to \mathrm{Gal}(L/F)$ is a well-defined surjective group homomorphism by Lemma 5.8. Its kernel is $\ker(r) = \{\varphi \in G : \varphi|_L = 1_L\} = \mathrm{Gal}(K/L) = H$. Now apply the First Isomorphism Theorem. □

In summary, the Main Theorem of Galois Theory can be stated as follows:

Corollary 5.12. Let K/F be a Galois extension with $G = \mathrm{Gal}(K/F)$.

(1) The function $L \mapsto \mathrm{Gal}(K/L)$ is a *bijection*
$$\left\{ \begin{array}{c} \text{intermediate fields} \\ F \subseteq L \subseteq K \end{array} \right\} \xrightarrow{\cong} \left\{ \begin{array}{c} \text{subgroups} \\ H \leqslant \mathrm{Gal}(K/F) \end{array} \right\}$$
with inverse $H \mapsto K^H$.
(2) Intermediate subfields $F \subseteq L \subseteq K$ that are Galois over F correspond precisely with the normal subgroups H of G; for any such L we have
$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/L).$$
(3) The correspondences are *inclusion reversing*:
- $F \subseteq L_1 \subseteq L_2 \subseteq K$ implies that $\mathrm{Gal}(K/L_2) \leqslant \mathrm{Gal}(K/L_1)$, and
- $H_1 \leqslant H_2 \leqslant G$ implies that $K^{H_2} \leqslant K^{H_1}$.

(4) For each intermediate field L with $H = \mathrm{Gal}(K/L)$, we have
$$[L : F] = [G : H] \quad \text{and} \quad [K : L] = |H|.$$

Proof. (1) follows from Theorem 5.2 and Theorem 5.4. (2) is Theorem 5.11. (3) is clear. (4) Theorem 4.17 tells us that $[K : F] = |G|$ and $[K : L] = |H|$, whereas $[L : F] = \frac{[K:F]}{[K:L]} = \frac{|G|}{|H|} = [G : H]$ by Theorem 2.13. □

6. Solvability by radicals

Definition 6.1. Let K/F be a finite extension. We say that K/F is *radical* if there exists a chain of intermediate subfields

$$F = F_0 \subset F_1 \subset \cdots \subset F_n = K, \tag{6.1}$$

such that for each $i = 1, \cdots, n$, there exist $\alpha_i \in F_i$ and positive integers d_i with

$$F_i = F_{i-1}(\alpha_i) \quad \text{and} \quad \alpha_i^{d_i} \in F_{i-1} \quad \text{for all} \quad i = 1, \cdots, n.$$

In this language, when F is a subfield of $\mathbb{C}$ and $\alpha \in \mathbb{C}$ is algebraic over F, α is solvable by radicals over F in the sense of Definition 1.3 if and only if α lies in some radical extension K over F.

Theorem 6.2. Let F be a field of characteristic zero and let α be algebraic over F. Then the following are equivalent:

(1) α lies in a radical extension of F,
(2) the Galois group $\mathrm{Gal}_F(m_{F,\alpha})$ is a solvable group.

Note that this immediately implies Theorem 1.15.

6.1. Solvable polynomials have solvable Galois groups.

We begin by looking at two special classes of field extensions. First, a *cyclotomic* extension:

Lemma 6.3. Let p be a prime number. Suppose that L is a field extension of F such that $L = F(\varepsilon)$ for some $\varepsilon \in L$ with $\varepsilon^p = 1$. Then L is a Galois extension of F and $\mathrm{Gal}(L/F)$ is abelian.

Proof. If $\varepsilon = 1$ then $L = F$ and the result is trivially true, so assume that $\varepsilon \neq 1$. Since p is prime, ε generates a cyclic group of order p in $L^\times$. Hence $t^p - 1$ splits completely in L as $\prod_{i=0}^{p-1}(t - \varepsilon^i)$. So L is the splitting field of $t^p - 1$ over F. Since $t^p - 1$ has no repeated roots, it is separable by Lemma 4.20(b). Hence L/F is Galois.

Let $\sigma \in G = \mathrm{Gal}(L/F)$. Then $\sigma(\varepsilon)^p = \sigma(1) = 1$, so $\sigma(\varepsilon) \in \{1, \varepsilon, \cdots, \varepsilon^{p-1}\}$. Say $\sigma(\varepsilon) = \varepsilon^{\chi(\sigma)}$ for some $\chi(\sigma) \in \{0, 1, \cdots, p-1\}$. Now for $\sigma, \tau \in G$ we have

$$\sigma\tau(\varepsilon) = \sigma(\varepsilon^{\chi(\tau)}) = (\varepsilon^{\chi(\sigma)})^{\chi(\tau)} = \varepsilon^{\chi(\sigma)\chi(\tau)}$$

which proves that $\chi(\sigma\tau) \equiv \chi(\sigma)\chi(\tau) \mod p$. Hence $\chi(\sigma\tau) = \chi(\tau\sigma)$ so that $\sigma(\tau(\varepsilon)) = \tau(\sigma(\varepsilon))$. Since ε generates L together with F, $\sigma\tau = \tau\sigma$. □

Now we look at *Kummer extensions*:

Lemma 6.4. Let p be a prime number. Suppose that the field L contains an element ε such that $\varepsilon^p = 1$ but $\varepsilon \neq 1$. Let $a \in L$ and suppose that $M = L(\alpha)$ where $\alpha^p = a$. Then M/L is a Galois extension, and $\mathrm{Gal}(M/L)$ is abelian.

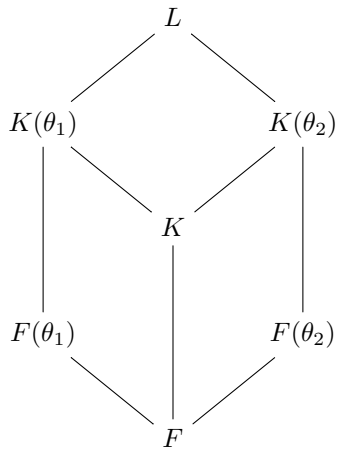
Proof. Because $\varepsilon \neq 1$ and p is prime, ε generates a cyclic group of order p in $L^\times$. Hence $t^p - a = \prod_{i=0}^{p-1} (t - \varepsilon^i \alpha)$ splits completely in M. We may assume that $a \neq 0$; then $t^p - a$ has distinct roots, so it is separable by Lemma 4.20(b). Its roots generate M, because α is a root and $M = L(\alpha)$. Hence M is Galois over L. Now if $\sigma \in \mathrm{Gal}(M/L)$ then $\sigma(\alpha)^p = a$ forces $\sigma(\alpha) = \varepsilon^{\psi(\sigma)}\alpha$ for some $\psi(\sigma) \in \{0, 1, \cdots, p-1\}$. For any other $\tau \in \mathrm{Gal}(M/L)$ we have $\sigma(\tau(\alpha)) = \sigma(\varepsilon^{\psi(\tau)}\alpha) = \varepsilon^{\psi(\sigma)+\psi(\tau)}\alpha = \tau(\sigma(\alpha))$ because both σ and τ are L-linear. Hence $\sigma\tau = \tau\sigma$ and $\mathrm{Gal}(M/L)$ is abelian. □

Definition 6.5. A finite field extension K/F is said to be *normal* if whenever $g \in F[t]$ is an irreducible polynomial such that g has a root in K, g splits completely in $K[t]$.

