

# Part II – Galois Theory

Based on lectures by Dr C. Brookes

Notes taken by Bhavik Mehta

Michaelmas 2017

## Contents

<b>0</b>	<b>Introduction</b>	<b>2</b>
0.1	Course overview . . . . .	2
<b>1</b>	<b>Field Extensions</b>	<b>3</b>
1.1	Motivatory Example . . . . .	4
1.2	Review of GRM . . . . .	5
1.3	Digression on (Non-)Constructibility . . . . .	7
1.4	Return to theory development . . . . .	9
<b>2</b>	<b>Separable, normal and Galois extensions</b>	<b>14</b>
2.1	Trace and Norm . . . . .	19
2.2	Normal extensions . . . . .	21
<b>3</b>	<b>Fundamental Theorem of Galois Theory</b>	<b>24</b>
3.1	Artin's Theorem . . . . .	24
3.2	Galois groups of polynomials . . . . .	27
3.3	Galois Theory of Finite Fields . . . . .	30
<b>4</b>	<b>Cyclotomic and Kummer extensions</b>	<b>32</b>
4.1	Cyclotomic extensions . . . . .	32
4.2	Kummer Theory . . . . .	34
4.3	Cubics . . . . .	36
4.4	Quartics . . . . .	38
4.5	Solubility by radicals . . . . .	40
<b>5</b>	<b>Final Thoughts</b>	<b>45</b>
5.1	Algebraic closure . . . . .	45
5.2	Symmetric polynomials and invariant theory . . . . .	47
	<b>Index</b>	<b>49</b>

## 0 Introduction

The primary motivation of this course is to study the solutions of polynomial equations in one variable to wonder whether there is a formula involving roots, a solution by radicals. Quadratics were typically studied in school, while the solution in radicals for cubics and quartics has been known for a long time and studied in particular in 1770 by Lagrange.

In 1799, Ruffini claimed that there were some quintics that can't be solved by radicals, that is, there is no general formula, but it took until 1824 before Abel used existing ideas about permutations to produce the first accepted proof of insolubility, before dying in 1829. Galois' main contribution was in 1831, when he gave the first explanation as to why some polynomials are soluble by radicals and others are not. He made use of the group of permutations of the roots of a polynomial, and realised in particular the importance of *normal* subgroups.

Galois' work was not known generally in his lifetime - it was only published by Liouville in 1846, who realised that it tied in well with the work of Cauchy on permutations. Galois had submitted his work for various competitions and for entry into the Ecole Polytechnique in Paris. Unfortunately Galois died in a duel in 1832, leaving a six and a half page letter indicating his thoughts about the future development of his theory.

### 0.1 Course overview

Most of this course is Galois Theory, but presented in a more modern fashion - in terms of field extensions. Recall from GRM that if  $f(t)$  is an irreducible polynomial in  $k[t]$  where  $k$  is a field, then  $k[t]/(f(t))$  is a field, where  $(f(t))$  denotes the ideal of  $k[t]$  generated by  $f(t)$ , and this new field contains  $k$ . In this way, we can see the field  $k[t]/(f(t))$  as a field extension of  $k$ .

**Prerequisites** Quite a lot of the Groups, Rings and Modules course, but no modules except in one place where it's useful to know the structure of finite abelian groups. The DPMMS website has a Galois Theory page with a long history of example sheets and notes, in particular see Tony Scholl's 2013-4 course page.

# 1 Field Extensions

**Definition 1.1** (Field extension). A **field extension**  $K \leq L$  is the inclusion of a field  $K$  into another field  $L$  with the same 0, 1, and where the restriction of  $+$  and  $\cdot$  (in  $L$ ) to  $K$  gives the  $+$  and  $\cdot$  of  $K$ .

**Example.**

(i)  $\mathbb{Q} \leq \mathbb{R}$

(ii)  $\mathbb{R} \leq \mathbb{C}$

(iii)  $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) = \{ \lambda + \mu\sqrt{2} \mid \lambda, \mu \in \mathbb{Q} \}$

(iv)  $\{ \lambda + \mu i \mid \lambda, \mu \in \mathbb{Q} \} = \mathbb{Q}(i) \leq \mathbb{C}$

Suppose  $K \leq L$  is a **field extension**. Then  $L$  is a  $K$ -vector space using the addition from the field structure and scalar multiplication given by the multiplication in the field  $L$ .

**Definition 1.2** (Degree). The **degree** of  $L$  over  $K$  is  $\dim_K L$ , the  $K$ -vector space dimension of  $L$ . This may not be finite. We typically denote this by  $|L : K|$ . If  $|L : K| < \infty$ , then the extension is **finite**, otherwise the extension is **infinite**.

**Example.**

(i)  $|\mathbb{C} : \mathbb{R}| = 2$ , with  $\mathbb{R}$ -basis  $1, i$

(ii)  $|\mathbb{Q}(i) : \mathbb{Q}| = 2$ , with  $\mathbb{Q}$ -basis  $1, i$

(iii)  $\mathbb{Q} \leq \mathbb{R}$  is an infinite extension.

**Theorem 1.3** (Tower law). Suppose  $K \leq L \leq M$  are **field extensions**. Then  $|M : K| = |M : L| |L : K|$ .

*Proof.* Assume that  $|M : L| < \infty$ , and  $|L : K| < \infty$ . Take an  $L$ -basis of  $M$ , given by  $\{ f_1, \dots, f_b \}$ , and a  $K$ -basis of  $L$  given by  $\{ e_1, \dots, e_a \}$ . Take  $m \in M$ , so  $m = \sum_{i=1}^b \mu_i f_i$  for some  $\mu_i \in L$ . Similarly,  $\mu_i = \sum_{j=1}^a \lambda_{ij} e_j$  for some  $\lambda_{ij} \in K$ , so

$$m = \sum_{i=1}^b \sum_{j=1}^a \lambda_{ij} e_j f_i$$

Thus  $\{ e_j f_i \mid 1 \leq j \leq a, 1 \leq i \leq b \}$  span  $M$ .

Linear independence: It's enough to show that if  $0 = m = \sum \sum \lambda_{ij} e_j f_i$  then  $\lambda_{ij}$  are all zero. However if  $m = 0$  the linear independence of  $f_i$  forces each  $\mu_i = 0$ . Then the linear independence of  $e_j$  forces  $\lambda_{ij}$  all to be zero, as required.  $\square$

The **Tower law** will not be proved for **infinite** extensions, but observe that if  $M$  is an infinite extension of  $L$  then it is an infinite extension of  $K$ , and similarly if  $L$  is an infinite extension of  $K$  then the larger field  $M$  must also be an infinite extension of  $K$ .

## 1.1 Motivatory Example

Observe  $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, i)$

- (i)  $\mathbb{Q}(\sqrt{2})$  has basis  $1, \sqrt{2}$  over  $\mathbb{Q}$ .
- (ii)  $\mathbb{Q}(\sqrt{2}, i)$  has basis  $1, i$  as a  $\mathbb{Q}(\sqrt{2})$ -vector space.
- (iii)  $\mathbb{Q}(\sqrt{2}, i)$  has basis  $1, \sqrt{2}, i, i\sqrt{2}$  over  $\mathbb{Q}$ .

$$|\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}| = 4 = 2 \cdot 2 = |\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})| |\mathbb{Q}(\sqrt{2}) : \mathbb{Q}|$$

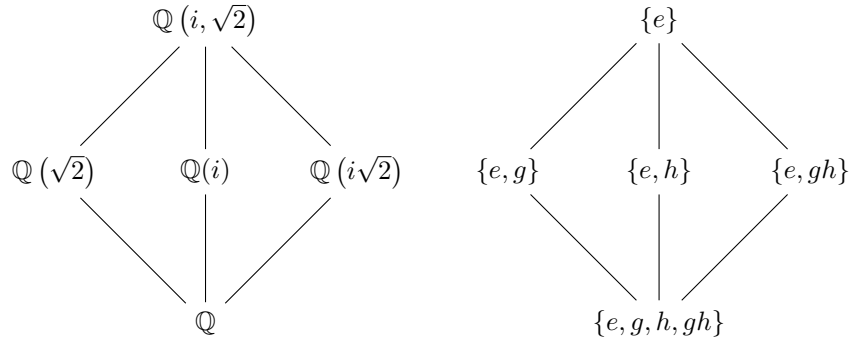
Any intermediate field strictly between  $\mathbb{Q}$  and  $\mathbb{Q}(\sqrt{2}, i)$  must be of degree 2 by the [Tower law](#).

What are these intermediate fields? There are  $\mathbb{Q}(\sqrt{2})$ ,  $\mathbb{Q}(i)$  and  $\mathbb{Q}(i\sqrt{2})$ , but are these all?

The Galois correspondence arising in the Fundamental Theorem of Galois Theory gives an order reversing bijection between the lattice of intermediate subfields and the subgroups of a group of ring automorphisms of the big field (in this case  $\mathbb{Q}(i, \sqrt{2})$ ) that fix the smaller field elementwise. For instance, consider the ring automorphisms of  $\mathbb{Q}(i, \sqrt{2})$  that fix  $\mathbb{Q}$ :

$$\begin{aligned} e : \sqrt{2} &\mapsto \sqrt{2} \\ i &\mapsto i \\ g : \sqrt{2} &\mapsto \sqrt{2} \\ i &\mapsto -i \\ h : \sqrt{2} &\mapsto -\sqrt{2} \\ i &\mapsto i \\ gh : \sqrt{2} &\mapsto -\sqrt{2} \\ i &\mapsto -i \end{aligned}$$

Notice that  $i$  and  $-i$  play the same role in the field  $\mathbb{Q}(\sqrt{2}, i)$ , both roots of  $t^2 + 1 = 0$ , similarly  $\sqrt{2}$  and  $-\sqrt{2}$  are both roots of  $t^2 - 2 = 0$ . The automorphism  $e$  is seen to be identity, and  $g$  is conjugation. These four form the group of order  $4 = |\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}|$ .



The recipe for producing an intermediate subfield from a subgroup is to take the elements of  $\mathbb{Q}(i, \sqrt{2})$  which are fixed by all elements of the subgroup. For instance,  $\mathbb{Q}(i\sqrt{2})$  is the field of elements fixed by both  $e$  and  $gh$ .

This correspondence doesn't always work for all finite field extensions. It works for Galois extensions. In the correspondence, normal extensions correspond to normal subgroups. In this example, all subgroups are normal and the extensions are normal. We'll also prove the Primitive Element Theorem, which in the context of finite extensions of  $\mathbb{Q}$  tells us that they are necessarily of the form  $\mathbb{Q}(\alpha)$  for some  $\alpha$ , for instance  $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$ .

## 1.2 Review of GRM

**Definition 1.4** (Algebraic). Suppose  $K \leq L$  is a field extension. Take  $\alpha \in L$  and define

$$I_\alpha = \{ f \in K[t] \mid f(\alpha) = 0 \}$$

We say  $\alpha$  is **algebraic** over  $K$  if  $I_\alpha \neq 0$ . Otherwise  $\alpha$  is **transcendental**. We say  $L$  is algebraic over  $K$  if  $\alpha$  is algebraic over  $K$  for all  $\alpha \in L$ .

**Remark.** We can see  $I_\alpha$  is an ideal of  $K[t]$  since it is the kernel of the ring homomorphism  $K[t] \rightarrow L$  given by  $f(t) \mapsto f(\alpha)$ .

**Example.**

- (i)  $\sqrt{2}$  is **algebraic** over  $\mathbb{Q}$
- (ii)  $\pi$  is not algebraic over  $\mathbb{Q}$

**Lemma 1.5.** Let  $K \leq L$  be a **finite field extension**. Then  $L$  is **algebraic** over  $K$ .

*Proof.* Let  $[L : K] = n$ , and take  $\alpha \in L$ . Consider  $1, \alpha, \alpha^2, \dots, \alpha^n$ , which must be linearly dependent in the  $n$ -dimensional  $K$ -vector space  $L$ . So,  $\sum_{i=0}^n \lambda_i \alpha^i = 0$  for some  $\lambda \in K$  not all zero, and hence  $\alpha$  is a root of  $f(t) = \sum_{i=0}^n \lambda_i t^i$ , so  $\alpha$  is **algebraic** over  $K$ .  $\alpha$  was arbitrary, so  $L$  is algebraic over  $K$ .  $\square$

**Definition 1.6** (Minimal polynomial). The non-zero ideal  $I_\alpha$  (where  $\alpha$  is **algebraic** over  $K$ ) is principal since  $K[t]$  is a principal ideal domain. In particular, we can say  $I_\alpha = (f_\alpha(t))$  where  $f_\alpha(t)$  can be assumed to be monic. Such a monic  $f_\alpha(t)$  is the **minimal polynomial** of  $\alpha$  over  $K$ .

**Remark.** Multiplication by  $\alpha$  within the field  $L$  gives a  $K$ -linear map  $L \rightarrow L$ , an automorphism (if  $\alpha \neq 0$ ). In GRM, we have seen the **minimal polynomial** of a linear map is unique.

**Example.**

- (i) The minimal polynomial of  $\sqrt{2}$  over  $\mathbb{Q}$  is  $t^2 - 2$ .
- (ii) The minimal polynomial of  $\sqrt{2}$  over  $\mathbb{R}$  is  $t - \sqrt{2}$ .

**Lemma 1.7.** Suppose  $K \leq L$  is a **field extension**,  $\alpha \in L$  and  $\alpha$  is **algebraic** over  $K$ . Then the **minimal polynomial**  $f_\alpha(t)$  of  $\alpha$  over  $K$  is irreducible in  $K[t]$  and  $I_\alpha$  is a prime ideal.

*Proof.* Suppose  $f_\alpha(t) = p(t)q(t)$ . We aim to show  $p(t)$  or  $q(t)$  is a unit in  $K[t]$ . But  $0 = f_\alpha(\alpha) = p(\alpha)q(\alpha)$ , so  $p(\alpha) = 0$  or  $q(\alpha) = 0$ , without loss of generality take  $p(\alpha) = 0$ , thus  $p(t) \in I_\alpha$ .

But  $I_\alpha = (f_\alpha(t))$ , so  $p(t) = f_\alpha(t)r(t)$ , giving  $f_\alpha(t) = f_\alpha(t)r(t)q(t)$  and so  $r(t)q(t) = 1$  in  $K[t]$ , and  $q(t)$  is a unit, as required. Recall from GRM that irreducible elements of  $K[t]$  are prime and hence generate prime ideals of  $K[t]$ . So  $I_\alpha$  is a prime ideal.  $\square$

**Definition 1.8** (Simple extension). Suppose  $K \leq L$  is a [field extension](#) and  $\alpha \in L$ .  $K(\alpha)$  is defined to be the smallest subfield of  $L$  containing  $K$  and  $\alpha$ . It's called the field **generated** by  $K$  and  $\alpha$ . We say that  $L$  is a **simple extension** if  $L = K(\beta)$  for some  $\beta \in L$ .

Given  $\alpha_1, \dots, \alpha_n \in L$ ,  $K \leq L$ .  $K(\alpha_1, \dots, \alpha_n)$  is the smallest field containing  $\alpha_1, \dots, \alpha_n$ . It is the field generated by  $K$  and  $\alpha_1, \dots, \alpha_n$ .

On the other hand  $K[\alpha]$  is the ring generated by  $K$  and  $\alpha$ , in particular the image of  $K[t]$  under the map  $f(t) \mapsto f(\alpha)$ .

**Theorem 1.9.** Suppose  $K \leq L$  is a [field extension](#) and  $\alpha \in L$  is [algebraic](#) over  $K$ . Then

- (i)  $K(\alpha) = K[\alpha]$
- (ii)  $[K(\alpha) : K] = \deg f_\alpha(t)$  where  $f_\alpha(t)$  is the [minimal polynomial](#) of  $\alpha$  over  $K$ .

*Proof.*

- (i) Clearly  $K[\alpha] \leq K(\alpha)$ . We aim to show that any non-zero element  $\beta$  of  $K[\alpha]$  is a unit, so  $K[\alpha]$  is a field.

By definition of  $K[\alpha]$ , we have  $\beta = g(\alpha)$  for some  $g(t) \in K[t]$ . Since  $\beta = g(\alpha) \neq 0$ ,  $g(t) \notin I_\alpha = (f_\alpha(t))$ . Thus  $f_\alpha(t) \nmid g(t)$ .

From [Lemma 1.7](#),  $f_\alpha(t)$  is irreducible and  $K[t]$  is a PID, we know  $\exists r(t), s(t) \in K[t]$  with

$$r(t)f_\alpha(t) + s(t)g(t) = 1 \in K[t].$$

Hence  $s(\alpha)g(\alpha) = 1$  in  $K[\alpha]$ , and so  $\beta = g(\alpha)$  is a unit, as required.

- (ii) Let  $n = \deg f_\alpha(t)$ . We'll show that  $T = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  is a  $K$ -vector space basis of  $K[\alpha]$ .

Spanning: If  $f_\alpha(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$  with  $a_i \in K$ , then  $\alpha^n = -a_{n-1}\alpha^{n-1} - \dots - a_0$ . This implies  $\alpha^n$  is a linear combination of  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ , and an easy induction shows that  $\alpha^m$  for  $m \geq n$  is likewise a linear combination of  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ , so we have spanning.

Linear independence: Suppose  $\lambda_{n-1}\alpha^{n-1} + \dots + \lambda_0 = 0$ . Let  $g(t) = \lambda_{n-1}t^{n-1} + \dots + \lambda_0$ . Since  $g(\alpha) = 0$ , we have  $g(t) \in I_\alpha = (f_\alpha(t))$ . So  $g(t) = 0$  or  $f_\alpha(t) \mid g(t)$ . The latter is not possible since  $\deg f_\alpha(t) > \deg g_\alpha(t)$  so  $g(t) = 0$  in  $K[t]$  and all the  $\lambda_i$ 's are zero.  $\square$

**Corollary 1.10.** If  $K \leq L$  is a [field extension](#) and  $\alpha \in L$ , then  $\alpha$  is [algebraic](#) over  $K$  if and only if  $K \leq K(\alpha)$  is [finite](#).

*Proof.*

( $\Rightarrow$ ) By [Theorem 1.9](#),  $[K(\alpha) : K] = \deg f_\alpha(t) \leq \infty$ .

( $\Leftarrow$ ) [Lemma 1.5](#)

□

**Corollary 1.11.** Let  $K \leq L$  be a field extension with  $|L : K| = n$ . Let  $\alpha \in L$ , then  $\deg f_\alpha(t) \mid n$ .

*Proof.* Use the Tower law on  $K \leq K(\alpha) \leq L$ . We deduce that  $|K(\alpha) : K|$  divides  $|L : K|$ . Theorem 1.9(ii) gives  $\deg f_\alpha(t) = |K(\alpha) : K|$ . □

### 1.3 Digression on (Non-)Constructibility

Schedules mention ‘other classical problems’ and we are now in a position to tackle some of these using Corollary 1.11.

A classical question from Greek geometry concerns the existence or otherwise of constructions using ruler and compasses (where a ruler refers to a single unmarked straight edge). If you’re an expert you can divide a line between 2 points into arbitrarily many equal segments, you can bisect an angle, or you can produce parallel lines. Given a polygon you can produce a square of the same area or double the area. However,

1. You cannot duplicate the cube using ruler and compasses (given a cube you can’t produce a cube of double the volume)
2. You cannot trisect the angle  $\pi/3$  using ruler and compasses.
3. The circle cannot be squared using ruler and compasses (given a circle you can’t construct a square of the same area)

Assume we’re given a set  $P_0$  of points in  $\mathbb{R}^2$ , and we can formalise our operations.

**Ruler operation** Draw a straight line through any two points in  $P_0$ .

**Compass operation** Draw a circle with the centre being a point in  $P_0$  and radius the distance between a pair of points in  $P_0$ .

**Definition 1.12** (Constructible). The points of intersection of any two distinct lines or circles drawn using these operations are **constructible in one step** from  $P_0$ . More generally, a point  $\mathbf{r} \in \mathbb{R}^2$  is **constructible** from  $P_0$  if there is a finite sequence  $\mathbf{r}_1, \mathbf{r}_2, \dots, \mathbf{r}_n = \mathbf{r}$  such that  $\mathbf{r}_1$  is constructible in one step from  $P_0 \cup \{\mathbf{r}_1, \dots, \mathbf{r}_{i-1}\}$ .

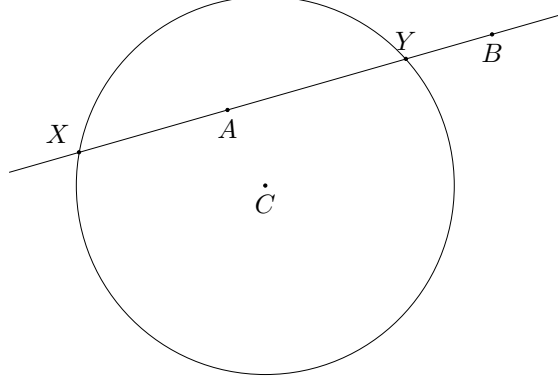
**Exercise.** Construct the midpoint of a line between two points.

Let  $K_0$  be the subfield of  $\mathbb{R}$  generated by  $\mathbb{Q}$  and the co-ordinates of the points in  $P_0$ . Let  $\mathbf{r}_i = (x_i, y_i)$  and set  $K_i = K_{i-1}(x_i, y_i)$ .

Thus  $K_0 \leq K_1 \leq K_2 \leq \dots \leq K_m \leq \mathbb{R}$ .

**Lemma 1.13.**  $x_i, y_i$  are both roots in  $K_i$  of quadratic polynomials in  $K_{i-1}[t]$ .

*Proof.* There are three cases for  $\mathbf{r}_i$ : line meets line, line meets circle, circle meets circle. We do the second case only here.



The line is defined by two points  $A = (p, q)$  and  $B = (r, s)$  while the circle is defined with a centre  $C = (t, u)$  and radius  $w$ . Then, points  $X$  and  $Y$  satisfy the equation of the line  $\frac{x-p}{r-p} = \frac{y-q}{s-q}$ , and the equation of the circle  $(x-t)^2 + (y-u)^2 = w^2$ . Solving these together gives coordinates of  $X$  and  $Y$  satisfying quadratic polynomials over  $K_{i-1}$ . The other two cases are left as an exercise for the reader.  $\square$

**Theorem 1.14.** If  $\mathbf{r} = (x, y)$  is [constructible](#) from a set  $P_0$  of points in  $\mathbb{R}^2$  and if  $K_0$  is the subfield of  $\mathbb{R}$  [generated](#) by  $\mathbb{Q}$  and the coordinates of the points in  $P_0$ , then the [degrees](#)  $|K_0(x) : K_0|$  and  $|K_0(y) : K_0|$  are powers of two.

*Proof.* Continue with the previous notation of  $K_i = K_{i-1}(x_i, y_i)$ . By the [Tower law](#),

$$|K_i : K_{i-1}| = |K_{i-1}(x, y) : K_{i-1}(x)| |K_{i-1}(x) : K_{i-1}|$$

But [Lemma 1.13](#) tells us that  $|K_{i-1}(x) : K_{i-1}|$  must be 1 or 2 depending on whether the quadratic polynomial arising in the lemma is reducible or not, using [Theorem 1.9\(ii\)](#). Similarly,  $|K_{i-1}(x, y) : K_{i-1}(x)|$  is 1 or 2.

So  $|K_i : K_{i-1}| = 1, 2$  or  $4$ , (but in fact 4 cannot happen), hence by the [Tower law](#),  $|K_n : K_0| = |K_n : K_{n-1}| |K_{n-1} : K_{n-2}| \dots |K_1 : K_0|$  is a power of two.

If  $r = (x, y)$  is constructible from  $P_0$ , then

$$x, y \in K_n \quad \text{and} \quad K_0 \leq K_0(x) \leq K_n \\ K_0 \leq K_0(y) \leq K_n$$

and the Tower Law again gives that  $|K_0(x) : K_0|$  and  $|K_0(y) : K_0|$  are also powers of 2.  $\square$

To use this for proofs about [non-constructibility](#) we need to be reasonably expert at working out [minimal polynomials](#).

**Theorem 1.15.** Let  $f(t)$  be a primitive integral polynomial. Then  $f(t)$  is irreducible in  $\mathbb{Q}[t]$  if and only if it is irreducible in  $\mathbb{Z}[t]$ .

*Proof.* A special case of Gauss' lemma from GRM.  $\square$

**Theorem 1.16** (Eisenstein's criterion). Let  $f(t) = a_n t^n + a_{n-1} t^{n-1} + \dots + a_0 \in \mathbb{Z}[t]$ . Suppose there is a prime  $p$  such that



- (i)  $p \nmid a_n$
- (ii)  $p \mid a_{n-1}, p \mid a_{n-2}, \dots, p \mid a_0$
- (iii)  $p^2 \nmid a_0$

Then  $f(t)$  is irreducible in  $\mathbb{Z}[t]$

*Proof.* Recall from GRM. □

**Example.** For  $p$  a prime, consider  $f(t) = t^{p-1} + t^{p-2} + \dots + 1$ . This is irreducible over  $\mathbb{Q}$  by considering  $f(t+1)$  and using  $p$  as the prime in [Eisenstein's criterion](#).

Another method is to consider an integral polynomial  $f(t) \pmod{p}$ . If  $f(t)$  is irreducible in  $\mathbb{Z}[t]$  then it is reducible over  $\mathbb{Z}/p\mathbb{Z}$ . So, if we find a prime  $p$  such that  $f(t) \pmod{p}$  is irreducible then  $f(t)$  is irreducible in  $\mathbb{Z}[t]$ .

**Example.**  $t^3 + t + 1$  is irreducible mod 2. If it were reducible it would have a linear factor and so the polynomial would have a root mod 2. But 0, 1 are not roots. So,  $t^3 + t + 1$  is irreducible in  $\mathbb{Z}[t]$ , hence irreducible in  $\mathbb{Q}[t]$ .

**Remark.** On a later example sheet you'll meet an irreducible polynomial in  $\mathbb{Z}[t]$  which is reducible mod  $p$  for all primes  $p$ .

**Theorem 1.17.** The cube cannot be duplicated by [ruler and compasses](#).

*Proof.* The problem amounts to whether given a unit distance, one can construct points distance  $\alpha$  apart, where  $\alpha$  satisfies  $t^3 - 2 = 0$ . Starting with points  $P_0 = \{(0, 0), (1, 0)\}$  can we produce  $(\alpha, 0)$ ?

No. If we could, [Theorem 1.14](#) would say  $|\mathbb{Q}(\alpha) : \mathbb{Q}|$  is a power of 2. But  $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$  since  $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg f_\alpha(t)$  where  $f_\alpha(t)$  is the [minimal polynomial](#) of  $\alpha$  over  $\mathbb{Q}$ .  $\alpha$  satisfies  $t^3 - 2$ , which is irreducible over  $\mathbb{Z}$  by [Eisenstein's criterion](#) hence irreducible over  $\mathbb{Q}$ . So  $t^3 - 2$  is the minimal polynomial  $f_\alpha(t)$ . □

**Theorem 1.18.** The circle cannot be squared using ruler and compasses.

*Proof.* Starting with  $(0, 0)$  and  $(1, 0)$ , we must [construct](#)  $(\sqrt{\pi}, 0)$  so that we have a square of side length  $\sqrt{\pi}$  and hence area  $\pi$ . But  $\pi$  and hence  $\sqrt{\pi}$  is transcendental over  $\mathbb{Q}$  (Lindemann - not proved here). [Theorem 1.14](#) tells us we can't do this construction. □

## 1.4 Return to theory development

**Lemma 1.19.** Let  $K \leq L$  be a [field extension](#). Then

- (i)  $\alpha_1, \dots, \alpha_n \in L$  are [algebraic](#) over  $K$  if and only if  $K \leq K(\alpha_1, \dots, \alpha_n)$  is a [finite](#) field extension.
- (ii) If  $K \leq M \leq L$  such that  $K \leq M$  is [finite](#), then there exist  $\alpha_1, \dots, \alpha_n \in L$  such that  $K(\alpha_1, \dots, \alpha_n) = M$ .

*Proof.*

- (i) By [Corollary 1.10](#),  $\alpha$  is algebraic over  $K$  if and only if  $K \leq K[\alpha]$  is a [finite field extension](#).  $\alpha_i$  is algebraic over  $K$  and hence algebraic over  $K(\alpha_1, \dots, \alpha_{i-1})$  and so

$$|K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})| < \infty.$$

By the [Tower law](#) applied to

$$K \leq K(\alpha_1) \leq K(\alpha_1, \alpha_2) \leq \dots \leq K(\alpha_1, \dots, \alpha_n),$$

we get  $|K(\alpha_1, \dots, \alpha_n) : K| < \infty$ .

Conversely, consider  $K \leq K(\alpha_i) \leq K(\alpha_1, \dots, \alpha_n)$ . Then the tower law says that if  $|K(\alpha_1, \dots, \alpha_n) : K| < \infty$  then  $|K(\alpha_i) : K| < \infty$  and by [Corollary 1.10](#),  $\alpha_i$  is algebraic over  $K$ .

- (ii) If  $|M : K| = n$  then  $M$  is an  $n$ -dimensional  $K$ -vector space, so there exists a  $K$ -basis  $\alpha_1, \dots, \alpha_n$  over  $M$ . Then  $K(\alpha_1, \dots, \alpha_n) \leq M$ . However, any element of  $M$  is a  $K$ -linear combination of  $\alpha_1, \dots, \alpha_n$  and so lies in  $K(\alpha_1, \dots, \alpha_n)$ , so  $M = K(\alpha_1, \dots, \alpha_n)$ .  $\square$

**Definition 1.20** (Homomorphism over a field). Suppose  $K \leq L$ ,  $K \leq L'$  are [field extensions](#). A  $K$ -**homomorphism**  $\phi : L \rightarrow L'$  is a ring homomorphism such that  $\phi|_K = \text{id}$ .

A  $K$ -homomorphism is a  $K$ -isomorphism if it is a ring isomorphism.

**Lemma 1.21.** Suppose  $K \leq L$ ,  $K \leq L'$  are [field extensions](#). Then

- (i) Any  $K$ -homomorphism  $\phi : L \rightarrow L'$  is injective and  $K \leq \phi(L)$  is a field extension.  
(ii) If  $|L : K| = |L' : K| < \infty$  then any  $K$ -homomorphism  $\phi : L \rightarrow L'$  is a [K-isomorphism](#).

*Proof.*

- (i)  $L$  is a field and  $\ker \phi$  is an ideal of  $L$ .

Note  $1 \mapsto 1$  and so  $\ker \phi$  can't be the whole of  $L$ , hence  $\ker \phi = \{0\}$ . So  $\phi(L)$  is a field and  $K \leq \phi(L)$  is a field extension.

- (ii)  $\phi$  is an injective  $K$ -linear map, so  $|\phi(L) : K| = |L : K|$ . In general,  $|\phi(L) : K| \leq |L' : K|$ , but since  $|L : K| = |L' : K|$  by assumption, we have  $|\phi(L) : K| = |L' : K|$ , hence  $\phi(L) = L'$  and  $\phi$  is a  $K$ -isomorphism  $L \rightarrow L'$ . (If  $L' = L$  then  $\phi$  would be a  $K$ -automorphism also.)  $\square$

**Definition 1.22** (Splitting). Let  $K \leq L$  be a field extension and  $f(t) \in K[t]$ . We say  $f$  **splits over  $L$**  if

$$f(t) = a(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_n)$$

where  $a \in K$  and  $\alpha_1, \dots, \alpha_n \in L$ .

We say  $L$  is a **splitting field for  $f$  over  $K$**  if  $L = K(\alpha_1, \dots, \alpha_n)$ .

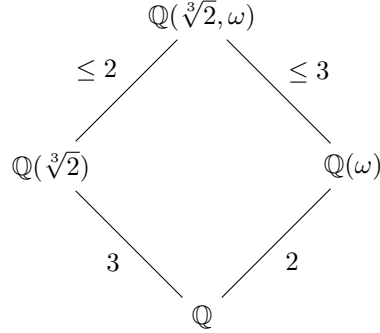
**Remark.** This is equivalent to saying that  $L$  is a [splitting field](#) for  $f$  over  $K$  iff

- (i)  $f$  splits over  $L$   
(ii) if  $K \leq M \leq L$  and  $f$  splits over  $M$  then  $M = L$ .