According to Ian Stewart, this is a trade-union definition: *one out — all out!*

Theorem 6.6. Let K/F be a Galois extension. Then K/F is normal.

Proof. Choose a separable $f \in F[t]$ such that K is a splitting field of f. View fg as an element of $K[t]$ and use Corollary 4.5 to find a splitting field L of fg containing K. Suppose that θ_1 and θ_2 are zeroes of g in L, and consider the following diagram:



Applying Theorem 2.13 several times, we have for $i = 1$ or $i = 2$

$$[K(\theta_i) : K][K : F] = [K(\theta_i) : F] = [K(\theta_i) : F(\theta_i)][F(\theta_i) : F].$$

Since g is irreducible, $g = m_{F,\theta_1} = m_{F,\theta_2}$, so by Lemma 2.6 and Lemma 2.7,

$$[F(\theta_1) : F] = \deg g = [F(\theta_2) : F].$$

By Lemma 4.12, we can find an F-linear isomorphism $\varphi : F(\theta_1) \xrightarrow{\cong} F(\theta_2)$ sending θ_1 to θ_2. On the other hand, $K(\theta_i)$ is a splitting field for f over $F(\theta_i)$ for $i = 1, 2$,

and f is separable over $F(\theta_i)$ by Problem Sheet 2, Question 5. So, we can use Theorem 4.13 to extend φ to an isomorphism of fields $K(\theta_1) \xrightarrow{\cong} K(\theta_2)$. Therefore

$$[K(\theta_1) : F(\theta_1)] = [K(\theta_2) : F(\theta_2)].$$

We can now conclude that

$$[K(\theta_1) : K] = \frac{[K(\theta_1) : F(\theta_1)][F(\theta_1) : F]}{[K : F]} = \frac{[K(\theta_2) : F(\theta_2)][F(\theta_2) : F]}{[K : F]} = [K(\theta_2) : K].$$

So if θ_1 is a root of g which lies in K, then $[K(\theta_2) : K] = [K(\theta_1) : K] = 1$ for any other root θ_2 of g in L. Hence all roots of g in L in fact lie in K. Hence $L = K$ and g splits completely over K. □

Corollary 6.7. Let K/F be a finite Galois extension and let $\alpha \in K$. Then

(a) $m_{F,\alpha}$ is separable, and
(b) there is a surjective group homomorphism $\mathrm{Gal}(K/F) \twoheadrightarrow \mathrm{Gal}_F(m_{F,\alpha})$.

Proof. (a) By Corollary 2.8, $m_{F,\alpha}$ is irreducible over F and has a zero in K. Therefore it splits completely over K by Theorem 6.6. Hence K contains a splitting field L of $m_{F,\alpha}$. Using Corollary 4.22 and Proposition 5.3(b), we have $m_{F,\alpha} = m_{K^G,\alpha} = f_{G\cdot\alpha}$, which is separable by Proposition 4.20(b).

(b) We know now that L/F is a Galois extension with $\mathrm{Gal}_F(m_{F,\alpha}) = \mathrm{Gal}(L/F)$. The result now follows from Theorem 5.11. □

Theorem 6.8. Let K/F be a radical Galois extension. Then $\mathrm{Gal}(K/F)$ is solvable.

Proof. We proceed by induction on $[K : F]$. Since K/F is radical, there is some $\alpha \in K\backslash F$ and $d \geq 2$ such that $\alpha^d \in F$. Choose the pair (α, d) so that d is smallest possible. If d is not prime then $d = mn$ with $1 < m, n < d$. Now $\alpha^m \notin F$ since $m < d$. But then $(\alpha^m)^n \in F$ contradicts the minimality of d. So, $d = p$ is prime.

Since $\alpha \notin F$ we have $\deg m_{F,\alpha} \geq 2$. The irreducible polynomial $m_{F,\alpha}$ splits completely in K by Theorem 6.6, since K/F is Galois. By Corollary 6.7(a), $m_{F,\alpha}$ is separable. Using Proposition 4.11, we see that K contains some $\beta \neq \alpha$ with $m_{F,\alpha}(\beta) = 0$. Let $a := \alpha^p \in F$; then $m_{F,\alpha} \mid t^p - a$ by Corollary 2.3, so β is a root of $t^p - a$ as well. Thus, $\alpha^p = \beta^p = a$.

Let $\varepsilon := \alpha/\beta \in K$ and let $L := F(\varepsilon)$. Then $\varepsilon^p = 1$, so L/F is Galois with $\mathrm{Gal}(L/F)$ abelian by Lemma 6.3. Note that we cannot apply the induction hypothesis immediately to K/L at this point of the proof, because it could be the case that $\varepsilon \in F$ and $L = F$. So, we work with a larger extension of L.

Let $M := L(\alpha) = F(\varepsilon, \alpha)$. The polynomial $t^p - a \in F[t]$ splits completely in $M[t]$, and has no repeated roots, hence it is separable by Lemma 4.20(b). So, M is a Galois extension of F. Also, $\mathrm{Gal}(M/L)$ is abelian by Lemma 6.4. Since $\alpha \in M\backslash F$, we have $[M : F] > 1$, so by Theorem 2.13, $[K : M] < [K : F]$. Since K/F is a radical Galois extension, so is K/M. Hence by induction, $\mathrm{Gal}(K/M)$ is solvable.

Using Theorem 5.11, we conclude that $G = \mathrm{Gal}(K/F)$ contains normal subgroups $H_1 = \mathrm{Gal}(K/L) \supseteq H_2 = \mathrm{Gal}(K/M)$ such that H_2 and $H_1/H_2 \cong \mathrm{Gal}(M/L)$ and $G/H_1 \cong \mathrm{Gal}(L/F)$ are all solvable. Hence G is also solvable. □

Proposition 6.9. Let K/F be a finite radical extension, where F **is a field of characteristic zero**. Then there exists a finite *Galois* radical extension M/F such that $K \subseteq M$.

Proof. Proceed by induction on the length r of a radical chain

$$F = F_0 \subset F_1 \subset \cdots \subset F_{r-1} \subset F_r = K,$$

the base case $r = 0$ being trivial. Since F_{r-1}/F is radical, by induction we can find a radical Galois extension L of F containing F_{r-1}. Write $F_r = F_{r-1}(\alpha)$ where $\alpha^d = \theta$ for some $\theta \in F_{r-1}$.