**Example.**

1. Consider  $f(t) = t^3 - 2$  over  $\mathbb{Q}$ .

$\mathbb{Q}(\sqrt[3]{2})$  is *not* a [splitting field](#) for  $f$  over  $\mathbb{Q}$ , but  $\mathbb{Q}(\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2})$  is a splitting field over  $\mathbb{Q}$  where  $\omega$  is a primitive cube root of unity  $\omega = e^{2\pi i/3}$



Starting in the bottom right, going clockwise:

- The [minimal polynomial](#) of  $\omega$  over  $\mathbb{Q}$  is  $t^2 + t + 1$ , so  $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$ .
- $t^3 - 2$  is irreducible over  $\mathbb{Q}$  by [Eisenstein's criterion](#), so  $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ .
- $\omega$  satisfies  $t^2 + t + 1$  over  $\mathbb{Q}$  and hence over  $\mathbb{Q}(\sqrt[3]{2})$  and so  $|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})| \leq 2$ .
- $\sqrt[3]{2}$  satisfies  $t^3 - 2$  over  $\mathbb{Q}$  and hence over  $\mathbb{Q}(\omega)$ , so  $|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\omega)| \leq 3$ .

Then by the [Tower law](#),  $2 \mid |\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}|$  and  $3 \mid |\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}|$ , so we deduce

$$\begin{aligned} |\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\omega)| &= 3 \\ |\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})| &= 2 \end{aligned}$$

2. Take  $f(t) = (t^2 - 3)(t^3 - 1)$ . The splitting field for  $f$  over  $\mathbb{Q}$  is

$$\begin{aligned} &\mathbb{Q}(\sqrt{3}, -\sqrt{3}, \omega, \omega^2, 1) \\ &= \mathbb{Q}(\sqrt{3}, \omega) = \mathbb{Q}(\sqrt{3}, i) \end{aligned}$$

since  $\omega = \frac{-1+i\sqrt{3}}{2}$ .

3.  $t^2 - 3$  and  $t^2 - 2t - 2$  have the same splitting field over  $\mathbb{Q}$ :  $\mathbb{Q}(\sqrt{3})$ .

4. Take  $f(t) = t^2 + t + 1$  in  $\mathbb{F}_2[t]$ .

$f(t)$  is irreducible over  $\mathbb{F}_2$  since it has no roots in  $\mathbb{F}_2$  and hence no linear factors in  $\mathbb{F}_2[t]$ . Hence,  $\mathbb{F}_2[t]/(t^2 + t + 1)$  is a field.

Set  $\alpha = t + (t^2 + t + 1) \in \mathbb{F}_2[t]/(t^2 + t + 1)$ , then

$$\frac{\mathbb{F}_2[t]}{(t^2 + t + 1)} = \mathbb{F}_2[\alpha].$$

The elements are  $0, 1, \alpha, 1 + \alpha$  noting that  $\alpha^2 + \alpha + 1 = 0$  and we have characteristic 2, so  $\alpha^2 = \alpha + 1$ .

$f(t)$  splits over  $\mathbb{F}_2[\alpha]$ :

$$f(t) = (t - \alpha)(t - 1 - \alpha)$$

Thus  $\mathbb{F}_2[\alpha]$  is the splitting field for  $f$  over  $\mathbb{F}_2$ .

We can use this final construction to produce splitting fields in general.

**Theorem 1.23** (Existence of splitting fields). Let  $K$  be a field and  $f(t) \in K[t]$ . Then there exists a [splitting field](#) for  $f$  over  $K$ .

*Proof.* If  $\deg f = 0$  then  $K$  is the splitting field for  $f$  over  $K$ .

Suppose  $\deg f > 0$  and pick an irreducible factor  $g(t)$  of  $f(t)$  in  $K[t]$ , noting that  $K \leq K[t]/(g(t))$  is a [field extension](#).

Take

$$\alpha_1 = t + (g(t)) \in K[t]/(g(t)),$$

then  $K[t]/(g(t)) = K(\alpha_1)$  and  $g(\alpha_1) = 0$  in  $K(\alpha_1)$ . Therefore  $f(\alpha_1) = 0$  in  $K(\alpha_1)$  and we can write  $f(t) = (t - \alpha_1)h(t)$  in  $K(\alpha_1)[t]$ .

Repeat, noting that  $\deg h(t) < \deg f(t)$  and so we get

$$f(t) = a(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_n)$$

where  $a$  is a constant in  $K$ . Thus, we have a factorisation of  $f(t)$  in  $K(\alpha_1, \dots, \alpha_n)[t]$ , and so  $K(\alpha_1, \dots, \alpha_n)$  is a splitting field for  $f$  over  $K$ .  $\square$

**Theorem 1.24** (Uniqueness of splitting fields). If  $K$  is a field and  $f(t) \in K[t]$ , then the [splitting field](#) for  $f$  over  $K$  is unique up to [K-isomorphism](#), that is, if there are two such splitting fields  $L$  and  $L'$ , there is a  $K$ -isomorphism  $\phi : L \rightarrow L'$ .

*Proof.* Suppose  $L$  and  $L'$  are splitting fields for  $f(t) \in K[t]$  over  $K$ . We need to show that there is a  $K$ -isomorphism  $L \rightarrow L'$ .

Suppose  $K \leq M \leq L$  and there exist  $M'$  with  $K \leq M' \leq L'$  and a  $K$ -isomorphism  $\psi : M \rightarrow M'$ . Clearly some  $M$  exists (we can take  $M = K$ ), so we pick  $M$  so that  $|M : K|$  is maximal among all such  $M, M', \psi$ .

We must show  $M = L$  and  $M' = L'$ . Note that if  $M = L$  then  $f(t)$  splits over  $M$ :

$$f(t) = a(t - \alpha_1) \cdots (t - \alpha_n) \in M[t]$$

Apply  $\psi$ , we get an induced map  $M[t] \rightarrow M'[t]$ .

$$f(t) = \psi(f(t)) = \psi(a)(t - \psi(\alpha_1)) \cdots (t - \psi(\alpha_n))$$

Thus  $f(t)$  splits over  $\psi(M) = M'$ . But  $L'$  is a splitting field and  $M' \leq L'$ , so  $M' = L'$ .

So, suppose  $M \neq L$  and we'll get a contradiction of maximality of  $M$ . Since  $M \neq L$ , there is a root  $\alpha$  of  $f(t)$  in  $L$  which isn't in  $M$ . Factorise  $f(t) = g(t)h(t)$  in  $M[t]$  so that  $g(t)$  is irreducible in  $M[t]$  while  $g(\alpha) = 0$  in  $L$ . Then there exists a  $K$ -homomorphism  $M[t]/(g(t)) \rightarrow L$  given by  $t + (g(t)) \mapsto \alpha$  which has image  $M(\alpha)$ .

The  $K$ -isomorphism  $M[t] \rightarrow M'[t]$  induced by  $\psi$  maps  $g(t) \in M[t]$  to  $\gamma(t) \in M'[t]$ .  $f(t) = g(t)h(t)$  in  $M[t]$  yields  $f(t) = \gamma(t)\delta(t)$  in  $M'[t]$ .

We have a field extension  $M' \leq M'[t]/(\gamma(t))$  and there exists a  $M'$ -homomorphism  $M'[t]/(\gamma(t)) \rightarrow L'$  given by  $t \mapsto \gamma(t)$  by picking a root  $\alpha'$  of  $\gamma(t)$  in  $L'$ . However  $\gamma(t) \mid f(t)$  in  $M'[t]$  and hence in  $L'[t]$  and so  $\alpha'$  is also a root of  $f(t)$  in  $L'$ . The  $M'$ -homomorphism gives a  $K$ -isomorphism

$$M'[t]/(\gamma(t)) \rightarrow M'(\alpha')$$

and so we have a  $K$ -isomorphism  $M(\alpha) \rightarrow M'(\alpha')$ . This contradicts the maximality of  $M$ , since  $M \not\subseteq M(\alpha)$ .  $\square$

**Definition 1.25** (Normal extension). A field extension  $K \leq L$  is **normal** if for every  $\alpha \in L$  the minimal polynomial  $f_\alpha(t)$  of  $\alpha$  over  $K$  splits over  $L$ .

**Theorem 1.26.** Let  $K \leq L$  be a finite field extension. Then  $K \leq L$  is normal  $\iff L$  is the splitting field for some  $f(t) \in K[t]$ .

*Proof.* Later.  $\square$

**Example 1.27.** Let  $\mathbb{F}$  be a finite field with  $|\mathbb{F}| = m$ .  $\mathbb{F}$  has characteristic  $p$  for some  $p$  and  $\mathbb{F}_p \leq \mathbb{F}$ , therefore  $m = p^r$  for some  $r$ . The non-zero elements form the multiplicative group of order  $m - 1 = n$  and they satisfy  $t^n - 1$ : they are roots of  $t^n - 1$ . So,

$$t^n - 1 = (t - \alpha_1) \cdots (t - \alpha_n)$$

where  $\alpha_1, \dots, \alpha_n$  are the non-zero elements of  $\mathbb{F}$ . Thus  $\mathbb{F}$  is the splitting field for  $t^n - 1$  over  $\mathbb{F}_p$ . By Theorem 1.24, any other field with  $m$  elements is  $\mathbb{F}_p$ -isomorphic to  $\mathbb{F}$ . (We'll show later that there is a field of  $m$  elements.)

**Theorem 1.28.** Let  $G$  be a finite subgroup of the multiplicative group of a field  $K$ . Then  $G$  is cyclic. In particular, the multiplicative group of a finite field is cyclic.

*Proof.* Let  $|G| = n$ . By the structure theorem of finite abelian groups from GRM,

$$G \cong C_{q_1^{m_1}} \times C_{q_2^{m_2}} \times \cdots \times C_{q_r^{m_r}}$$

with  $q_i$  prime, not necessarily distinct. However if  $q = q_i = q_j$  for some  $i \neq j$ , there are at least  $q^2$  distinct solutions of  $t^q - 1 = 0$  in  $K$  (since  $C_q \times C_q \cong$  subgroup of  $G$ ). But in a field (or even an integral domain), a polynomial of degree  $q$  has at most  $q$  roots, a contradiction. So all the  $q_i$  are distinct and hence  $G$  is cyclic, generated by  $(g_1, \dots, g_r)$  where  $g_i$  generates  $C_{q_i^{m_i}}$  using the Chinese Remainder Theorem.  $\square$

## 2 Separable, normal and Galois extensions

**Definition 2.1** (Separable polynomial). Let  $K$  be a field and  $f(t) \in K[t]$ . Suppose  $f(t)$  is irreducible in  $K[t]$  and  $L$  is a [splitting field](#) for  $f(t)$  over  $K$ . Then  $f(t)$  is **separable** over  $K$  if  $f(t)$  has no repeated roots in  $L$ .

For general  $f(t)$  we say  $f(t)$  is separable over  $K$  if every irreducible factor in  $K[t]$  is separable over  $K$ .

All constant polynomials are separable.

**Definition 2.2** (Formal differentiation). If  $K$  is a field then **formal differentiation**

$$\begin{aligned} D : K[t] &\rightarrow K[t] \\ t^n &\mapsto nt^{n-1} \end{aligned}$$

is a  $K$ -linear map. We denote this by  $D(f(t)) = f'(t)$ .

**Lemma 2.3.** Let  $K$  be a field and  $f(t), g(t) \in K[t]$ . Then:

- (a)  $D(f(t)g(t)) = f'(t)g(t) + f(t)g'(t)$  (Leibniz' rule)
- (b) Assume  $f(t) \neq 0$ . Then  $f(t)$  has a repeated root in a splitting field  $L$  if and only if  $f(t)$  and  $f'(t)$  have a common irreducible factor in  $K[t]$ .

*Proof.*

- (a)  $D$  is a  $K$ -linear map and so we only need to check for  $f(t) = t^n$ ,  $g(t) = t^m$ . Left as an exercise.
- (b) Let  $\alpha$  be a repeated root in a splitting field  $L$ , then

$$\begin{aligned} f(t) &= (t - \alpha)^2 g(t) \in L[t] \\ f'(t) &= (t - \alpha)^2 g'(t) + 2(t - \alpha)g(t) \end{aligned}$$

and so  $f'(\alpha) = 0$ . Therefore the [minimal polynomial](#)  $f_\alpha(t)$  of  $\alpha$  in  $K[t]$  divides both  $f(t)$  and  $f'(t)$  and thus  $f_\alpha(t)$  is a common irreducible factor of  $f(t)$  and  $f'(t)$ .

Conversely, let  $h(t)$  be a common irreducible factor of  $f(t)$  and  $f'(t)$  in  $K[t]$ . Pick a root  $\alpha$  in  $L$  of  $h(t)$ .

So  $f(\alpha) = 0 = f'(\alpha)$ , thus  $f(t) = (t - \alpha)g(t)$  in  $L[t]$ , and  $f'(t) = (t - \alpha)g'(t) + g(t)$ . Since  $f'(\alpha) = 0$  we have  $(t - \alpha) \mid f'(t)$ . and so  $(t - \alpha) \mid g(t)$ . Hence  $(t - \alpha)^2 \mid f(t)$  and we have a repeated root.  $\square$

**Corollary 2.4.** If  $K$  is a field and  $f(t) \in K[t]$  is irreducible:

- (i) If the characteristic of  $K$  is 0, then  $f(t)$  is [separable](#) over  $K$ .
- (ii) If the characteristic of  $K$  is  $p > 0$ , then  $f(t)$  is not separable if and only if  $f(t) \in K[t^p]$ .

*Proof.* By [Lemma 2.3](#),  $f(t)$  is not separable over  $K$  if and only if  $f(t)$  and  $f'(t)$  have a common irreducible factor. Since we're assuming  $f(t)$  is irreducible, this is equivalent to saying  $f'(t) = 0$ .

$$\begin{aligned} f(t) &= a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 \\ f'(t) &= n a_n t^{n-1} + \cdots + a_1 \end{aligned}$$

Thus  $f'(t) = 0 \iff i a_i = 0$  for all  $i > 0$ .

- (i) If  $\text{char } K = 0$  then  $f'(t) \neq 0$  for any non-constant polynomial, so  $f(t)$  is separable over  $K$ .
- (ii) If  $\text{char } K = p > 0$  then if  $f'(t) = 0$  we have  $ia_i = 0$  for all  $i > 0$ , so  $f(t)$  is not separable  $\iff f(t) \in K[t^p]$ .  $\square$

**Definition 2.5** (Separable extension). We say  $\alpha \in L$  is **separable over  $K$**  if its **minimal polynomial** is **separable** over  $K$ .

$L$  is **separable over  $K$**  if all  $\alpha \in L$  are separable over  $K$ .

If  $f_\alpha(t) = (t - \alpha)^n = t^n - \alpha^n$  where  $n$  is a power of  $p (= \text{char } K)$ , we say that  $\alpha$  is **purely inseparable over  $K$** .

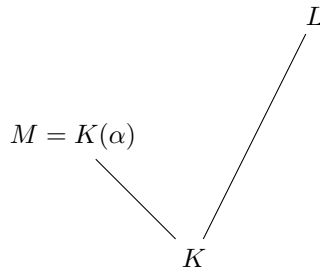
**Example.**

- (1) Let  $\mathbb{Q} \subseteq L$  be an **algebraic field extension**. Then  $L$  is **separable** over  $\mathbb{Q}$ .
- (2) Let  $L = \mathbb{F}_p(X)$  be the rational functions in  $X$  over  $\mathbb{F}_p$ , and  $K = \mathbb{F}_p(X^p)$ . Then  $K \leq L$  is not separable. Observe that if  $f(t) = t^p - X^p \in K[t]$  then  $f'(t) = 0$ . But  $t^p - X^p = (t - X)^p$  in  $L[t]$  since the binomial expansion gives other terms divisible by  $p$  and hence 0 since the characteristic is  $p$ .  
However  $f(t)$  is irreducible in  $K[t]$ : Suppose  $f(t) = g(t)h(t)$  in  $K[t]$  and hence in  $L[t]$ . So we get  $g(t) = (t - X)^r$  for some  $0 < r < p$  if the factorisation is non-trivial. But this would mean  $X^r$  was in  $K$ . However,  $\exists$  integers  $a, b$  such that  $ar + bp = 1$ . So  $(X^r)^a (X^p)^b \in K$  and so  $X \in K$ , thus we'd have  $X = \frac{u(X^p)}{v(X^p)}$ , a contradiction.  
Thus  $f(t) = t^p - X^p$  is the **minimal polynomial** of  $X$  over  $K$ , thus  $X$  is **purely inseparable** over  $K$  and  $K \leq L$  is not separable.
- (3) Take  $\mathbb{F}$  a finite field with order  $m$ , a power of  $p$  where  $\text{char } \mathbb{F} = p$ . Consider  $f(t) = t^n - 1$  where  $n = m - 1$ . This is separable over  $\mathbb{F}_p$  since we saw that  $f(t)$  has distinct linear factors in  $\mathbb{F}[t]$ .