Let $G = \mathrm{Gal}(L/F)$. By Lemma 4.20(a), the polynomial

$$f_{G\cdot\theta} = \prod_{\psi \in G\cdot\theta} (t - \psi) \in L[t]$$

actually has coefficients in L^G, which equals F by Corollary 4.22. Therefore

$$g(t) := f_{G\cdot\theta}(t^d)$$

also lies in $F[t]$. Using Corollary 4.5, choose a splitting field M of g containing L:

$$\begin{array}{ccccc} F & \longrightarrow & F_{r-1} & \longrightarrow & L \\ & & \downarrow & & \downarrow \\ & & F_r = F_{r-1}(\alpha) & \cdots\cdots\succ & M \end{array}$$

Now, M is generated as an extension of L by the roots of $t^d - \psi$, for each $\psi \in G \cdot \theta$. Hence M/L is radical. Since L/F is radical by induction, so is M/F. Since L/F is Galois, it is a splitting field of some $h \in F[t]$; then since $hg \in F[t]$ and M is generated by the roots of hg together with F, it is also a splitting field of hg over F. Since we're assuming that F has characteristic zero, hg is a separable polynomial by Remark 4.9. Hence M/F is a radical and Galois extension. It remains to show that we can find an embedding $F_r \hookrightarrow M$ making the above diagram commutative.

Since $\alpha^d = \theta$, we see that $m_{F_{r-1},\alpha} \mid t^d - \theta$ in $F_{r-1}[t]$. On the other hand, $t^d - \theta$ divides g in $L[t]$, so we can find some $q \in L[t]$ such that $g = m_{F_{r-1},\alpha} q$. Since g splits completely in $M[t]$, we can then find some $\beta \in M$ such that $m_{F_{r-1},\alpha}(\beta) = 0$. Using Lemma 4.12, we can then find a monomorphism $F_r = F_{r-1}(\alpha) \hookrightarrow F_{r-1}(\beta) \subseteq M$ sending α to β. □

Note that Proposition 6.9 fails in positive characteristic: this follows from the existence of inseparable polynomials over certain fields of positive characteristic, together with the fact that Galois extensions are separable — see Problem Sheet 3 Question 5. We can now prove the (1) ⇒ (2) direction of Theorem 6.2.

Theorem 6.10. Let F be a field of characteristic zero and let α be algebraic over F. Suppose that α lies in a radical extension K of F. Then the Galois group $\mathrm{Gal}_F(m_{F,\alpha})$ is solvable.

Proof. Using Proposition 6.9, we may enlarge K if necessary and thereby assume that K/F is Galois over F. Then $G := \mathrm{Gal}(K/F)$ is a solvable group by Theorem 6.8. Now $\mathrm{Gal}_F(m_{F,\alpha})$ is a homomorphic image of G by Corollary 6.7 and is therefore also solvable. □

Lemma 6.11. Let $f \in F[t]$ have n distinct roots in a splitting field K. Then $G = \mathrm{Gal}(K/F)$ is naturally isomorphic to a subgroup of S_n.

Proof. Consider the action of G on $V(f) = \{\alpha_1, \cdots, \alpha_n\}$ from Lemma 3.3. It gives rise to an associated permutation representation

$$\rho : G \to \mathrm{Sym}(V(f)) \cong S_n.$$

This map must be injective, because if $\rho(\sigma) = 1$ for some $\sigma \in G$, then σ fixes $V(f)$ pointwise, but $V(f)$ generates K as a field together with F, so σ fixes all elements of K and hence $\sigma = 1$. Hence $G \cong \rho(G) \leqslant S_n$. □

We will frequently **identify** G with its image in $S_n \cong \mathrm{Sym}(V(f))$. We can now give an actual example of a polynomial which is not solvable by radicals.

Theorem 6.12. The polynomial $f := t^5 - 6t + 3 \in \mathbb{Q}[t]$ is not solvable by radicals.

Proof. By Eisenstein's Criterion at $p = 3$ together with Gauss's Lemma, f is irreducible over $\mathbb{Q}$. It is separable by Remark 4.9, so it has 5 distinct roots in a splitting field K by Proposition 4.11. Since $\mathbb{C}$ is algebraically closed, we will identify K with a subfield of $\mathbb{C}$, and using Lemma 6.11, we will identify $G = \mathrm{Gal}_{\mathbb{Q}}(f) = \mathrm{Gal}(K/\mathbb{Q})$ with a subgroup of S_5.

We have $f(-2) = -17 < 0$, $f(0) = 3 > 0$, $f(1) = -2 < 0$ and $f(2) = 23 > 0$. Hence f has a real root in $(-2, 0)$, $(0, 1)$ and $(1, 2)$. Suppose f has five real roots. Then by the Mean Value Theorem, $f' = 5t^4 - 6$ would have at least four real roots, which is visibly not the case. Hence f has precisely three real roots. Hence complex conjugation $c : \mathbb{C} \to \mathbb{C}$ preserves K, so $c|_K \in G$ and $c|_K$ is a transposition: c fixes the three real roots and swaps the two non-real roots of f.

Now $[\mathbb{Q}(z) : \mathbb{Q}] = 5$ for any $z \in V(f)$, as f is irreducible over $\mathbb{Q}$. Hence 5 divides $[K : \mathbb{Q}]$ by Theorem 2.13, which is equal to $|G|$ by Theorem 4.17. By Cauchy's Theorem, G contains an element σ of order 5. Then σ is necessarily a 5-cycle. Since S_5 is generated by a transposition and a 5-cycle (see Problem Sheet 3), we conclude that $G = S_5$. □

6.2. **Polynomials with solvable Galois groups are solvable by radicals.**

Proposition 6.13. Let K/F be a Galois extension with $[K : F] = p$ where p is a prime number. Suppose for some $1 \neq \varepsilon \in F$ we have $\varepsilon^p = 1$. Then there exists $u \in K$ such that $u^p \in F$ and $K = F(u)$.

Proof. Let $G = \mathrm{Gal}(K/F)$. Since K/F is Galois, we have $|G| = [K : F] = p$ by Theorem 4.17. Hence $G = \langle\sigma\rangle$ is a cyclic group of order p. Now $\sigma : K \to K$ is an F-linear map satisfying $\sigma^p = 1$. The minimal polynomial of this linear map divides $t^p - 1 = \prod_{i=0}^{p-1}(t - \varepsilon^i)$ and therefore it splits completely over F. Hence by the Primary Decomposition Theorem from Linear Algebra, σ is diagonalisable. Since $\sigma \neq 1$, some eigenvalue of σ is a non-trivial p-th root of unity. Without loss of generality, we can assume that ε is an eigenvalue of σ.

Let $u \in K$ be a corresponding eigenvector so that $\sigma(u) = \varepsilon u$. Since σ is also a ring homomorphism, we have

$$\sigma(u^p) = \sigma(u)^p = (\varepsilon u)^p = \varepsilon^p u^p = u^p.$$

Hence $u^p \in K^G$ which is equal to F by Corollary 4.22. Since $\sigma(u) \neq u$, we know that $u \notin F$ and hence $[F(u) : F] > 1$. But this divides $[K : F] = p$ by Theorem 2.13, so since p is prime, we conclude that $[F(u) : F] = p$ and hence $K = F(u)$. □

We can now prove the (2) ⇒ (1) direction of Theorem 6.2.

Theorem 6.14. Let F be a field of characteristic zero and let α be algebraic over F. Suppose that the Galois group $\mathrm{Gal}_F(m_{F,\alpha})$ is solvable. Then α lies in a radical extension of F.