**Remark.** It's useful to have an alternative approach to **separability of field extensions** without having to check **separability of minimal polynomials** for all elements of the larger field. This is where we start thinking about  **$K$ -homomorphisms**.

**Lemma 2.6.** Let  $M = K(\alpha)$ , where  $\alpha$  is **algebraic** over  $K$  and let  $f_\alpha(t)$  be the **minimal polynomial** of  $\alpha$  over  $K$ .

Then, for any **field extension**  $K \leq L$ , the number of  **$K$ -homomorphisms** of  $M$  to  $L$  is equal to the number of distinct roots of  $f_\alpha(t)$  in  $L$ . Thus this number is  $\leq \deg f_\alpha(t) = |K(\alpha) : K| = |M : K|$ .



*Proof.* We saw in [Lemma 1.21](#) that any  $K$ -homomorphism  $M \rightarrow L$  is injective, and we have

$$K(\alpha) \cong \frac{K[t]}{(f_\alpha(t))}.$$

For any root  $\beta$  of  $f_\alpha(t)$  in  $L$  we can define a  $K$ -homomorphism

$$\begin{aligned} \frac{K[t]}{(f_\alpha(t))} &\rightarrow L \\ t + (f_\alpha(t)) &\mapsto \beta \end{aligned}$$

Thus we get a  $K$ -homomorphism  $M \rightarrow L$ .

Conversely, for any  $K$ -homomorphism  $\phi : M \rightarrow L$  the image  $\phi(\alpha)$  must satisfy

$$f_\alpha(\phi(\alpha)) = 0.$$

These processes are inverse to each other, giving a 1-1 correspondence

$$\{K \text{ homomorphisms } M \rightarrow L\} \longleftrightarrow \{\text{roots of } f_\alpha(t) \in L\}. \quad \square$$

**Example.** Take  $K = \mathbb{Q}$ ,  $L = \mathbb{Q}(\sqrt[3]{2})$ , and use  $\alpha = \sqrt[3]{2}$ , with [minimal polynomial](#)  $f_\alpha(t) = t^3 - 2$ .

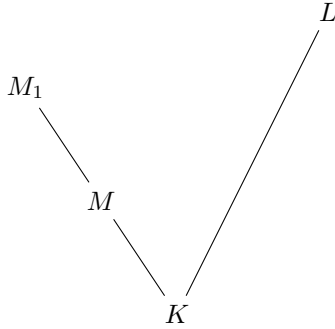
Then, there is only one  $K$ -homomorphism  $M = K(\sqrt[3]{2}) = L \rightarrow L$ , the identity map.

**Corollary 2.7.** The number of  $K$ -homomorphisms  $K(\alpha) \rightarrow L = \deg f_\alpha(t) \iff L$  is large enough, in particular  $L$  contains a [splitting field](#) for  $f_\alpha(t)$  and  $\alpha$  is [separable](#) over  $K$ .

*Proof.* Immediate from [Lemma 2.6](#).  $\square$

**Lemma 2.8.** Let  $K \leq M$  be a [field extension](#) and  $M_1 = M(\alpha_1)$  (where  $\alpha_1$  is [algebraic](#) over  $M$ ). Let  $f(t)$  be the [minimal polynomial](#) of  $\alpha_1$  over  $M$  and let  $K \leq L$ . Let  $\phi : M \rightarrow L$  be a  $K$ -homomorphism. Then there is a correspondence

$$\{\text{Extensions } \phi_1 : M_1 \rightarrow L \text{ of } \phi\} \longleftrightarrow \{\text{roots of } \phi(f(t)) \in L\}.$$



**Remark.** [Lemma 2.6](#) is the special case  $M = K$  and  $\phi =$  inclusion of  $K$  in  $L$ .

*Proof.*  $f(t)$  is irreducible in  $M[t]$ , so  $\phi(f(t))$  is irreducible in  $\phi(M)[t]$ . Any extension  $\phi_1 : M_1 \rightarrow L$  of  $\phi$  produces a root  $\phi_1(\alpha)$  of  $\phi(f(t))$ .

Conversely, given a root  $\gamma$  of  $\phi(f(t))$  in  $L$ ,

$$M_1 = M(\alpha_1) \cong \frac{M[t]}{(f(t))} \cong \frac{\phi(M)[t]}{(\phi(f(t)))} \cong \phi(M)(\gamma) \leq L.$$

Thus we get an extension  $\phi_1$  of  $\phi$  as required.  $\square$



**Corollary 2.9.** If  $L$  is large enough, the number of  $\phi_1$  which extend  $\phi$  is equal to the number of distinct roots of  $f(t)$  in  $L$ . This is equal to  $|M_1 : M| \iff \alpha$  is [separable](#) over  $M$ .

*Proof.* Immediate from [Lemma 2.8](#). □

**Corollary 2.10.** Let  $K \leq M \leq N$  be finite field extensions,  $K \leq L$ . Let  $\phi : M \rightarrow L$  be a  $K$ -homomorphism. Then the number of extensions of  $\phi$  to maps  $\theta : N \rightarrow L$  is  $\leq |N : M|$ . Moreover, such a  $\theta$  exists if  $L$  is large enough.

*Proof.* Pick  $\alpha_1, \dots, \alpha_r$  so that  $N = M(\alpha_1, \dots, \alpha_r)$  and set  $M_i = M(\alpha_1, \dots, \alpha_i)$ . Then we've got

$$M \leq M_1 \leq M_2 \leq \dots \leq M_r = N.$$

Using [Lemma 2.8](#), there are

$$\begin{aligned} &\leq |M_1 : M| \text{ extensions } \phi_1 : M_1 \rightarrow L \text{ of } \phi \\ &\leq |M_2 : M_1| \text{ extensions } \phi_2 : M_2 \rightarrow L \text{ of } \phi_1 \\ &\vdots \\ &\leq |M_r : M_{r-1}| \text{ extensions } \phi_r : M_r \rightarrow L \text{ of } \phi_{r-1} \end{aligned}$$

By the [Tower law](#), the number of extensions  $\theta : N \rightarrow L$  (recall  $N = M_r$ ) of  $\phi : M \rightarrow L$  is

$$\leq |M_r : M_{r-1}| |M_{r-1} : M_{r-2}| \dots |M_1 : M| = |N : M|$$

where the last part comes from the proof of [Lemma 2.8](#) - we need  $L$  to contain roots. □

**Remark 2.11.** This proof together with [Corollary 2.9](#) shows that the number of extensions  $\theta$  of  $\phi$  is equal to  $|N : M|$  iff  $L$  is large enough (so that everything splits) and  $\alpha_i$  is [separable](#) over  $M(\alpha_1, \dots, \alpha_{i-1})$ .

**Lemma 2.12.** Let  $K \leq N$  be a field extension with  $|N : K| = n$  and  $N = K(\alpha_1, \dots, \alpha_r)$  say. Then the following are equivalent:

- (i)  $N$  is [separable](#) over  $K$ .
- (ii) Each  $\alpha_i$  is separable over  $K(\alpha_1, \dots, \alpha_{i-1})$ .
- (iii) If  $K \leq L$  is large enough there are exactly  $n$  distinct [K-homomorphisms](#)  $N \rightarrow L$ .

*Proof.* (i)  $\Rightarrow$  (ii).  $N$  is [separable](#) over  $K \implies \alpha_i$  is separable over  $K$ . The [minimal polynomial](#) of  $\alpha_i$  over  $K(\alpha_1, \dots, \alpha_{i-1})$  divides the minimal polynomial of  $\alpha_i$  over  $K$  (in  $K(\alpha_1, \dots, \alpha_{i-1})[t]$ ).

So if the latter has distinct roots in a splitting field then the former does. So  $\alpha_i$  separable over  $K \implies \alpha_i$  separable over  $K(\alpha_1, \dots, \alpha_{i-1})$ .

(ii)  $\Rightarrow$  (iii) follows from [Remark 2.11](#).

(iii)  $\Rightarrow$  (i). Assume (iii) is true and (i) false, aiming for a contradiction. So,  $\exists \beta \in N$  that is not [separable](#) over  $K$ , so there are  $\leq |K(\beta) : K|$   $K$ -homomorphisms  $\phi : K(\beta) \rightarrow L$  by [Corollary 2.7](#).

By [Corollary 2.10](#),  $\phi$  extends to  $\leq |N : K(\beta)|$  extensions  $\theta : N \rightarrow L$ , and so there are  $\leq |N : K(\beta)| |K(\beta) : K|$   $K$ -homomorphisms  $N \rightarrow L$ , contradiction. □

**Definition 2.13** (Separably generated). We say  $M = K(\alpha_1, \dots, \alpha_r)$  is **separably generated** by  $\alpha_1, \dots, \alpha_r$  over  $K$  if each  $\alpha_i$  is **separable** over  $K$ .

**Corollary 2.14.** A finite extension is **separable**  $\iff$  it is **separably generated**.

*Proof.* Lemma 2.12. □

**Lemma 2.15.** If  $K \leq M \leq L$  **finite field extensions**,  $M \leq L$ , then

$$K \leq M, \quad M \leq L \text{ are both } \text{separable} \iff K \leq L \text{ is separable}$$

*Proof.* Example sheet. □

**Example 2.16.** Take  $\mathbb{F}$  a finite field,  $|\mathbb{F}| = m$ . Multiplicative group of order  $n = m - 1$  is cyclic. Take a generator  $\alpha$ , then  $\mathbb{F} = \mathbb{F}_p(\alpha)$ , and so the **minimal polynomial** of  $\alpha$  divides  $t^n - 1$ . Observe this has distinct roots, which are all of  $\mathbb{F} \setminus \{0\}$  since  $\alpha^n = 1$ . So the minimal polynomial of  $\alpha$  is **separable**, and  $\mathbb{F} = \mathbb{F}_p(\alpha)$  is separable over  $\mathbb{F}_p$ .

**Theorem 2.17** (Primitive Element Theorem). Any **finite separable** extension  $K \leq M$  is a **simple** extension, that is,  $M = K(\alpha)$  for some  $\alpha$ , called a primitive element.

*Proof.* First deal with the case where  $K$  is a finite field. Then  $M$  is also finite and we can take  $\alpha$  to be a generator of the multiplicative group of  $M$ , which is cyclic.

Now assume  $K$  is an infinite field.

Since  $K \leq M$  is a finite extension,  $M = K(\alpha_1, \alpha_2, \dots, \alpha_n)$  for some  $\alpha_i$ . It is enough to show that any field  $M = K(\alpha, \beta)$  with  $\beta$  separable over  $K$  is of the form  $K(\gamma)$ .

Take  $f(t)$  and  $g(t)$  to be the **minimal polynomials** of  $\alpha$  and  $\beta$  over  $K$  and let  $L$  be the **splitting field** for  $f(t)g(t)$  over  $K(\alpha, \beta)$ . Say the distinct zeros of  $f(t)$  in  $L$  are  $\alpha = \alpha_1, \dots, \alpha_a$  and of  $g(t)$  are  $\beta = \beta_1, \dots, \beta_b$ .

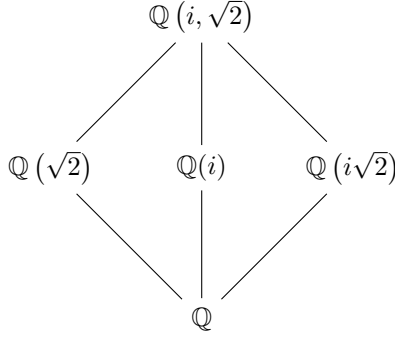
By separability,  $b = \deg g(t)$ . Choose  $\lambda \in K$  such that all  $\alpha_i + \lambda\beta_j$  are distinct, which is possible since  $K$  is infinite. Set  $\gamma = \alpha + \lambda\beta$ .

Let  $F(t) = f(\gamma - \lambda t) \in K(\gamma)[t]$ . We have  $g(\beta) = 0$  and  $F(\beta) = f(\alpha) = 0$ . Thus  $F(t)$  and  $g(t)$  have a common zero.

Any other common zero would have to be  $\beta_j$  for some  $j > 1$ . But then  $F(\beta_j) = f(\alpha + \lambda(\beta - \beta_j))$ . By assumption,  $\alpha + \lambda(\beta - \beta_j)$  is never an  $\alpha_i$  and so  $F(\beta_j) \neq 0$ . Separability of  $g(t)$  says its linear factors are all distinct, so  $(t - \beta)$  is a highest common factor of  $F(t)$  and  $g(t)$  in  $L[t]$ .

However the minimal polynomial  $h(t)$  of  $\beta$  over  $K(\gamma)$  then divides  $F(t)$  and  $g(t)$  in  $K(\gamma)[t]$  and hence in  $L[t]$ . This implies  $h(t) = t - \beta$  and so  $\beta \in K(\gamma)$ . Therefore  $\alpha = \gamma - \lambda\beta \in K(\gamma)$  and so  $K(\alpha, \beta) \subset K(\gamma)$  and equality holds since  $\gamma \in K(\alpha, \beta)$ . □

**Example.** From our example in Section 1.1,  $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, i)$ , we had intermediate subfields.



If we follow the procedure of the proof of [Theorem 2.17](#),  $\alpha = \sqrt{2}$ ,  $\beta = i$ ,  $f(t) = t^2 - 2$ ,  $g(t) = t^2 + 1$ . Consider  $\sqrt{2} + \lambda i$  where  $\pm\sqrt{2} \pm \lambda i$  are distinct. For instance  $\lambda = 1$ , so  $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$ .

## 2.1 Trace and Norm

**Definition 2.18** (Trace and norm). Let  $K \leq M$  be a [finite field extension](#), and  $\alpha \in M$ . Multiplication by  $\alpha$  gives a  $K$ -linear map  $\theta_\alpha : M \rightarrow M$ .

Then we define

**Trace of  $\alpha$  over  $K$**  is given by  $\text{Tr}_{M/K}(\alpha) = \text{trace of } \theta_\alpha \in K$ .

**Norm of  $\alpha$  over  $K$**  is given by  $N_{M/K}(\alpha) = \text{determinant of } \theta_\alpha \in K$ .

Note these are dependent on the field extension.

**Theorem 2.19.** With the above notation, suppose  $f_\alpha(t) = t^s + a_{s-1}t^{s-1} + \cdots + a_0$  is the [minimal polynomial](#) for  $\alpha$  over  $K$ . Let  $r = [M : K(\alpha)]$ , then the characteristic polynomial of  $\theta_\alpha$  is  $(f_\alpha(t))^r$ .

Note

$$[M : K] = [M : K(\alpha)] [K(\alpha) : K] = rs.$$

Then  $\text{Tr}_{M/K}(\alpha) = -ra_{s-1}$  and  $N_{M/K}(\alpha) = ((-1)^s a_0)^r$ .

*Proof.* Regard  $M$  as a  $K(\alpha)$ -vector space with basis  $1 = \beta_1, \dots, \beta_r$ . Now take the  $K$ -vector space basis  $1, \alpha, \alpha^2, \dots, \alpha^{s-1}$  of  $K(\alpha)$ . So,  $1, \alpha, \alpha^2, \dots, \alpha^{s-1}, \beta_2, \beta_2\alpha, \dots, \beta_2\alpha^{s-1}, \beta_3, \dots$  is a  $K$ -vector space basis for  $M$ . Multiplication by  $\alpha$  in  $K(\alpha)$  is represented by matrix

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ 0 & 0 & 1 & \dots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -a_{s-1} \end{pmatrix}$$

an  $s \times s$  matrix whose characteristic polynomial is  $f_\alpha(t)$ .

Multiplication by  $\alpha$  in  $M$  is represented by the  $rs \times rs$  matrix

$$\begin{pmatrix} \mathbf{A} & 0 & 0 & \dots & 0 \\ 0 & \mathbf{A} & 0 & \dots & 0 \\ 0 & 0 & \mathbf{A} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \mathbf{A} \end{pmatrix}$$

whose characteristic polynomial is  $(f_\alpha(t))^r$ .

Look at the terms of this characteristic polynomial to get the trace and norm.  $\square$

**Theorem 2.20.** Let  $K \leq M$  be a [finite separable field extension](#) and  $[M : K] = n$ ,  $\alpha \in M$ . Let  $K \leq L$  be large enough so that there are  $n$  distinct  $K$ -homomorphisms

$$\sigma_1, \sigma_2, \dots, \sigma_n : M \longrightarrow L.$$

Then the characteristic polynomial of  $\theta_\alpha : M \rightarrow M$  (the multiplication map) is

$$\prod_{i=1}^n (t - \sigma_i(\alpha))$$

hence

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \quad \text{and} \quad N_{M/K}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

*Proof.* Write

$$\begin{aligned} f_\alpha(t) &= (t - \alpha_1) \dots (t - \alpha_s) \in L[t] \\ &= t^s + a_{s-1}t^{s-1} + \dots + a_0 \end{aligned}$$

the [minimal polynomial](#) of  $\alpha$  over  $K$  (where  $L$  large enough implies  $f_\alpha(t)$  splits in  $L$ ). There are  $s$  [K-homomorphisms](#)  $K[\alpha] \rightarrow L$  corresponding to maps sending  $\alpha$  to  $\alpha_i$ .

Each of these extends in  $|M : K(\alpha)|$  ways to give  $K$ -homomorphisms  $M \rightarrow L$  (by [separability](#) and [Corollary 2.9](#)).

However each of these extensions of a map sending  $\alpha \rightarrow \alpha_i$  still sends  $\alpha \rightarrow \alpha_i$ . Set  $r = |L : K(\alpha)|$ . Thus there are  $r$  maps sending  $\alpha \rightarrow \alpha_i$  for each  $i$ . Thus if the  $n(= rs)$  distinct  $K$ -homomorphisms  $M \rightarrow L$  are  $\sigma_1, \dots, \sigma_n$ , then

$$\begin{aligned} \sum_{i=1}^n \sigma_i(\alpha) &= r(\alpha_1 + \alpha_2 + \dots + \alpha_s) = -ra_{s-1} = \mathrm{Tr}_{M/K}(\alpha) \\ \prod_{i=1}^n \sigma_i(\alpha) &= ((-1)^s a_0)^n = N_{M/K}(\alpha). \end{aligned} \quad \square$$

**Theorem 2.21.** Let  $K \leq M$  be a [finite separable extension](#). Then we define a  $K$ -bilinear form

$$\begin{aligned} T : M \times M &\rightarrow K \\ (x, y) &\longmapsto \mathrm{Tr}_{M/K}(xy). \end{aligned}$$

Then this is non-degenerate and in particular the  $K$ -linear map  $\mathrm{Tr}_{M/K} : M \rightarrow K$  is non-zero, and hence surjective.

**Remark.** If  $K \leq M$  is a finite extension which is not [separable](#) then  $\text{Tr}_{M/K} : M \rightarrow K$  is always zero and so  $T : M \times M \rightarrow K$  is degenerate (see example sheet).

*Proof.* Separability and finiteness give  $M = K(\alpha)$  for some  $\alpha$ , by [Theorem 2.17](#). We have a  $K$ -basis  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  of  $K(\alpha)$  where  $n = [M : K]$ . The  $K$ -bilinear form is represented by

$$A = \begin{pmatrix} \text{Tr}_{M/K}(1) & \text{Tr}_{M/K}(\alpha) & \dots \\ \text{Tr}_{M/K}(\alpha) & \text{Tr}_{M/K}(\alpha^2) & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}.$$

Let  $L$  be the splitting field of the minimal polynomial  $f_\alpha(t)$  of  $\alpha$  over  $K$ .

Thus  $f_\alpha(t) = (t - \alpha_1) \cdots (t - \alpha_n)$  with  $\alpha_1, \dots, \alpha_n \in L$ . The entries in  $A$  are of the form  $\text{Tr}_{M/K}(\alpha^e)$  which is  $\alpha_1^e + \dots + \alpha_n^e$  using [Theorem 2.20](#).

Now consider  $\Delta = \prod_{i < j} (\alpha_i - \alpha_j)$ , the discriminant of  $V$ :

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{pmatrix}.$$

Observe that  $VV^T = A$ , and  $0 \neq \Delta^2 = |VV^T| = |A|$ , so  $A$  is non-singular and therefore the bilinear form  $T$  is non-degenerate.  $\square$

**Remark.** We'll meet  $\Delta$  again shortly, as it is the discriminant of the polynomial  $f_\alpha(t)$ .

## 2.2 Normal extensions

We restate [Definition 1.25](#) and [Theorem 1.26](#):

**Definition 1.25** (Normal extension). An [extension](#)  $K \leq L$  is **normal** if for every  $\alpha \in L$  the [minimal polynomial](#)  $f_\alpha(t)$  of  $\alpha$  over  $K$  [splits](#) over  $L$ .

**Theorem 1.26.** Let  $K \leq L$  be a [finite field extension](#). Then  $K \leq L$  is [normal](#)  $\iff$   $L$  is the [splitting field](#) for some  $f(t) \in K[t]$ .

*Proof.* Assume  $K \leq M$  is [normal](#). Pick  $\alpha_1, \dots, \alpha_r \in M$  so that  $M = K(\alpha_1, \dots, \alpha_r)$ . Let  $f_{\alpha_i}(t)$  be the [minimal polynomial](#) for  $\alpha_i$  over  $K$ .

Let

$$f(t) = f_{\alpha_1}(t)f_{\alpha_2}(t) \cdots f_{\alpha_r}(t).$$

By normality, each  $f_{\alpha_i}(t)$  splits over  $M$  and therefore  $f(t)$  splits over  $M$ .  $M$  is the splitting field of  $f(t)$  over  $K$  since if  $\beta_1, \dots, \beta_m$  are the roots of  $f(t)$  then  $M = K(\beta_1, \dots, \beta_m)$ .

Conversely, suppose  $M$  is a splitting field for  $f(t)$  over  $K$ . Thus  $M = K(\beta_1, \dots, \beta_m)$  where the  $\beta_j$  are the roots of  $f(t)$  in  $M$ .

Take  $\alpha \in M$ . Let  $f_\alpha(t)$  be the minimal polynomial of  $\alpha$  over  $K$ . Let  $M \leq L$  large enough so that  $f_\alpha(t)$  splits in  $L$  and consider [K-homomorphisms](#)  $\phi : M \rightarrow L$ .  $\phi(\beta_j)$  is also a root of  $f(t)$  and is therefore one of the  $\beta_j$ s. Injectivity of  $K$ -homomorphisms ([Lemma 1.21](#)) implies that  $\phi(\beta_j)$  generate the  $\beta_j$ .

$M = K(\beta_1, \dots, \beta_m)$  and so  $\phi$  is determined by the images of the  $\beta_j$  and thus  $\phi(M) = M$ . However if  $\alpha_i$  is a root of  $f_\alpha(t)$  in  $L$ , there is a  $K$ -homomorphism

$$\begin{aligned} K(\alpha) &\longrightarrow K(\alpha_i) \leq L \\ \alpha &\longmapsto \alpha_i. \end{aligned}$$

This extends by [Corollary 2.10](#) to a  $K$ -homomorphism  $\phi : M \rightarrow L$  with  $\phi(\alpha) = \alpha_i$ . But  $\phi(M) = M$ , so  $\alpha_i \in M$ . Thus  $M$  is normal over  $K$ .  $\square$

**Remark.** As for [separability](#), the property of ‘normality’ is equivalent to ‘normally generated’. In particular, a [finite extension](#)  $K \leq L$  is normal if and only if  $L = K(\alpha_1, \dots, \alpha_r)$ , with each  $f_{\alpha_i}(t)$  [splitting](#) over  $L$ .

**Definition 2.22** (Automorphism group). Let  $K \leq M$  be a [finite field extension](#). Its  $K$ -**automorphism** group is  $\text{Aut}_K(M) = \{ \phi \mid \phi \text{ a } K\text{-homomorphism } M \rightarrow M \}$ .

From [Lemma 1.21](#) we know that such  $K$ -homomorphisms are isomorphisms and thus have inverses. Composition gives the group operation.

**Lemma 2.23.**

$$|\text{Aut}_K(M)| \leq |M : K|.$$

*Proof.* [Corollary 2.10](#).  $\square$

**Theorem 2.24.** Let  $K \leq M$  be a [finite field extension](#). Then  $|\text{Aut}_K(M)| = |M : K|$  iff the extension is both [normal](#) and [separable](#).

**Definition 2.25** (Galois extension). A [finite field extension](#) that is [normal](#) and [separable](#) is a **Galois extension**.

**Definition 2.26** (Galois group). Let  $K \leq M$  be a [Galois extension](#). Then, the  $K$ -**automorphism group** of  $M$  is the **Galois group** of  $M$  over  $K$ . Write this as  $\text{Gal}(M/K)$ .

**Remark.** Some authors use ‘Galois group’ for the [automorphism group](#) even when the extension is not [Galois](#).

*Proof of Theorem 2.24.* ( $\Rightarrow$ ). Suppose  $|\text{Aut}_K(M)| = |M : K| = n$ . Let  $L$  be large enough containing  $M$ .

The  $n$  distinct  $K$ -homomorphisms  $\phi : M \rightarrow M \leq L$  give us  $n$   $K$ -homomorphisms  $\phi : M \rightarrow L$  and [Lemma 2.12](#) says that  $M$  is separable over  $K$ . For normality, pick  $\alpha \in M$  with [minimal polynomial](#)  $f_\alpha(t)$  over  $K$ .

Take  $M = K(\alpha_1, \dots, \alpha_m)$  as in the proof of [Corollary 2.10](#) with  $\alpha = \alpha_1$  and  $L = M$ . We only get  $|M : K|$  extensions of the inclusion  $K \hookrightarrow M$  if each inequality in the proof is an equality. In particular we need the number of  $K$ -homomorphisms  $K(\alpha_1) \rightarrow M$  to be  $|K(\alpha_1) : K|$ .

But then [Lemma 2.6](#) says we have  $|K(\alpha) : K|$  distinct roots of  $f_\alpha(t)$  in  $M$ . Thus  $f_\alpha(t)$  [splits](#) over  $M$ .

Conversely, suppose  $K \leq M$  is separable and normal. Then for  $K \leq M \leq L$  with  $L$  large enough, separability implies there are  $|M : K|$   $K$ -homomorphisms  $\phi : M \rightarrow L$  by [Lemma 2.12](#). However since  $K \leq M$  is normal, it is the splitting field for some polynomial  $f(t) \in K[t]$  ([Theorem 1.26](#)) and thus  $M = K(\alpha_1, \dots, \alpha_n)$ , where  $f(t) = (t - \alpha_1) \cdots (t - \alpha_n)$ . Note that  $\phi(\alpha_j)$  is also a root of  $\phi(f(t)) = f(t)$  and is therefore one of the  $\alpha_j$ s. Thus  $\phi(M) = M$ . Thus we have  $|M : K|$   $K$ -homomorphisms  $\phi : M \rightarrow M$ .  $\square$

**Remark 2.27.** In the proof we have shown that if  $K \leq M \leq L$  and  $\phi : M \rightarrow L$  is a [K-homomorphism](#) and  $K \leq M$  is [normal](#), then  $\phi(M) = M$ .

**Example.**

- (1)  $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, i)$  is [Galois](#).  $\text{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$  has 4 elements:

$$\begin{aligned}\sigma : \sqrt{2} &\mapsto \pm\sqrt{2} \\ i &\mapsto \pm i\end{aligned}$$

In particular,  $\text{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong C_2 \times C_2$ , all non-identity elements have order 2.

- (2) Consider  $f(t) = t^3 - 2$ . The [splitting field](#) over  $\mathbb{Q}$  is  $\mathbb{Q}(\sqrt[3]{2}, \omega)$ , where  $\omega$  is a primitive cube root of 1.

Thus  $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$  is Galois and  $|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}| = 6$  (we saw this in the example before [Theorem 1.23](#)).

$$\begin{aligned}\sigma_1 : \begin{cases} \sqrt[3]{2} &\mapsto \sqrt[3]{2} \\ \omega &\mapsto \omega \end{cases} & \text{identity} \\ \sigma_2 : \begin{cases} \sqrt[3]{2} &\mapsto \omega \sqrt[3]{2} \\ \omega &\mapsto \omega \end{cases} & \text{order 3} \\ \sigma_3 : \begin{cases} \sqrt[3]{2} &\mapsto \omega^2 \sqrt[3]{2} \\ \omega &\mapsto \omega \end{cases} & \text{order 3} \\ \sigma_4 : \begin{cases} \sqrt[3]{2} &\mapsto \sqrt[3]{2} \\ \omega &\mapsto \omega^2 \end{cases} & \begin{array}{l} \text{complex conjugation} \\ \text{order 2} \end{array} \\ \sigma_5 : \begin{cases} \sqrt[3]{2} &\mapsto \omega^2 \sqrt[3]{2} \\ \omega &\mapsto \omega^2 \end{cases} & \text{order 2} \\ \sigma_6 : \begin{cases} \sqrt[3]{2} &\mapsto \omega \sqrt[3]{2} \\ \omega &\mapsto \omega^2 \end{cases} & \text{order 2}\end{aligned}$$

Observe also  $\sigma_4 \sigma_2 \sigma_4^{-1} = \sigma_3$ , so this is the dihedral group.

### 3 Fundamental Theorem of Galois Theory

#### 3.1 Artin's Theorem

**Definition 3.1** (Fixed field). Let  $K \leq L$  be a [field extension](#) and  $H \leq \text{Aut}_K(L)$ . The **fixed field** of  $H$  is,

$$L^H := \{ \alpha \in L \mid \sigma(\alpha) = \alpha \text{ for all } \sigma \in H \}$$

**Exercise.** Check it is a field and  $K \leq L^H \leq L$ .

**Theorem 3.2** (Fundamental Theorem of Galois Theory). Let  $K \leq L$  be a [finite Galois extension](#). Then

- (i) there is a 1 to 1 correspondence

$$\begin{aligned} \{\text{intermediate subfields } K \leq M \leq L\} &\longleftrightarrow \{\text{subgroups } H \text{ of } \text{Gal}(L/K)\} \\ M &\longmapsto \text{Aut}_M(L) \\ L^H &\longleftarrow H \end{aligned}$$

This is called the Galois correspondence.

- (ii)  $H$  is a normal subgroup of  $\text{Gal}(L/K)$  iff  $K \leq L^H$  is [normal](#) iff  $K \leq L^H$  is [Galois](#).
- (iii) If  $H \triangleleft \text{Gal}(L/K)$  then the map

$$\theta : \text{Gal}(L/K) \longrightarrow \text{Gal}(L^H/K)$$

given by restriction to  $L^H$  is a surjective group homomorphism with kernel  $H$ .

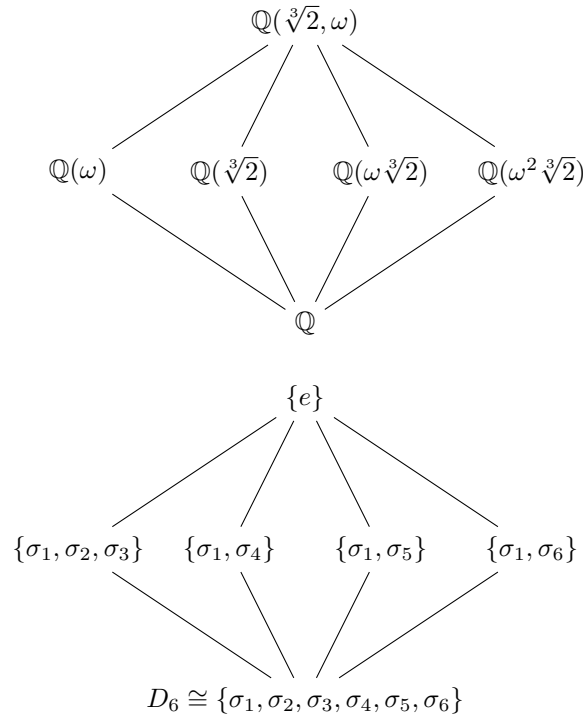
**Remark.**

- (i) Observe that  $M \leq L$  is [Galois](#) and so we could have written  $\text{Gal}(L/M)$  instead of  $\text{Aut}_M(L)$  in (i). To see this: [separability](#) follows from [Lemma 2.15](#). [Normality](#): If  $\alpha \in L$ , the [minimal polynomial](#) of  $\alpha$  over  $M$  divides the minimal polynomial of  $\alpha$  over  $K$ . But the latter splits over  $L$ .
- (ii) If  $K \leq M$  is normal then [Remark 2.27](#) says that if  $\sigma : L \rightarrow L$  then  $\sigma(M) = M$  and so we can talk about the restriction of  $\alpha$  to  $M$  giving an [automorphism](#) of  $M$ .