Proof. Let K/F be a splitting field of $m_{F,\alpha}$; proceed by induction on $[K : F]$. Suppose that $G := \mathrm{Gal}_F(m_{F,\alpha}) = \mathrm{Gal}(K/F)$ is solvable. Then we can find a normal subgroup H of G such that $p := [G : H]$ is prime. Let $L = K^H$ be the corresponding intermediate subfield. Let M be a splitting field of $(t^p - 1)m_{F,\alpha}$ containing K; since $\mathrm{char}\, F = 0$, M is Galois over F by Remark 4.9. Let $\varepsilon \in M$ be a root of $t^p - 1$ such that $\varepsilon \neq 1$, which exists by Proposition 4.11; then $M = K(\varepsilon)$.

Since $K(\varepsilon)$ is then also Galois over $L(\varepsilon)$ by Lemma 5.1, Corollary 6.7 tells us that there is a surjective group homomorphism

$$\mathrm{Gal}(K(\varepsilon)/L(\varepsilon)) \twoheadrightarrow \mathrm{Gal}_{L(\varepsilon)}(m_{L(\varepsilon),\alpha}).$$

Next, since K is also Galois over L by Lemma 5.1, the subfield K of $K(\varepsilon)$ is $\mathrm{Gal}(K(\varepsilon)/L)$-stable by Lemma 5.9. This gives us a well-defined restriction map

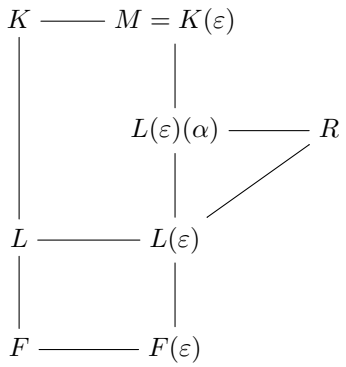
$$\mathrm{Gal}(K(\varepsilon)/L(\varepsilon)) \hookrightarrow \mathrm{Gal}(K(\varepsilon)/L) \to \mathrm{Gal}(K/L).$$

This restriction map is injective, because an $L(\varepsilon)$-linear automorphism of $K(\varepsilon)$ fixing K must fix all of $K(\varepsilon)$. Hence $\mathrm{Gal}(K(\varepsilon)/L(\varepsilon))$ is isomorphic to a subgroup

of $\mathrm{Gal}(K/L)$. Hence $\mathrm{Gal}_{L(\varepsilon)}(m_{L(\varepsilon),\alpha})$ is isomorphic to a subquotient of the finite solvable group $\mathrm{Gal}(K/F)$, and it is therefore solvable. Using Theorem 2.13 we have

$$|\operatorname{Gal}_{L(\varepsilon)}(m_{L(\varepsilon),\alpha})| \leqslant [K(\varepsilon) : L(\varepsilon)] \leqslant [K : L] = \frac{1}{p}[K : F].$$

Hence by induction we can find a radical extension R of $L(\varepsilon)$ containing α.



Consider the extension $L(\varepsilon)/F$. Since $L = K^H$ and H is normal in G, L is Galois over F by Theorem 5.11. Also, $F(\varepsilon)/F$ is Galois by Lemma 6.3. Let $\sigma \in \mathrm{Gal}(K(\varepsilon)/F)$; then σ preserves both L and $F(\varepsilon)$; hence it preserves $L(\varepsilon)$. Hence $L(\varepsilon)$ is Galois over F by Lemma 5.9. The restriction map

$$\mathrm{Gal}(L(\varepsilon)/F(\varepsilon)) \to \mathrm{Gal}(L/F)$$

is injective by similar reasoning to the above. By Theorem 4.17, $[L(\varepsilon) : F(\varepsilon)]$ divides $[L : F] = p$, so it is 1 or p. Hence $L(\varepsilon)/F(\varepsilon)$ is radical by Proposition 6.13, and $F(\varepsilon)/F$ is radical by definition. Thus R/F is also radical. □

6.3. **Determinant and discriminant.** Let $f \in F[t]$ be a polynomial of degree n and choose a splitting field K. Let $\{\alpha_1, \cdots, \alpha_n\}$ be the roots of f in K.

Definition 6.15. (a) The *determinant* of f is

$$\delta := \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i).$$

(b) The *discriminant* of f is

$$\Delta := \delta^2 = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i)^2.$$

We see that $\delta \neq 0$ if and only if $\Delta \neq 0$ if and only if the roots of f are pairwise distinct. Of course this is automatic whenever f is irreducible and separable.

Example 6.16. If $f = x^2 + bx + c = (x - \alpha_1)(x - \alpha_2)$, then

$$\delta^2 = b^2 - 4c.$$

Proof. We have $\alpha_1 + \alpha_2 = -b$ and $\alpha_1\alpha_2 = c$, so

$$(\alpha_2 - \alpha_1)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c. \qquad \square$$

We assume from now on that the roots of f are pairwise distinct. Recall that the *sign* of a permutation $\sigma \in S_n$ is 1 if σ is even, and -1 if σ is odd:

$$\operatorname{sgn} : S_n \to \{\pm 1\}, \quad \sigma \mapsto \begin{cases} 1 & \text{if} \quad \sigma \in A_n \\ -1 & \text{if} \quad \sigma \notin A_n. \end{cases}$$

Identify $G := \operatorname{Gal}(K/F)$ with a subgroup of S_n using Lemma 6.11.

Proposition 6.17. We have $g \cdot \delta = \operatorname{sgn}(g)\delta$ for all $g \in G$.

Proof. It is possible to do this directly. But a much better way is to consider the *Van der Monde matrix*

$$V := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \cdots & x_n^{n-1} \end{pmatrix}.$$

in n indeterminates $x_1, \cdots, x_n$. The symmetric group S_n acts on $\mathbb{Z}[x_1, \cdots, x_n]$ by permuting these variables. If we swap any two columns of this matrix, then the determinant changes sign:

$$\tau \cdot \det V = \det(\tau \cdot V) = -\det V \quad \text{for any transposition} \quad \tau \in S_n.$$

Since the transpositions generate S_n, we see that

$$\sigma \cdot \det V = \operatorname{sgn}(\sigma) \det V \quad \text{for all} \quad \sigma \in S_n.$$

For a fixed pair $1 \leqslant i < j \leqslant n$, consider the substitution map

$$\Psi_{i,j} : \mathbb{Z}[x_1, \cdots, x_n] \to \mathbb{Z}[x_1, \cdots, x_n]$$

which sends x_j to x_i and sends x_k to x_k for all $k \neq j$. Then $\ker \Psi_{i,j} = \langle x_i - x_j \rangle$ and $\Psi_{i,j}(\det V) = 0$. Since the $\binom{n}{2}$ linear polynomials $\{x_j - x_i : 1 \leqslant i < j \leqslant n\}$ in $\mathbb{Z}[x_1, \cdots, x_n]$ are coprime and since this ring is a UFD, we deduce

$$\prod_{1 \leqslant i < j \leqslant n} (x_j - x_i) \quad | \quad \det V.$$

Both of these expressions are homogeneous polynomials of degree $1+2+\cdots+n-1 = \binom{n}{2}$, and the coefficient of $1 \cdot x_2 \cdot x_3^2 \cdot \cdots \cdot x_n^{n-1}$ in both is equal to 1. Hence

$$\det V = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i).$$

Evaluating x_i at $\alpha_i \in K$ then gives the result. $\square$

Corollary 6.18. Assume that $\operatorname{char} F \neq 2$ and that f has no repeated roots.

(a) $K^{G\cap A_n} = F(\delta)$.
(b) $G \leqslant A_n$ if and only if Δ is a square in F.

Proof. Proposition 6.17 tells us that $\delta \in K^{A_n\cap G}$, and also that $\Delta = \delta^2 \in K^G = F$, using Corollary 4.22. Hence we have inclusions of fields

$$F \subseteq F(\delta) \subseteq K^{A_n\cap G}.$$

If $G \leqslant A_n$ then $K^{A_n\cap G} = K^G = F$, so these are equalities. Then $\delta \in F$ and $\Delta = \delta^2$ is a square in F. If, on the other hand, $G \not\subseteq A_n$ then we can find some odd permutation $\tau \in G$. Then $\tau \cdot \delta = -\delta$. But since f has no repeated roots, $\delta \neq 0$, and since $\operatorname{char} F \neq 2$, $-\delta \neq \delta$. Hence $\delta \notin F$. Now, Corollary 5.12(4) implies that

$$[K^{A_n\cap G} : F] = [G : A_n \cap G] = [GA_n : A_n]$$

which is equal to 2 since $A_n < GA_n \leqslant S_n$ forces $GA_n = S_n$. Hence in this case we have $K^{A_n\cap G} = F(\delta)$ and this field has degree 2 over F. □

6.4. **Cubic equations.** Let F be a field with $\operatorname{char} F \neq 3$, and let

$$f := t^3 + pt + q \in F[t]$$

be an **irreducible** cubic. The assumption that $\operatorname{char} F \neq 3$ guarantees that f is separable, because $D(f) = 3t^2 + p$ cannot then be the zero polynomial. We will now follow the proof of Theorem 6.14 to see how to solve the cubic equation $f = 0$ by radicals, and in particular, we see where the substitution $t = z - \frac{p}{3z}$ from §1.2 came from. The key is to study carefully the proof of Proposition 6.13.

Let K/F be a splitting field of f and let $V(f) = \{\alpha_1, \alpha_2, \alpha_3\}$ be the three roots of f in K. We **identify** $G = \operatorname{Gal}(K/F) = \operatorname{Gal}_F(f)$ with a subgroup of $\operatorname{Sym}(V(f)) \cong S_3$ using Lemma 6.11.

Lemma 6.19. Assume that $\operatorname{char}(F) \neq 2, 3$ and that f is irreducible.

(a) $G = A_3$ or $G = S_3$.
(b) If Δ is a square in F, then $G = A_3$. Otherwise, $G = S_3$.

Proof. (a) Since f is irreducible over F, Corollary 2.3 implies that $m_{F,\alpha_1} = f$, and hence $[F(\alpha_1) : F] = \deg m_{F,\alpha_1} = \deg f = 3$ by Corollary 2.11. Hence $[F(\alpha_1) : F]$ divides $[K : F]$ by Theorem 2.13, whereas $|G| = [K : F]$ by Theorem 4.17. Hence $3 \mid |G|$. The only subgroups of S_3 with this property are A_3 and S_3.

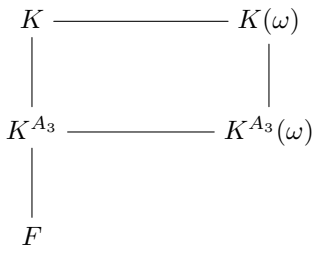
(b) Since $\operatorname{char}(F) \neq 2$, this follows from (a) together with Corollary 6.18(b). □

We deduce from Lemma 6.19 that $\sigma := (123) \in G$; thus $A_3 = \langle\sigma\rangle \leqslant G$. Then Theorem 5.4 tells us that K/K^{A_3} is a Galois extension with

$$\operatorname{Gal}(K/K^{A_3}) = A_3$$

which is a cyclic group of order 3. We would like to apply Proposition 6.13 to this extension, but unfortunately, it will not be true in general that K contains a

non-trivial third root ω of unity. Thus, we adjoin this root to K: we let ω be any zero of t^2+t+1 and form $K(\omega)$:



Lemma 6.20. (a) $K(\omega)$ is a Galois extension of F.
(b) $\mathrm{Gal}(K(\omega)/K^{A_3}(\omega))$ is isomorphic to A_3.

Proof. (a) By construction, $K(\omega)$ is a splitting field of $(t^2+t+1)\cdot f$. The polynomial t^2+t+1 is separable: for this we may assume it is irreducible and then $D(t^2+t+1) = 2t+1$ is not zero since its constant term 1 is non-zero. Hence $(t^2+t+1)\cdot f$ is also separable, and $K(\omega)$ is Galois over F.

(b) Since K is Galois over F, it is $\mathrm{Gal}(K(\omega)/F)$-stable by Proposition 5.9. Hence we have a restriction map $r : \mathrm{Gal}(K(\omega)/K^{A_3}(\omega)) \to \mathrm{Gal}(K/K^{A_3})$ which is injective. By Theorem 2.13 we see that $3 = [K : K^{A_3}]$ divides

$$[K(\omega) : K^{A_3}] = [K^{A_3}(\omega) : K^{A_3}] \cdot [K(\omega) : K^{A_3}(\omega)].$$

Since ω is a root of a quadratic polynomial, the first factor is either 1 or 2, so we must have $3 \mid [K(\omega) : K^{A_3}(\omega)]$. So, $\mathrm{Gal}(K(\omega)/K^{A_3}(\omega))$ is a subgroup of the cyclic group $\mathrm{Gal}(K/K^{A_3}) = A_3$ of order 3, of order dividing 3. This forces the restriction map r to be an isomorphism. □

So, there exists an extension $\sigma : K(\omega) \to K(\omega)$ of $\sigma : K \to K$ which fixes $K^{A_3}(\omega)$. We can now apply Proposition 6.13 to the cyclic cubic Galois extension

$$K(\omega)/K^{A_3}(\omega)$$

to find at least one element $u \in K(\omega)$ such that

$$K(\omega) = K^{A_3}(\omega)(u) \quad \text{and} \quad u^3 \in K^{A_3}(\omega).$$

The proof of Proposition 6.13 tells us to *look for σ-eigenvectors in $K(\omega)$*. Since σ permutes the roots $\alpha_1, \alpha_2, \alpha_3$ of f cyclically, we can use Linear Algebra to write down the following eigenvectors:

$$\boxed{u := \frac{\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3}{3} \quad \text{and} \quad v := \frac{\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3}{3}}$$

At this point, we know that u^3 and v^3 both lie in $K^{A_3}(\omega)$, by Proposition 6.13. But how do we 'compute' these quantities?

Lemma 6.21. Assume $\mathrm{char}(F) \neq 3$ and that $f = t^3 + pt + q \in F[t]$ is an irreducible cubic. Then

(a) $uv = -\frac{p}{3}$,
(b) $u^3v^3 = -\frac{p^3}{27}$,
(c) $u^3 + v^3 = -q$, and
(d) u^3, v^3 are roots of a quadratic polynomial with coefficients in F.