**Example.**

- (i)  $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, i)$ . We saw in [Section 1](#) the lattice of intermediate fields and subgroups  $\text{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong C_2 \times C_2$  abelian. All subgroups are normal and intermediate subfields are [normal](#) extensions of  $\mathbb{Q}$ .
- (ii)  $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$ :





The subgroup  $H$  of order 3 is normal but those of order 2 are not.

$$\mathbb{Q} \leq \mathbb{Q}(\omega) \text{ is normal} \longleftrightarrow H \text{ of order 3}$$

$$\begin{aligned} \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) &\mapsto \text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \\ D_6 &\mapsto C_2 \end{aligned}$$

This final mapping has kernel  $H$ , and the image is generated by conjugation.

**Theorem 3.3** (Artin's Theorem). Let  $K \leq L$  be a [field extension](#) and  $H$  a finite subgroup of  $\text{Aut}_K(L)$ . Let  $M = L^H$ . Then  $M \leq L$  is a [finite Galois](#) extension, and  $H = \text{Gal}(L/M)$ .

**Remark.** This implies some of the Galois correspondence

$$H \longrightarrow L^H \longrightarrow \text{Gal}(L/L^H)$$

we get back to  $H$ .

*Proof of [Artin's Theorem](#).* Take  $\alpha \in L$ .

**First step:** Show that  $|M(\alpha) : M| \leq |H|$ . Let

$$\underbrace{\{\alpha_1, \dots, \alpha_n\}}_{\text{all distinct}} = \{\phi(\alpha) \mid \phi \in H\}.$$

Define  $g(t) = \prod_{i=1}^n (t - \alpha_i)$ . Each  $\phi$  induces a homomorphism  $L[t] \rightarrow L[t]$  that sends  $g(t)$  to itself, since  $\phi$  is permuting the  $\alpha_i$ . So the coefficients of  $g(t)$  are fixed by all  $\phi \in H$  and thus they all lie in  $L^H = M$ . Thus  $g(t) \in M[t]$ .

By definition,  $g(\alpha) = 0$  since  $\alpha$  is one of the  $\alpha_i$ . Hence the minimal polynomial  $f_\alpha(t)$  of  $\alpha$  over  $M$  divides  $g(t)$ . Thus  $|M(\alpha) : M| = \deg f_\alpha(t) \leq \deg g(t) \leq |H|$ . We've shown that  $\alpha$  is algebraic over  $M$ . Moreover,  $f_\alpha(t)$  is separable since  $g(t)$  is. Thus  $M \leq L$  is a separable extension.

**Next step:** Show that  $M \leq L$  is a simple extension. Pick  $\alpha \in L$  with  $|M(\alpha) : M|$  maximal. We'll show that  $L = M(\alpha)$  for this choice of  $\alpha$ . Suppose  $\beta \in L$ . Then  $M \leq M(\alpha, \beta)$  is finite and is [separably generated](#) and hence is a finite separable extension by [Lemma 2.12](#).

By the [Primitive Element Theorem](#),  $M(\alpha, \beta) = M(\gamma)$  for some  $\gamma$ . But  $M \leq M(\alpha) \leq M(\gamma)$ . The maximality of  $|M(\alpha) : M|$  forces  $M(\alpha) = M(\gamma)$ . Thus  $\beta \in M(\gamma) = M(\alpha)$  and so  $L = M(\alpha)$  so  $|L : M| \leq |H|$ .

**Finally,**

$$|L : M| = |M(\alpha) : M| \leq |H| \leq |\text{Aut}_M(L)| \leq |L : M|$$

$\uparrow$   
[Lemma 2.23](#)

We must have equality throughout, and so  $|L : M| = |\text{Aut}_M(L)| = |H|$ . Hence by [Theorem 2.24](#) we have  $M \leq L$  is a finite Galois extension and  $H = \text{Gal}(L/M)$ .  $\square$

**Theorem 3.4.** Let  $K \leq L$  be a [finite field extension](#). Then the following are equivalent:

- (i)  $K \leq L$  is [Galois](#)
- (ii)  $L^H = K$  when  $H = \text{Aut}_K(L)$

**Remark.** The theorem allows some authors yet another alternative definition of a 'Galois extension'.

*Proof. (i)  $\Rightarrow$  (ii):* Let  $M = L^H$  where  $H = \text{Aut}_K(L)$ . By [Artin's Theorem](#),  $M \leq L$  is a Galois extension, and  $|L : M| = |\text{Gal}(L/M)|$  and  $H = \text{Gal}(L/M)$ .

However if  $K \leq L$  is Galois then  $|H| = |\text{Aut}_K(L)| = |L : K|$  by [Theorem 2.24](#). Thus  $|L : M| = |L : K|$  and so  $M = K$ .

**(ii)  $\Leftarrow$  (i):** Use [Theorem 3.3](#).  $\square$

*Proof of Fundamental Theorem of Galois Theory.*

- (i) Composing the maps  $H \rightarrow L^H$  and  $M \rightarrow \text{Gal}(L/M)$  gives  $H \rightarrow H$  by [Theorem 3.3](#). Also  $M \rightarrow \text{Gal}(L/M) \rightarrow L^H$  where  $H = \text{Gal}(L/M)$  yields  $M$  since  $M \leq L^H$  where  $H = \text{Gal}(L/M)$  and

$$|L : L^H| \underset{(2.24)}{=} |H| = |\text{Gal}(L/M)| \underset{(2.24)}{=} |L : M|$$

$\underset{(3.3)}{=}$

So  $M = L^H$ .

- (ii) Take  $H \leq \text{Gal}(L/K)$ , then  $L^{\phi H \phi^{-1}} = \phi(L^H)$  when  $\phi \in \text{Gal}(L/K)$ . So by (i),  $H$  is [normal](#) iff  $\phi(L^H) = L^H$ . Set  $M = L^H$ .

We'll show that  $K \leq M$  is normal iff  $\phi(M) = M \quad \forall \phi \in \text{Gal}(L/K)$ .  $K \leq M$  is normal  $\implies \phi(M) = M$  by remark 2 after the statement of [Fundamental Theorem of Galois Theory](#).

Conversely if  $\phi(M) = M \quad \forall \phi \in \text{Gal}(L/K)$ , pick  $\alpha \in M$  and let  $f_\alpha(t)$  be its minimal polynomial over  $K$ . Take  $\beta$  to be a root of  $f_\alpha(t)$  in  $L$  (possible by normality). Then there is a  $K$ -homomorphism

$$K(\alpha) \cong \frac{K[t]}{(f_\alpha(t))} \rightarrow K(\beta) \cong \frac{K[t]}{(f_\alpha(t))} \leq L$$

$$\alpha \longmapsto \beta.$$

This extends to a  $K$ -homomorphism  $\phi : L \rightarrow L$ .

However we are assuming  $\phi(M) = M$  and so  $\phi(\alpha) = \beta \in M$ . Thus  $K \leq M$  is normal. Note that  $K \leq L^H$  is [separable](#) since  $K \leq L^H \leq L$  and  $K \leq L$  separable.

(iii) By remark 2 after statement of [Theorem 3.2](#), the restriction map

$$\theta : \text{Gal}(L/K) \rightarrow \text{Gal}(L^H/K)$$

is defined. Surjectivity follows from being able to extend a  $K$ -homomorphism  $L^H \rightarrow L^H \leq L$  to a  $K$ -homomorphism  $L \rightarrow L$  by [Corollary 2.10](#). Clearly  $H \leq \text{Ker } \theta$ . However

$$\begin{aligned} \frac{|L : K|}{|\text{Ker } \theta|} &= \frac{|\text{Gal}(L/K)|}{|\text{Ker } \theta|} \\ &= |\text{Gal}(L^H/K)| \quad \text{by surjectivity of } \theta \\ &= |L^H : K| \quad \text{since } K \leq L^H \text{ is Galois} \\ &= \frac{|L : K|}{|L : L^H|} \quad \text{by Tower law} \end{aligned}$$

So  $|\text{Ker } \theta| = |L : L^H| = |\text{Gal}(L/L^H)| = |H|$  by [Theorem 3.3](#), so  $H = \text{Ker } \theta$ . □

### 3.2 Galois groups of polynomials

**Definition 3.5** (Galois group of polynomial). Let  $f(t)$  be a [separable](#) polynomial  $\in K[t]$  and let  $K \leq L$  with  $L$  a [splitting field](#) for  $f(t)$ . Then the **Galois group of  $f(t)$**  over  $K$  is

$$\text{Gal}(f) := \text{Gal}(L/K).$$

Since  $L$  is a splitting field for  $f(t)$ ,  $L = K(\alpha_1, \dots, \alpha_n)$  where  $\alpha_1, \dots, \alpha_n$  are the roots of  $f(t)$  in  $L$ . Observe that if  $\phi \in \text{Gal}(L/K)$  it maps

$$\{\text{roots of } f(t)\} \longrightarrow \{\text{roots of } f(t)\}$$

Thus  $\phi$  permutes the  $\alpha_i$ . Moreover, if  $\phi$  fixes each  $\alpha_i$ , it also fixes all elements of  $L$ , and so is the identity map. Thus  $\text{Gal}(f)$  may be regarded as a permutation group of the  $n$  roots, so  $\text{Gal}(f) \leq S_n$ .

**Lemma 3.6.** Suppose  $f(t)$  is [separable](#),  $f(t) = g_1(t) \cdots g_s(t)$  with  $g_i(t)$  irreducible in  $K[t]$  is a factorisation in  $K[t]$ . Then the orbits of  $\text{Gal}(f)$  on the roots of  $f(t)$  correspond to the factors  $g_j(t)$ .

Two roots are in the same orbit  $\iff$  they are roots of the same  $g_j(t)$ .

In particular, if  $f(t)$  is irreducible in  $K[t]$  there is one orbit, i.e.,  $\text{Gal}(f)$  acts transitively on the roots of  $f(t)$ .

*Proof.* Let  $\alpha_k, \alpha_l$  be in the same orbit under  $\text{Gal}(f)$ . Thus there is  $\phi \in \text{Gal}(f)$  with  $\alpha_l = \phi(\alpha_k)$ . But if  $\alpha_k$  is a root of  $g_j(t)$  then  $\phi(\alpha_k) = \alpha_l$  is also a root of  $g_j(t)$ .

Conversely, if  $\alpha_k, \alpha_l$  are roots of  $g_j(t)$  then

$$K(\alpha_k) \cong \frac{K[t]}{(g_j(t))} \cong K(\alpha_l) \leq L$$

$\phi_0$

with  $\phi_0(\alpha_k) = \alpha_l$ .  $\phi_0$  extends to a  $\phi : L \rightarrow L \in \text{Gal}(L/K)$ , thus  $\alpha_k, \alpha_l$  are in the same orbit.  $\square$

Since the Galois group of an irreducible polynomial acts transitively, and is a subgroup of  $S_n$ , it is useful to know what the transitive subgroups of  $S_n$  are.

**Lemma 3.7.** The transitive subgroups of  $S_n$  for  $n \leq 5$  are

$$\begin{aligned} n = 2: & \quad S_2 (\cong C_2) \\ n = 3: & \quad A_3 (\cong C_3), S_3 \\ n = 4: & \quad C_4, V_4, D_8, A_4, S_4 \\ n = 5: & \quad C_5, D_{10}, H_{20}, A_5, S_5 \end{aligned}$$

where  $H_{20}$  is generated by a 5-cycle and a 4-cycle.

*Proof.* Exercise.  $\square$

**Theorem 3.8.** Let  $p$  be a prime, and  $f(t)$  irreducible  $\in \mathbb{Q}[t]$  of degree  $p$ . Suppose  $f(t)$  has exactly 2 non-real roots in  $\mathbb{C}$ . Then  $\text{Gal}(f)$  over  $\mathbb{Q} \cong S_p$ .

*Proof.*  $\text{Gal}(f)$  acts on the  $p$  distinct roots of  $f(t)$  in a [splitting field](#)  $L$  of  $f(t)$  (in  $\mathbb{C}$ ). By [Lemma 3.6](#), the irreducibility of  $f(t)$  implies that  $\text{Gal}(f)$  is acting transitively on the  $p$  roots. By the orbit-stabiliser theorem,  $p \mid |\text{Gal}(f)|$  but  $|\text{Gal}(f)| \leq |S_p| = p!$  and so  $\text{Gal}(f)$  has a Sylow  $p$ -subgroup of order  $p$ , necessarily cyclic. Thus,  $\text{Gal}(f)$  contains a  $p$ -cycle.

The supposition that we have precisely 2 non-real roots gives that complex conjugation yields a transposition in  $\text{Gal}(f)$ . The  $p$ -cycle and transposition generate the whole of  $S_p$ .  $\square$

**Example 3.9.** Consider  $f(t) = t^5 - 6t + 3 \in \mathbb{Q}[t]$ . Then  $\text{Gal}(f) \cong S_5$ .

*Proof.*  $f(t)$  is irreducible by [Eisenstein's criterion](#) with  $p = 3$ . We want to show that  $f(t)$  has three real roots, two non-real ones and apply [Theorem 3.8](#).

$$f(-2) = -17, f(-1) = 8, f(1) = -2, f(2) = 23$$

and  $f'(t) = 5t^4 - 6$  which has two real roots. From the intermediate value theorem,  $f$  has at least three real roots, and by Rolle's theorem there are at most three real roots, so we are done.  $\square$

**Definition 3.10** (Discriminant). Let  $f(t) \in K[t]$  with distinct roots  $\alpha_1, \dots, \alpha_n$  in a splitting field (with  $f(t)$  not necessarily irreducible). Let

$$\Delta = \prod_{i < j} (\alpha_i - \alpha_j).$$

Then the **discriminant**  $D = D(f)$  of  $f$  is

$$\begin{aligned} D = \Delta^2 &= \prod_{i < j} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j). \end{aligned}$$

**Remark.** We've already met this in the proof of [Theorem 2.21](#).

**Lemma 3.11.** Let  $f(t)$  be [separable](#)  $\in K[t]$  of degree  $n$  with  $\text{char } K \neq 2$ . Then

$$\text{Gal}(f) \leq A_n \iff D(f) \text{ is a square in } K.$$

*Proof.* Let  $L$  be a [splitting field](#) of  $f(t)$  over  $K$ . Then  $D(f) \neq 0$  and is fixed by all elements of  $G = \text{Gal}(L/K)$  as the latter permutes the roots. Thus  $D \in K$ , since  $L^G = K$  (by Galois correspondence).

On the other hand, if  $\sigma \in G$  then  $\sigma(\Delta) = (\text{sgn } \sigma)\Delta$  where we're regarding  $G$  as a subgroup of  $S_n$  and the signature of  $\sigma$ :

$$\text{sgn } \sigma = \begin{cases} +1 & \text{if } \sigma \text{ even} \\ -1 & \text{if } \sigma \text{ odd} \end{cases}$$

(This is where we need  $\text{char } K \neq 2$ ).

Thus if  $G \leq A_n$  we get that  $\Delta$  is fixed by all  $\sigma \in G$ . Thus  $\Delta \in K = L^G$ . Otherwise if  $G \not\leq A_n$ , we get  $\sigma(\Delta) = -\Delta$  if  $\sigma$  is an odd permutation, and so  $\Delta \notin K = L^G$ . Note that if  $D$  does have square roots, they must be  $\pm\Delta$ .  $\square$

**Example 3.12.** For  $n = 2$ , take  $f(t) = t^2 + bt + c$ . Then  $D(f) = b^2 - 4c$ .

For  $n = 3$ , consider  $f(t) = t^3 + ct + d$ . Then we can check that  $D(f) = -4c^3 - 27d^2$ . Any general monic cubic can be written in the above form by suitable substitutions.

Take  $f(t) = t^3 - t - 1 \in \mathbb{Q}[t]$ .  $f$  is irreducible since it is irreducible in  $\mathbb{Z}[t]$  since it is irreducible mod 2.  $D(f) = -23$ , which is not a square in  $\mathbb{Q}$ , so  $\text{Gal}(f) \cong S_3$ .

$f(t) = t^3 - 3t - 1 \in \mathbb{Q}[t]$  is irreducible since it is irreducible mod 2. Now  $D(f) = 81$ , so  $\text{Gal}(f) \cong A_3$ .

For irreducible quartics, we saw that the possible [Galois groups](#) are  $C_4, V_4, D_8, A_4, S_4$ . Those that are subgroups of  $A_4$  are  $V_4$  and  $A_4$ . From looking at the discriminant, one gets information as to whether the group is one of  $V_4, A_4$  or is  $C_4, D_8, S_4$ . We need further methods to pin down which group we are dealing with.