Proof. (a) Equating the coefficients in $t^3 + pt + q = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)$ we have

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = p, \quad \alpha_1\alpha_2\alpha_3 = -q.$$

Using the fact that $\omega + \omega^2 = -1$, we can expand uv as follows:

$$\begin{aligned} 9uv &= (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3) \\ &= \alpha_1^2 + \omega\alpha_1\alpha_2 + \omega^2\alpha_1\alpha_3 + \omega^2\alpha_1\alpha_2 + \alpha_2^2 + \omega\alpha_2\alpha_3 + \omega\alpha_1\alpha_3 + \omega^2\alpha_2\alpha_3 + \alpha_3^2 \\ &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_2\alpha_3 - \alpha_3\alpha_1 \\ &= (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) \\ &= -3p. \end{aligned}$$

Since $\mathrm{char}\, F \neq 3$, we get $uv = -\frac{p}{3}$ as claimed.

(b) This follows immediately from (a).

(c) We spot that $u^3 + v^3 = (u+v)(\omega u + \omega^2 v)(\omega^2 u + \omega v)$. Then

$$\begin{aligned} 3(u+v) &= 2\alpha_1 + (\omega + \omega^2)\alpha_2 + (\omega^2 + \omega)\alpha_3 = 3\alpha_1, \\ 3(\omega u + \omega^2 v) &= (\omega + \omega^2)\alpha_1 + (\omega^2 + \omega)\alpha_2 + 2\alpha_3 = 3\alpha_3, \\ 3(\omega^2 u + \omega v) &= (\omega^2 + \omega)\alpha_1 + 2\alpha_2 + (\omega + \omega^2)\alpha_3 = 3\alpha_2. \end{aligned}$$

Multiplying these together and cancelling 27, we obtain $u^3 + v^3 = \alpha_1\alpha_2\alpha_3 = -q$.

(d) This follows immediately from (b,c). □

It follows from Lemma 6.21 that u^3 and v^3 are roots of the quadratic equation

$$z^2 + qz - \frac{p^3}{27} = 0$$

that appeared in §1.2. Since $uv = -\frac{p}{3}$ by Lemma 6.21(a) and since $\alpha_1 = u + v$,

$$\alpha_1 = u - \frac{p}{3u}.$$

This explains the substitution $y = z - \frac{p}{3z}$ that we used there.

‘

6.5. **Quartic equations.** In §6.4, we performed a ‘Galois descent’ from a splitting field K of f to the ground field F using the normal series

$$\{1\} \lhd A_3 \lhd S_3.$$

Now suppose that f is an irreducible polynomial of degree 4 over F, K is a splitting field of f with Galois group $G = \mathrm{Gal}(K/F) = \mathrm{Gal}_F(f)$, which we identify with a subgroup of S_4 via the permutation representation $G \to \mathrm{Sym}(V(f)) \cong S_4$.

This time, we use the normal series

$$\{1\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4.$$

Let $H := G \cap V_4$, a normal subgroup of G. The extension K/K^H is then Galois with abelian Galois group isomorphic to H. According to general principles, certain F-linear combinations of the roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ will have squares lying in the fixed field K^H: they are

$$u_1 = \frac{1}{2}(\alpha_1+\alpha_2-\alpha_3-\alpha_4), \quad u_2 = \frac{1}{2}(\alpha_1-\alpha_2+\alpha_3-\alpha_4), \quad u_3 = \frac{1}{2}(\alpha_1-\alpha_2-\alpha_3+\alpha_4),$$

Note that $\{u_1, u_2, u_3\}$ is permuted by $\mathrm{Sym}(\{2,3,4\}) \cong S_3$. Since this group, together with V_4, generates all of S_4, it follows that $\{u_1^2, u_2^2, u_3^2\}$ is G-stable, and therefore *the cubic resolvent*

$$(t-u_1^2)(t-u_2^2)(t-u_3^2)$$

has coefficients in F by Lemma 4.20(a) and Corollary 4.22. Note that $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ lies in the F-linear span of u_1, u_2, u_3, because $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \in F$ is up to sign the coefficient of x^3 in f and hence lies in F, and because the matrix

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

is invertible. Therefore $K = K^H(u_1, u_2, u_3)$, which means that we can express the roots of f using linear combinations of the square roots of $u_1^2, u_2^2, u_3^2 \in K^H$, and of course these three elements can be written as radical expressions of elements in $F = K^G$ by solving the resolvent cubic as we did in §6.4.

Note, however, that there are other possibilities for the cubic resolvent: for example, one could instead choose

$$v_1 := \alpha_1\alpha_2 + \alpha_3\alpha_4, \quad v_2 := \alpha_1\alpha_3 + \alpha_2\alpha_4, \quad v_3 := \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

Then $\{v_1, v_2, v_3\}$ is a G-stable subset of K^H. Alternatively, one could take

$$w_1 := (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \quad w_2 := (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4), \quad w_3 := (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

and $\{w_1, w_2, w_3\}$ is again a G-stable subset of K^H.

7. Other topics

7.1. **Finite fields.**

Lemma 7.1. Let F be a finite field. Then $|F| = p^n$ for some prime p and some positive integer n.

Proof. Since F is finite, it must have positive characteristic. Since F is a field, this characteristic is a prime p. Hence F contains a copy of $\mathbb{F}_p$. Regard F as a vector space over $\mathbb{F}_p$. Since F is finite, it has finite dimension n, say. Then $|F| = p^n$. □

For a prime number p, we write $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. It is a field of order p.

Definition 7.2. Let F be a field of characteristic p. The *Frobenius endomorphism*

$$\phi : F \to F$$

is defined by $\phi(x) = x^p$ for all $x \in F$.

Lemma 7.3. Let F be a finite field of characteristic p. Then $\phi \in \mathrm{Gal}(F/\mathbb{F}_p)$.

Proof. The fact that ϕ is multiplicative is clear. Its additivity follows from the binomial theorem:

$$(x+y)^p = x^p + px^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{p-2}x^2y^{p-2} + pxy^{p-1} + y^p = x^p + y^p$$

because $p \mid \binom{p}{i}$ whenever $0 < i < p$. Therefore $\phi : F \to F$ is a ring homomorphism. Since F is a field, it must be injective. Since F is finite, it must also be surjective. Finally, F is $\mathbb{F}_p$-linear because $\phi(x) = x^p = x$ for all $x \in \mathbb{F}_p$ by Fermat's Little Theorem. Hence $\phi \in \mathrm{Gal}(F/\mathbb{F}_p)$. □

Theorem 7.4. Let p be a prime and let n be a positive integer.

(a) Any field of order p^n is a splitting field of $t^{p^n} - t$ over $\mathbb{F}_p$.

(b) Any splitting field of $t^{p^n} - t$ over $\mathbb{F}_p$ is a field of order p^n.

Proof. (a) Let F be a field of order p^n. It must contain $\mathbb{F}_p$. Then $x^{p^n-1} = 1$ for all $x \in F^\times$ by Lagrange's Theorem. Hence $x^{p^n} = x$ for all $x \in F$, so all elements of F are roots of $t^{p^n} - t$. Hence $t^{p^n} - t$ splits completely in $F[t]$, and its roots generate F. Hence F is a splitting field of $t^{p^n} - t$ over $\mathbb{F}_p$.

(b) Let F be a splitting field of $f = t^{p^n} - t$ containing $\mathbb{F}_p$. Suppose that α is a repeated root of f in F. Then $D(f)(\alpha) = 0$. But $D(f) = p^n t^{p^n-1} - 1 = -1$, a contradiction. Hence f has $\deg(f) = p^n$ distinct roots in F, so $|F| \geq p^n$.

Let V be the set of roots of f in F. Then $V = \{\alpha \in F : \alpha^{p^n} = \alpha\} = F^{\langle \phi^n \rangle}$. Hence V is a subfield of F. Since F is a splitting field of f by assumption, V generates F as a field, we must have $V = F$. Hence $|F| = |V| = p^n$. □

Corollary 7.5. (a) Up to isomorphism, there is a *unique* field $\mathbb{F}_{p^n}$ of order p^n.

(b) $\mathbb{F}_{p^n}$ is Galois over $\mathbb{F}_p$.

Proof. (a) Use Theorem 7.4 and Corollary 4.15(c).

(b) If g is an irreducible factor of $t^{p^n} - t$, then g has no repeated roots in any splitting field. So, g is separable by Lemma 4.20(b). By Theorem 7.4, $\mathbb{F}_{p^n}$ is a splitting field of the separable polynomial $t^{p^n} - t$, and is hence Galois over $\mathbb{F}_p$. □

We will now compute the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Proposition 7.6. Let p be a prime and let n be a positive integer.

(a) $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ has order n in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.
(b) $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi \rangle$ is a cyclic group of order n.

Proof. (a) Since $\alpha^{p^n} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$ by Lagrange, this means that $\phi^n = 1$. On the other hand, if $\phi^m = 1$ for some $1 \leqslant m \leqslant n$, then $\alpha^{p^m} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$. Then $t^{p^m} - t$ has $|\mathbb{F}_{p^n}| = p^n$ distinct roots in $\mathbb{F}_{p^n}$, forcing $p^m \geq p^n$. Hence $m \geq n$ and the order of ϕ is precisely n.

(b) Using Theorem 3.12, we have $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leqslant [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. But ϕ has order n, so we must have equality, and then ϕ must generate all of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. □

Corollary 7.7. Let a, b be positive integers. Then $\mathbb{F}_{p^a}$ embeds into $\mathbb{F}_{p^b}$ if and only if $a \mid b$.

Proof. ($\Rightarrow$). Suppose that $\mathbb{F}_{p^a}$ embeds into $\mathbb{F}_{p^b}$. Let $G = \mathrm{Gal}(\mathbb{F}_{p^b}/\mathbb{F}_p)$, a cyclic group of order b by Proposition 7.6(b). Let $H = \mathrm{Gal}(\mathbb{F}_{p^b}/\mathbb{F}_{p^a})$ be the subgroup of G corresponding to $\mathbb{F}_{p^a}$. Since G is abelian, H is normal and $G/H \cong \mathrm{Gal}(\mathbb{F}_{p^a}/\mathbb{F}_p)$ by Corollary 5.12(2). Applying Proposition 7.6(b) again, we see that G/H is a cyclic group of order a. Hence $a \mid b$ by Lagrange.

($\Leftarrow$). Suppose that $a \mid b$. Then $p^a - 1 \mid p^b - 1$, so $t^{p^a-1} - 1 \mid t^{p^b-1} - 1$, so $t^{p^a} - t \mid t^{p^b} - t$. Hence $t^{p^a} - t$ splits completely in $\mathbb{F}_{p^b}[t]$. Hence $\mathbb{F}_{p^a}$ embeds into $\mathbb{F}_{p^b}$ by Corollary 4.15(a). □

7.2. **Cyclotomic extensions.** We fix a positive integer n throughout.

Definition 7.8. Let K be a field. An element $\zeta \in K$ is said to be a *primitive* n^{th} *root of unity* if ζ has order precisely n in the multiplicative group $K^\times$.

For example, $\zeta = e^{\frac{2\pi i}{n}}$ is a primitive n^{th} root of unity in $\mathbb{C}$.

Lemma 7.9. Suppose K is a field admitting a primitive n^{th} root of unity.

(a) $\mu_n(K) := \{\zeta \in K : \zeta^n = 1\}$ is a cyclic group of order n.
(b) The primitive n^{th} roots of unity are precisely the generators of $\mu_n(K)$.

Note that the condition on K is far from vacuous. For example, if K is a field of characteristic p, then K can never contain any non-trivial p^{th} roots of unity, because $\zeta^p = 1$ implies $\zeta^p - 1 = (\zeta - 1)^p = 0$ and hence $\zeta = 1$. We now restrict to the case where $K = \mathbb{Q}$.

Definition 7.10. (a) The n^{th} *cyclotomic polynomial* is

$$\Phi_n := \prod_{\zeta \in \mu_n(\mathbb{C}) : o(\zeta) = n} (t - \zeta) \in \mathbb{C}[t],$$

the monic polynomial whose roots are all the primitive n^{th} roots of 1 in $\mathbb{C}$.
(b) Let $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$; $\mathbb{Q}(\zeta_n) \subset \mathbb{C}$ is called the n^{th} *cyclotomic extension* of $\mathbb{Q}$.

Note that $\deg \Phi_n = |(\mathbb{Z}/n\mathbb{Z})^\times| =: \phi(n)$, where ϕ is the *Euler ϕ-function*.

Lemma 7.11. $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$.

Proof. We have $\mu_n(\mathbb{C}) = \langle \zeta_n \rangle$. Then $\mathbb{Q}(\zeta_n)$ is the splitting field of $t^n - 1$ containing $\mathbb{Q}$. Hence it is a Galois extension of $\mathbb{Q}$. □

Example 7.12. We have $\Phi_1 = t - 1$, $\Phi_2 = t + 1$, $\Phi_3 = (t - \omega)(t - \omega^2) = t^2 + t + 1$, $\Phi_4 = (t - i)(t + i) = t^2 + 1$, $\Phi_5 = t^4 + t^3 + t^2 + t + 1$ and $\Phi_6 = (t - \zeta_6)(t - \zeta_6^{-1}) = t^2 - 2\cos\frac{2\pi}{6}\ t + 1 = t^2 - t + 1$.

Let $\Gamma_n := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$; our aim will be to compute this finite group.

Lemma 7.13. Γ_n acts faithfully on $\mu_n(\mathbb{C})$ by group automorphisms.

The element $\zeta_n = e^{\frac{2\pi i}{n}}$ gives rise to a group isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mu_n(\mathbb{C})$ given by $\overline{k} \mapsto \zeta_n^k$. Recall that

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times :$$

every automorphism of $\mathbb{Z}/n\mathbb{Z}$ is given by multiplication by unit in the ring $\mathbb{Z}/n\mathbb{Z}$. Hence we obtain a group homomorphism

$$\chi_n : \Gamma_n \to (\mathbb{Z}/n\mathbb{Z})^\times$$

which is determined by $\sigma(\zeta_n) = \zeta_n^{\chi_n(\sigma)}$ for all $\sigma \in \Gamma_n$.

Definition 7.14. χ_n is called the n^{th} *cyclotomic character*.