**Theorem 3.13** (Mod  $p$  reduction). Let  $f(t) \in \mathbb{Z}[t]$  be monic of degree  $n$  with  $n$  distinct roots in a [splitting field](#). Let  $p$  be a prime such that  $\bar{f}(t)$ , the reduction of  $f(t) \bmod p$  also has  $n$  distinct roots in a splitting field. Let  $\bar{f}(t) = \bar{g}_1(t) \cdots \bar{g}_s(t)$  be the factorisation into irreducibles in  $\mathbb{F}_p[t]$  with  $n_j = \deg \bar{g}_j(t)$ . Then  $\text{Gal}(\bar{f}) \hookrightarrow \text{Gal}(f)$  and has an element of cycle type  $(n_1, n_2, \dots, n_s)$ .

*Proof.* We will talk about the last sentence after thinking about Galois groups of finite fields. The fact that  $\text{Gal}(\bar{f}) \hookrightarrow \text{Gal}(f)$  is from Number Fields - see Tony Scholl's teaching page on Galois.  $\square$

**Example 3.14.** For  $f(t) = t^4 + dt + e$ , we have  $D(f) = -27d^4 + 256e^3$ , not proved here. Consider  $f(t) = t^4 - t - 1$ , which is irreducible since it is irreducible mod 2. Then  $D(f) = -283$ , which is not a square in  $\mathbb{Q}$ .

Now take  $p = 7$ .

$$\begin{aligned}\bar{f}(t) &= t^4 - t - 1 \\ &= (t + 4)(t^3 + 3t^2 + 2t + 5) \pmod{7}\end{aligned}$$

and the latter factor is irreducible over  $\mathbb{F}_7$  as it is a cubic which has no roots in  $\mathbb{F}_7$ .

By [Theorem 3.13](#),  $\text{Gal}(f)$  contains an element of cycle type  $(1, 3)$ , i.e. a 3-cycle. We deduce  $\text{Gal}(f) \cong S_4$ , as the other possibilities that contain an odd permutation do not contain 3-cycles.

### 3.3 Galois Theory of Finite Fields

Recall what we already know from [Section 1](#). From [Example 1.27](#), a finite field  $\mathbb{F}$  is of characteristic  $p > 0$ ,  $p$  necessarily prime, and  $|\mathbb{F}| = p^r$  for some  $r$ . The multiplicative group of  $\mathbb{F}$  is cyclic ([Theorem 1.28](#)). It is a splitting field for  $t^n - 1$  over  $\mathbb{F}_p$  where  $n = p^r - 1$ . By the [Uniqueness of splitting fields](#), this is unique. Observe we could also describe  $\mathbb{F}$  as the splitting field of  $t^{p^r} - t$  over  $\mathbb{F}_p$ . What we haven't shown yet is that for any  $p^r$ , there is a field  $\mathbb{F}$  with  $|\mathbb{F}| = p^r$ .

**Definition 3.15** (Frobenius automorphism). Let  $\mathbb{F}$  be a finite field of characteristic  $p$ . Then the **Frobenius automorphism** of  $\mathbb{F}$  is

$$\begin{aligned}\phi : \mathbb{F} &\longrightarrow \mathbb{F} \\ \alpha &\longmapsto \alpha^p.\end{aligned}$$

**Remark.**

- (i)  $(\alpha + \beta)^p = \alpha^p + \beta^p$  since all other terms in binomial expansion are divisible by  $p$ .
- (ii)  $\mathbb{F}_p$  is fixed under this, so it is an  $\mathbb{F}_p$ -automorphism. Since  $t^{p^r}$  splits as a product of distinct linear factors  $(t - \alpha)$  in  $\mathbb{F}$ , we have that  $\mathbb{F}_p \leq \mathbb{F}$  is a [Galois extension](#) and so we consider  $\text{Gal}(\mathbb{F}/\mathbb{F}_p) = G$ . It is of order  $r$  since  $|\mathbb{F} : \mathbb{F}_p| = r$ .

**Theorem 3.16** (Galois groups of finite fields). Let  $\mathbb{F}$  be a finite field with  $|\mathbb{F}| = p^r$ . Then  $\mathbb{F}_p \leq \mathbb{F}$  is a [Galois extension](#) with  $\text{Gal}(\mathbb{F}/\mathbb{F}_p) = G$ , a cyclic group with the [Frobenius automorphism](#) as generator.

*Proof.* It remains to show that the order of the [Frobenius automorphism](#) is  $r$ . Suppose  $\phi^s = \text{id}$ . Then  $\alpha^{p^s} = \alpha \forall \alpha \in \mathbb{F}$ . But  $t^{p^s} - t$  has at most  $p^s$  roots in  $\mathbb{F}$ , so we deduce that  $s \geq r$ . Observe that  $\phi^r = \text{id}$  since  $\alpha^{p^r} = \alpha, \forall \alpha \in \mathbb{F}$ .  $\square$

Now apply the [Fundamental Theorem of Galois Theory](#):

$$\{\mathbb{F}_p \leq M \leq \mathbb{F} \text{ intermediate fields } M\} \longleftrightarrow \{\text{subgroups } H \leq G\}$$

where  $G = \text{Gal}(\mathbb{F}/\mathbb{F}_p)$  is cyclic.

But we know all about subgroups of a cyclic group with generator  $\phi$  of order  $r$ . There is exactly one subgroup of order  $s$  for each  $s \mid r$  generated by  $\phi^{\frac{r}{s}}$ . The corresponding

intermediate subfields are the fixed fields  $\mathbb{F}^{\langle \phi^{\frac{r}{s}} \rangle}$ , and  $|\mathbb{F} : \mathbb{F}^{\langle \phi^{\frac{r}{s}} \rangle}| = s$ . By the Tower Law,  $|\mathbb{F}^{\langle \phi^{\frac{r}{s}} \rangle} : \mathbb{F}_p| = \frac{r}{s}$ . Observe that all subgroups of cyclic groups are normal and therefore all our intermediate fields are **normal extensions** of  $\mathbb{F}_p$ .

By [Theorem 3.2](#) part (iii),  $\text{Gal}(\mathbb{F}^{\langle \phi^{\frac{r}{s}} \rangle} / \mathbb{F}_p) \cong \text{Gal}(\mathbb{F} / \mathbb{F}_p) / H$  where  $H = \langle \phi^{\frac{r}{s}} \rangle$ .

**Corollary 3.17.** Let  $\mathbb{F}_p \leq M \leq \mathbb{F}$  be finite fields. Then  $\text{Gal}(\mathbb{F} / M)$  is cyclic, generated by  $\phi^u$ , where  $\phi$  is the **Frobenius automorphism** and  $|M| = p^u$  and  $M$  is the **fixed field** of  $\langle \phi^u \rangle$ .

*Proof.* Set  $n = \frac{r}{s}$ . □

**Theorem 3.18** (Existence of finite fields). Let  $p$  be a prime and  $u \geq 1$ . Then there is a field of order  $p^u$ , unique up to isomorphism.

*Proof.* Consider the splitting field  $L$  of  $f(t) = t^{p^u} - t$  over  $\mathbb{F}_p$ . It is a finite Galois extension  $\mathbb{F}_p \leq L$ . However the roots of  $f(t)$  form a field, the fixed field of  $\phi^u$ . Set  $L = \mathbb{F}$  and  $|\mathbb{F} : \mathbb{F}_p| = u$ . □

**Remark** (About [Theorem 3.13](#)). We'll discover in Number Fields that  $\text{Gal}(\bar{f}) \hookrightarrow \text{Gal}(f)$  if  $f(t) \in \mathbb{Z}[t]$ . We factorised  $\bar{f}(t) = \bar{g}_1(t) \cdots \bar{g}_s(t)$ , a product of irreducibles. We know from [Lemma 3.6](#) that the orbits of  $\text{Gal}(\bar{f})$  correspond to the factorsiation.

We now know  $\text{Gal}(\bar{f})$  is cyclic generated by the Frobenius map, which must have cycle type  $(n_1, \dots, n_s)$  where  $n_j = \deg \bar{g}_j(t)$

## 4 Cyclotomic and Kummer extensions

### 4.1 Cyclotomic extensions

**Definition 4.1** (Cyclotomic extension). Suppose  $\text{char } K = 0$  or  $p$  prime where  $p \nmid m$ . The  $m$ th **cyclotomic extension** of  $K$  is the **splitting field**  $L$  of  $t^m - 1$ .

**Remark.**  $f(t) = t^m - 1$  and  $f'(t) = mt^{m-1}$  have no common roots, and so the roots of  $f(t)$  are distinct, the  $m$ th roots of unity. They form a finite subgroup  $\mu_m$  of  $L^\times$ , and hence by [Theorem 1.28](#) a cyclic group  $\langle \xi \rangle$ . Thus,  $L = K(\xi)$  is a **simple extension**.

**Definition 4.2** (Primitive  $m$ th root of unity). An element  $\xi \in \mu_m$  is a **primitive  $m$ th root of unity** if  $\mu_m = \langle \xi \rangle$ .

Choosing a **primitive  $m$ th root of unity** determines  $\mu_m \rightarrow \mathbb{Z}/m\mathbb{Z}$  an isomorphism. Note that  $\xi^i$  is a generator of  $\mu_m$  iff  $(i, m) = 1$  and so the primitive  $m$ th roots of unity correspond to elements of  $(\mathbb{Z}/m\mathbb{Z})^\times$ .

Now consider **Galois groups of cyclotomic extensions**: we'll see they must be abelian. Observe  $f(t) = t^m - 1$  is **separable** and so the **extension**  $K \leq L$  is **Galois**. Let  $G = \text{Gal}(L/K)$ . An element  $\sigma \in G$  sends a primitive  $m$ th root of unity  $\xi$  to a primitive  $m$ th root of unity  $\xi^i$  where  $(i, m) = 1$ . Then  $\xi \mapsto \xi^i$  determines a  **$K$ -homomorphism**  $K^L(\xi) \rightarrow K^L(\xi)$  with  $\xi \mapsto \xi^i$ . Thus we get an injective map:

**Definition 4.3** (Group of roots of unity).

$$\theta : G \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$$

This is a group homomorphism: If  $\sigma(\xi) = \xi^c, \phi(\xi) = \xi^j$  then  $(\sigma\phi)(\xi) = \sigma(\xi^j) = \xi^{cj}$ . Hence  $G$  is abelian.

Thus we regard  $G$  as a subgroup of  $(\mathbb{Z}/m\mathbb{Z})^\times$ .

**Definition 4.4** (Cyclotomic polynomial). The  $m$ th **cyclotomic polynomial** is

$$\Phi_m(t) = \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} (t - \xi^i),$$

the product of the linear factors of  $t^m - 1$  corresponding to the **primitive  $m$ th roots of unity**.

**Remark.**

$$f(t) = t^m - 1 = \prod_{i \in \mathbb{Z}/m\mathbb{Z}} (t - \xi^i) = \prod_{d|m} \Phi_d(t).$$

**Example.** Take  $K = \mathbb{Q}$ .

$$\Phi_1(t) = t - 1, \Phi_2(t) = t + 1, \Phi_3(t) = t^2 + t + 1, \Phi_4(t) = t^2 + 1, \Phi_8(t) = t^4 + 1$$

since  $t^8 - 1 = (t - 1)(t + 1)(t^2 + 1)(t^4 + 1)$ .

**Lemma 4.5.**  $\Phi_m(t) \in \mathbb{Z}[t]$  if  $\text{char } K = 0$  (with  $\mathbb{Q} \hookrightarrow K$ , prime subfield).  $\Phi_m(t) \in \mathbb{F}_p[t]$  if  $\text{char } K = p$  (with  $\mathbb{F}_p \hookrightarrow K$ , prime subfield).



*Proof.* Induct on  $m$ .  $m = 1$  is clearly true.

For  $m > 1$ , consider

$$f(t) = t^m - 1 = \Phi_m(t) \left( \prod_{\substack{d|m \\ d \neq m}} \Phi_d(t) \right).$$

Note that  $\prod_{\substack{d|m \\ d \neq m}} \Phi_d(t)$  is monic and is defined in  $\mathbb{Z}[t]$  or  $\mathbb{F}_p[t]$  by induction.

If  $\text{char } K = 0$ , we deduce  $\Phi_m(t) \in \mathbb{Q}[t]$  by division of polynomials and by Gauss' Lemma it is in  $\mathbb{Z}[t]$ . If  $\text{char } K = p > 0$ , we deduce by division that  $\Phi_m(t) \in \mathbb{F}_p[t]$ .  $\square$

**Lemma 4.6.** The homomorphism  $\theta : G \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times$  defined in [Definition 4.3](#) is an isomorphism iff  $\Phi_m(t)$  is irreducible.

*Proof.* We know from [Lemma 3.6](#) that the orbits of  $G = \text{Gal}(L/K)$  correspond to the factorisation of  $f(t)$  in  $K[t]$ . In particular, the [primitive  \$m\$ th roots of unity](#) form one orbit iff  $\Phi_m(t)$  is irreducible. Then  $\theta$  is surjective iff  $\Phi_m(t)$  is irreducible.  $\square$

**Theorem 4.7.** Let  $L$  be the  [\$m\$ th cyclotomic extension](#) of finite field  $\mathbb{F} = \mathbb{F}_q$  where  $q = p^n$ . Then the Galois group  $G = \text{Gal}(L/\mathbb{F})$  is isomorphic to the cyclic subgroup of  $(\mathbb{Z}/m\mathbb{Z})^\times$  generated by  $q$ .

*Proof.* We know from [Corollary 3.17](#) that  $G$  is generated by  $\alpha \mapsto \alpha^{p^n} = \alpha^q$  so  $\theta(G) = \langle q \rangle \leq (\mathbb{Z}/m\mathbb{Z})^\times$ .  $\square$

**Remark.** Thus if  $(\mathbb{Z}/m\mathbb{Z})^\times$  is not cyclic then  $\theta$  is not surjective for any finite field  $\mathbb{F}$  and  $\Phi_m(t)$  is reducible over  $\mathbb{F}$ .

**Example.** Take  $\mathbb{F} = \mathbb{F}_3$ , then  $\Phi_8(t) = t^4 + 1 = (t^2 + t - 1)(t^2 - t - 1)$ .  $t^8 - 1$  factorises as a product of linear and quadratic polynomials mod 3, so the splitting field  $L = \mathbb{F}_9$  is the unique field of order 9 whose multiplicative group is cyclic  $C_8$ .

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\} \cong C_2 \times C_2$$

We have  $|L : \mathbb{F}_3| = 2$ , so  $|\text{Gal}(L/\mathbb{F}_3)| = 2$  hence  $\text{Gal}(L/\mathbb{F}_3)$  cyclic order 2, so  $\theta$  is not surjective.

What happens when  $K = \mathbb{Q}$ ?

**Theorem 4.8.** For all  $m > 0$ ,  $\Phi_m(t)$  is irreducible in  $\mathbb{Z}[t]$  and hence in  $\mathbb{Q}[t]$ . Thus  $\theta$  in [Definition 4.3](#) is an isomorphism and thus  $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$  where  $\xi$  = primitive  $m$ th root of unity.

**Remark.** We already know this when  $m = p$  prime by substitution and [Eisenstein's criterion](#).

*Proof of Theorem 4.8.* Gauss' Lemma gives us that irreducibility in  $\mathbb{Z}[t]$  implies irreducibility in  $\mathbb{Q}[t]$ . From [Lemma 4.5](#), irreducibility corresponds to surjectivity of  $\theta$ . It's left to show that  $\Phi_m(t)$  is irreducible in  $\mathbb{Z}[t]$ .

Suppose not, and  $\Phi_m(t) = g(t)h(t)$  in  $\mathbb{Z}[t]$  with  $g(t)$  irreducible, monic and  $\deg g(t) \leq \deg \Phi_m(t)$ . Let  $\mathbb{Q} \leq L$  be the  $m$ th cyclotomic extension and  $\xi$  be a root of  $g(t)$ ,  $\xi$  primitive  $m$ th root of unity.

**Claim:** if  $p \nmid m$ ,  $p$  prime, then  $\xi^p$  is also a root of  $g(t)$  in  $L$ . Suppose not. Then  $\xi^p$  is also a primitive  $m$ th root of 1, since  $p \nmid m$ , as a root of  $\Phi_m(t)$ . By the supposition,  $\xi^p$  is a root of  $h(t)$ . Define  $r(t) = h(t^p)$ . Then  $r(\xi) = 0$  but  $g(t)$  is the minimal polynomial of  $\xi$  over  $\mathbb{Q}$ . So  $g(t) \mid r(t)$  in  $\mathbb{Q}[t]$ .