Corollary 7.15. Φ_n lies in $\mathbb{Q}[t]$.

Proof. Suppose that $o(\varepsilon) = n$ and $\sigma \in \Gamma_n$. Then $o(\sigma(\varepsilon)) = n$ as well. Therefore the set of primitive n^{th} roots of unity is Γ_n-stable, and σ permutes the linear factors of $\Phi_n(t)$ for all $\sigma \in \Gamma_n$. Hence $\Phi_n(t) \in \mathbb{Q}(\zeta_n)^{\Gamma_n}[t]$ by Lemma 4.20(a). This completes the proof because $\mathbb{Q}(\zeta_n)^{\Gamma_n} = \mathbb{Q}$ by Corollary 4.22. □

Lemma 7.16. We have $\prod_{d|n} \Phi_d = t^n - 1$.

Lemma 7.17. Suppose that $k = hf$ where $k, f \in \mathbb{Z}[t]$ are monic, and $h \in \mathbb{Q}[t]$. Then $h \in \mathbb{Z}[t]$ as well.

Proof. Write $h = a_0 + a_1 t + \cdots + a_{m-1}t^{m-1} + a_m t^m$, $f = b_0 + b_1 t + \cdots + b_{n-1}t^{n-1} + b_n t^n$ and $k = c_0 + c_1 t + \cdots + c_{m+n-1}t^{m+n-1} + c_{m+n}t^{m+n}$, where $a_0, \cdots, a_{m-1} \in \mathbb{Q}, b_0, \cdots b_{n-1} \in \mathbb{Z}$ and $c_0, c_1, \cdots, c_{n+m-1} \in \mathbb{Z}$. Then for $0 \leqslant j \leqslant m$ we have

$$c_{n+j} = a_j b_n + a_{j+1} b_{n-1} + \cdots + a_{m-1} b_{n+j+1-m} + a_m b_{n+j-m}.$$

Since h is monic, we have $a_m = 1$. Let $0 \leqslant j < m$, and assume inductively that $a_i \in \mathbb{Z}$ for $i > j$. Since f is monic, $b_n = 1$ so

$$a_j = c_{n+j} - a_{j+1} b_{n-1} - \cdots - a_{m-1} b_{n+j+1-m} - a_m b_{n+j-m} \in \mathbb{Z}.$$

This completes the induction and shows that $h \in \mathbb{Z}[t]$. □

Corollary 7.18. We have $\Phi_n \in \mathbb{Z}[t]$.

Proof. We proceed by induction on n. Let $k = t^n - 1 \in \mathbb{Z}[t]$, $h = \Phi_n \in \mathbb{Q}[t]$ and $f = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d$. By induction, $f \in \mathbb{Z}[t]$ and f is monic. Then $k = hf$ by Lemma 7.16, so Lemma 7.17 implies that $h = \Phi_n \in \mathbb{Z}[t]$. □

Theorem 7.19. The cyclotomic polynomial Φ_n is irreducible over $\mathbb{Q}$.

Proof. Suppose Φ_n is not irreducible over $\mathbb{Q}$. Then it is also not irreducible over $\mathbb{Z}$ by Gauss's Lemma. Write $\Phi_n = fg$ for some monic $f, g \in \mathbb{Z}[t]$ of degree ≥ 1; we may assume that f is irreducible over $\mathbb{Q}$ and that $f(\zeta_n) = 0$.

Let ε be a primitive n^{th}-root of 1 and let $p \nmid n$ be a prime; we will show that $f(\varepsilon^p) = 0$. Suppose for a contradiction that $f(\varepsilon^p) \neq 0$; then since ε^p is still a primitive n^{th} root of unity, we have $\Phi_n(\varepsilon^p) = 0$, so $g(\varepsilon^p) = 0$. Define

$$k(t) := g(t^p) \in \mathbb{Z}[t].$$

Then $k(\varepsilon) = g(\varepsilon^p) = 0$. Since f is irreducible over $\mathbb{Q}$, it is equal to $m_{\mathbb{Q},\zeta_n}$ and must hence divide k in $\mathbb{Q}[t]$, so $k = hf$ for some $h \in \mathbb{Q}[t]$. Since k and f are both monic, Lemma 7.17 implies that $h \in \mathbb{Z}[t]$. We can now reduce $k = hf$ modulo p to obtain

$$\overline{k}(t) = \overline{g(t^p)} = \overline{g(t)}^p, \quad \text{hence} \quad \overline{hf} = \overline{g}^p \quad \text{in} \quad \mathbb{F}_p[t].$$

Let $\overline{q}$ be any irreducible factor of $\overline{f}$ in $\mathbb{F}_p[t]$; then $\overline{q}$ divides $\overline{g}^p$ and therefore also $\overline{g}$. But then $\overline{q}^2 \mid \overline{f}\overline{g} = \overline{fg} = \overline{\Phi_n} \mid t^n - 1$. Hence q divides the formal derivative $D(t^n - 1) = nt^{n-1}$ as well as $t^n - 1$. Since $p \nmid n$, this implies that q divides 1. This contradiction shows that $f(\varepsilon^p) = 0$ after all.

Now, let r be a positive integer coprime to n. Write $r = p_1 \cdot \cdots \cdot p_s$ for some prime numbers $p_1, \cdots, p_s$, all coprime to n. As we saw above, $f(\zeta_n) = 0$ implies that $f(\zeta_n^{p_1}) = 0$. Since $\zeta_n^{p_1}$ is still a primitive n^{th} root of unity, we can apply the argument again to see that $f(\zeta_n^{p_1 p_2}) = 0$ as well. Continuing like this, we conclude that $f(\zeta_n^r) = f(\zeta_n^{p_1 \cdots \cdot p_s}) = 0$. Hence f vanishes at *all* primitive n^{th} roots of unity, so $\Phi_n \mid f$. This forces $\deg g = 0$, which is a contradiction. □

Corollary 7.20. The cyclotomic character

$$\chi_n : \Gamma_n = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

is an isomorphism.

Proof. If $\chi_n(\sigma) = 1$ then $\sigma(\zeta) = \zeta$, so $\sigma = 1$. Hence χ_n is injective. Now $|\Gamma_n| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ by Theorem 4.17, and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg m_{\mathbb{Q},\zeta_n}$ by Corollary 2.11. Finally, since Φ_n is monic and irreducible over $\mathbb{Q}$ by Theorem 7.19, and since $\Phi_n(\zeta) = 0$, we conclude that $m_{\mathbb{Q},\zeta_n} = \Phi_n$. Therefore

$$|\operatorname{Im} \chi_n| = |\Gamma_n| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg m_{\mathbb{Q},\zeta_n} = \deg \Phi_n = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

and we see that χ_n is surjective. Hence it is an isomorphism. □

A Galois extension $K/\mathbb{Q}$ is said to be *abelian* if $\mathrm{Gal}(K/\mathbb{Q})$ is an abelian group. We have now exhibited abelian Galois extensions with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$ for all positive integers n.

Theorem 7.21 (Kronecker-Weber)**.** Let $K/\mathbb{Q}$ be an abelian Galois extension. Then K embeds into $\mathbb{Q}(\zeta_n)$ for some positive integer n.