By Gauss' Lemma,  $r(t) = g(t)s(t)$  with  $s(t) \in \mathbb{Z}[t]$ . Now reduce mod  $p$ .  $\bar{r}(t) = \bar{g}(t)\bar{s}(t)$ . But  $\bar{r}(t) = \bar{h}(t^p) = (\bar{h}(t))^p$ . If  $\bar{a}(t)$  is any irreducible factor of  $\bar{g}(t)$  in  $\mathbb{F}_p[t]$  then  $\bar{a}(t) \mid (\bar{h}(t))^p$  and so  $\bar{a}(t) \mid \bar{h}(t)$ . But then  $(\bar{a}(t))^2 \mid \bar{g}(t)\bar{h}(t) = \bar{\Phi}_m(t)$ . Hence  $\bar{\Phi}_m(t)$  has a repeated root and thus  $t^m - 1$  has repeated root mod  $p$ . Contradiction, since  $p \nmid m$ , so claim is true.

Now consider a root  $\gamma$  of  $h(t)$ . Then it is also a primitive root of 1 and so  $\gamma = \xi^i$  for some  $i$  with  $(i, m) = 1$ . Write  $i = p_1 \cdots p_k$  factorisation with  $p_j$  prime, not necessarily distinct,  $p_j \nmid m$ . Applying the claim repeatedly we get that  $\gamma$  is a root of  $g(t)$ , and so  $\Phi_m(t)$  has a repeated root.

Hence  $\Phi_m(t)$  is irreducible over  $\mathbb{Q}$ . □

**Definition 4.9** (Cyclic, abelian extension). An extension  $K \leq L$  is **cyclic** if the extension is **Galois** and  $\text{Gal}(L/K)$  is cyclic. Similarly, it is called **abelian** if  $\text{Gal}(L/K)$  is abelian.

**Example.** In [Corollary 3.17](#) we saw that for finite fields  $\mathbb{F} \leq L$  is **cyclic** and from [Definition 4.3](#) cyclotomic extensions are abelian. However [Theorem 4.8](#) says that  $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$  and so if  $m = 8$ ,  $\mathbb{Q} \leq \mathbb{Q}(\xi)$  is an abelian, non-cyclic extension, where  $\xi$  primitive 8th root of unity.

## 4.2 Kummer Theory

We consider **Galois** extensions  $K \leq L$  where  $L$  is a **splitting field** of a polynomial of the form  $t^m - \lambda$  with  $\lambda \in K$ .

**Theorem 4.10.** Let  $f(t) = t^m - \lambda \in K[t]$  and  $\text{char } K \nmid m$ . Then the **splitting field**  $L$  of  $f(t)$  over  $K$  contains a **primitive  $m$ th root of unity**  $\xi$  and  $\text{Gal}(L/K(\xi))$  is cyclic of order dividing  $m$ . Moreover  $f(t)$  is irreducible over  $K(\xi)$  iff  $|L : K(\xi)| = m$ .

**Remark.**

$$\begin{array}{ccc}
 L & & \{e\} \\
 \downarrow & & \downarrow \text{cyclic} \\
 K(\xi) & & \text{Gal}(L/K(\xi)) \\
 \downarrow & & \downarrow \text{abelian} \\
 K & & \text{Gal}(L/K)
 \end{array}$$

As  $\text{Gal}(L/K(\xi))$  is cyclic,  $\text{Gal}(L/K(\xi)) \triangleleft \text{Gal}(L/K)$ .

By [Theorem 3.2](#) part (iii),  $\text{Gal}(L/K)/\text{Gal}(L/K(\xi)) \cong \text{Gal}(K(\xi)/K)$  is abelian.

*Proof of Theorem 4.10.* Since  $t^m - \lambda$  and  $mt^{m-1}$  are coprime, we know that  $t^m - \lambda$  has distinct roots  $\alpha_1, \dots, \alpha_m$  in the splitting field  $L$ . Since  $(\alpha_i \alpha_j^{-1})^m = \lambda \lambda^{-1} = 1$ , the elements  $1 = \alpha_1 \alpha_1^{-1}, \alpha_2 \alpha_1^{-1}, \dots, \alpha_m \alpha_1^{-1}$  are  $m$  distinct  $m$ th roots of unity in  $L$  and so

$$t^m - \lambda = (t - \beta)(t - \xi\beta)(t - \xi^2\beta) \cdots (t - \xi^{m-1}\beta) \in L[t]$$

where  $\beta = \alpha_1$  and  $\xi$  primitive  $m$ th root of unity.

So  $L = K(\xi, \beta)$ . Let  $\sigma \in \text{Gal}(L/K(\xi))$ , which is determined by its action on  $\beta$ . Note that  $\sigma(\beta)$  is another root of  $t^m - \lambda$  and so  $\sigma(\beta) = \xi^{j(\sigma)}\beta$ , where  $0 \leq j(\sigma) < m$ . Also, if  $\sigma, \tau \in \text{Gal}(L/K(\xi))$  then

$$\tau\sigma(\beta) = \tau(\xi^{j(\sigma)}\beta) = \xi^{j(\sigma)}\tau(\beta) = \xi^{j(\sigma)}\xi^{j(\tau)}\beta$$

since  $\xi$  is fixed by  $\tau$ . Thus  $\sigma \rightarrow j(\sigma)$  gives a group homomorphism

$$\theta : \text{Gal}(L/K(\xi)) \rightarrow \mathbb{Z}/m\mathbb{Z}.$$

Note that  $j(\sigma) = 1$ , only if  $\sigma$  is the identity and so  $\theta$  is injective. Hence  $\text{Gal}(L/K(\xi)) \cong$  subgroup of  $\mathbb{Z}/m\mathbb{Z}$ . Finally  $|L : K(\xi)| = |\text{Gal}(L/K(\xi))| \leq m$  with equality exactly when the action of  $\text{Gal}(L/K(\xi))$  is transitive on the roots, i.e. when  $t^m - 1$  is irreducible over  $K(\xi)$  by [Lemma 3.6](#).  $\square$

**Example.** Consider  $f(t) = t^6 + 3$ . If  $\xi$  is a primitive 6th root of unity,  $\xi = -\omega$ , with  $\omega$  a primitive cube root of 1.

$$\mathbb{Q}(\xi) = \mathbb{Q}(\omega) = \mathbb{Q}\left(\frac{1}{2}(1 + \sqrt{-3})\right) = \mathbb{Q}(\sqrt{-3})$$

$f(t)$  is irreducible over  $\mathbb{Q}$  by [Eisenstein's criterion](#) with  $p = 3$ . However over  $\mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{-3})$  it factorises as

$$f(t) = (t^3 - \sqrt{-3})(t^3 + \sqrt{-3})$$

Let  $L$  be the splitting field of  $f(t)$ . From [Theorem 4.10](#) since  $f(t)$  factorises over  $K(\xi)$ ,  $\text{Gal}(L/K(\xi)) \leq \mathbb{Z}/6\mathbb{Z}$ .

$$\begin{array}{ccc} L & & \{e\} \\ 3 \downarrow & & \downarrow 3 \\ \mathbb{Q}(\xi) & & \text{Gal}(L/\mathbb{Q}(\xi)) \\ 2 \downarrow & & \downarrow 2 \\ \mathbb{Q} & & \text{Gal}(L/\mathbb{Q}) \end{array}$$

$\text{Gal}(L/\mathbb{Q})$  is dihedral of order 6, and  $\text{Gal}(L/\mathbb{Q}(\xi)) \hookrightarrow \mathbb{Z}/6\mathbb{Z}$  is cyclic of order 3. The element of order 2 is given by complex conjugation. Take  $\beta$  a root of  $f(t)$ . Then, the roots are

$$\begin{array}{cccccc} \beta & \xi\beta & \xi^2\beta & \xi^3\beta & \xi^4\beta & \xi^5\beta \\ | & | & | & | & | & | \\ \beta & & \omega^2\beta & & \omega\beta & \\ & -\omega\beta & & -\beta & & \omega^2\beta \end{array}$$

A 3-cycle is given by permuting  $\beta, \omega^2\beta, \omega\beta$ . Conjugating by complex conjugation yields the inverse of the 3-cycle - a dihedral relation.

We have a converse of [Theorem 4.10](#):

**Theorem 4.11.** Suppose  $K \leq M$  is a [cyclic extension](#) with  $|L : K| = m$ , where  $\text{char } K \nmid m$  and that  $K$  contains a [primitive  \$m\$ th root of unity](#). Then  $\exists \lambda \in K$  such that  $t^m - \lambda$  is irreducible over  $K$  and  $K$  is the splitting field of  $t^m - \lambda$  over  $K$ . If  $\beta$  is a root of  $t^m - \lambda$  in  $L$ , then  $L = K(\beta)$ .

**Definition 4.12** (Kummer extension). A [cyclic extension](#)  $K \leq L$  with  $|L : K| = m$ , where  $\text{char } K \nmid m$  and  $K$  contains a [primitive  \$m\$ th root of unity](#) is a **Kummer extension**.

The proof of [Theorem 4.11](#) uses

**Lemma 4.13.** Let  $\phi_1, \dots, \phi_n$  be embeddings of a field  $K$  into a field  $L$ . Then there do not exist  $\lambda_1, \dots, \lambda_n$  not all zero such that  $\lambda_1 \phi_1(x) + \dots + \lambda_n \phi_n(x) = 0 \ \forall x \in K$ .

*Proof.* Example sheet 2, question 10. □

*Proof of Theorem 4.11.* Let  $\text{Gal}(L/K) = \langle \sigma \rangle$  of order  $m$ . Observe that  $1, \sigma, \sigma^2, \dots, \sigma^{m-1}$  are distinct maps  $L \rightarrow L$ , and we can apply [Lemma 4.13](#). There exists  $\alpha \in L$  such that

$$\beta = \alpha + \xi \sigma(\alpha) + \dots + \xi^{m-1} \sigma^{m-1}(\alpha) \neq 0$$

where  $\xi$  is a primitive  $m$ th root of unity. Observe that  $\sigma(\beta) = \xi^{-1} \beta \neq \beta$  and so  $\beta \notin K$ , the [fixed field](#) of  $\text{Gal}(L/K)$ .

$\sigma(\beta^m) = (\sigma(\beta))^m = \beta^m$ . Let  $\lambda = \beta^m \in K$ . But  $t^m - \lambda = (t - \beta)(t - \xi\beta) \dots (t - \xi^{m-1}\beta)$  in  $L[t]$ , and so  $K(\beta)$  is the [splitting field](#) of  $t^m - \lambda$  over  $K$  (recall  $\xi \in K$ ). Observe that  $1, \sigma, \dots, \sigma^{m-1}$  are distinct  [\$K\$ -automorphisms](#) of  $K(\beta)$  and so  $|K(\beta) : K| \geq m$ .

So  $L = K(\beta) = K(\xi\beta)$  since  $\xi \in K$ .  $t^m - \lambda$  is the [minimal polynomial](#) of  $\beta$  over  $K$  and hence is irreducible. □

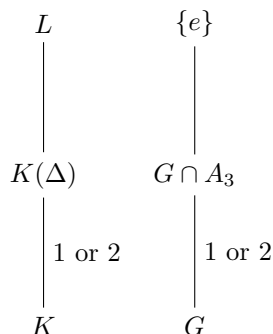
**Definition 4.14** (Extension by radicals). A field extension  $K \leq L$  is an **extension by radicals** if  $\exists K = L_0 \leq L_1 \leq \dots \leq L_n = L$  such that each  $L_i \leq L_{i+1}$  is either cyclotomic or Kummer extension. A polynomial  $f(t) \in K[t]$  is **soluble by radicals** if its splitting field lies in an extension by radicals.

### 4.3 Cubics

We've already seen that if  $f(t)$  is a monic irreducible cubic in  $K[t]$  with  $L$  its [splitting field](#) over  $K$ ,

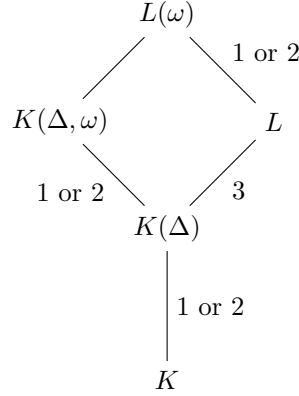
$$\text{Gal}(f) = \text{Gal}(L/K) = G \text{ is } A_3 \text{ or } S_3$$

(since irreducibility  $\implies$  action on roots is transitive, and transitive subgroups of  $S_3$  are  $A_3$  or  $S_3$ ).



where  $\Delta^2 = D(f)$  the discriminant of  $f$ . But to see that we can [solve  \$f\$  by radicals](#) we want to make use of [Theorem 4.11](#), and so we need to adjoin the appropriate roots of unity.

Now we get a bigger picture, denoting  $\omega$  a primitive cube root of 1.



From the [Tower law](#),  $|L(\omega) : K(\Delta, \omega)| = 3$ . Hence  $\text{Gal}(L(\omega)/K(\Delta, \omega)) \cong C_3$ . We can apply [Theorem 4.11](#) to see that  $L(\omega) = K(\Delta, \omega)(\beta)$ , where  $\beta$  is a root of an irreducible polynomial  $t^3 - \lambda \in K(\Delta, \omega)[t]$ . In fact, from the proof of [Theorem 4.11](#) we see that  $\beta = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$  where  $\alpha_1, \alpha_2, \alpha_3$  roots of  $f(t)$ .

Now all the extensions  $K \leq K(\Delta) \leq K(\Delta, \omega) \leq L(\omega)$  are [cyclotomic](#) or [Kummer](#). So  $f(t)$  is soluble by radicals.

### In practice

Given an irreducible cubic

$$\begin{aligned}
 f(t) &= t^3 + at^2 + bt + c \\
 &= (t - \alpha_1)(t - \alpha_2)(t - \alpha_3)
 \end{aligned}$$

we have  $\alpha_1 + \alpha_2 + \alpha_3 = -a$ .

Replace the  $\alpha_i$ s by  $\alpha'_i = \alpha_i + \frac{a}{3}$  so that  $\alpha'_1 + \alpha'_2 + \alpha'_3 = 0$ . They are roots of a polynomial  $t^3 + pt + q$  and  $K(\alpha_1, \alpha_2, \alpha_3) = K(\alpha'_1, \alpha'_2, \alpha'_3)$ . We have  $D(g) = -4p^3 - 27q^2$ .

Set  $\beta = \alpha'_1 + \omega\alpha'_2 + \omega^2\alpha'_3$ ,  $\gamma = \alpha'_1 + \omega^2\alpha'_2 + \omega\alpha'_3$ . Then

$$\begin{aligned}
 \beta\gamma &= \alpha'_1 + \alpha'_2 + \alpha'_3 + (\omega + \omega^2)(\alpha'_1\alpha'_2 + \alpha'_1\alpha'_3 + \alpha'_2\alpha'_3) \\
 &= (\alpha'_1 + \alpha'_2 + \alpha'_3)^2 - 3(\alpha'_1\alpha'_2 + \alpha'_1\alpha'_3 + \alpha'_2\alpha'_3) \\
 &= -3p
 \end{aligned}$$

and so  $\beta^3\gamma^3 = -27p^3$ .

$$\begin{aligned}
 \beta^3 + \gamma^3 &= (\alpha_1 + \omega\alpha'_2 + \omega^2\alpha'_3)^3 + (\alpha'_1 + \omega^2\alpha'_2 + \omega\alpha'_3)^3 + (\alpha'_1 + \alpha'_2 + \alpha'_3)^3 \\
 &= 3(\alpha'^3_1 + \alpha'^3_2 + \alpha'^3_3) + 18\alpha'_1\alpha'_2\alpha'_3 \\
 &= -27q
 \end{aligned}$$

since  $\alpha'^3_i = -p\alpha'_i - q$  and so  $\alpha'^3_1 + \alpha'^3_2 + \alpha'^3_3 = -3q$ .

So  $\beta^3$  and  $\gamma^3$  are roots of a quadratic  $t^2 + 27qt - 27p^3$ , hence they are

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

We can solve for  $\beta^3$  and  $\gamma^3$  in  $K(\sqrt{-3}, \sqrt{D}) = K(\omega, \Delta)$ . We can get  $\beta$  by adjoining a cube root of  $\beta^3$ , and then set  $\gamma = \frac{-3p}{\beta}$ . Finally we solve in  $L(\omega)$  for  $\alpha'_1, \alpha'_2, \alpha'_3$  (remembering  $\alpha'_1 + \alpha'_2 + \alpha'_3 = 0$ ), using

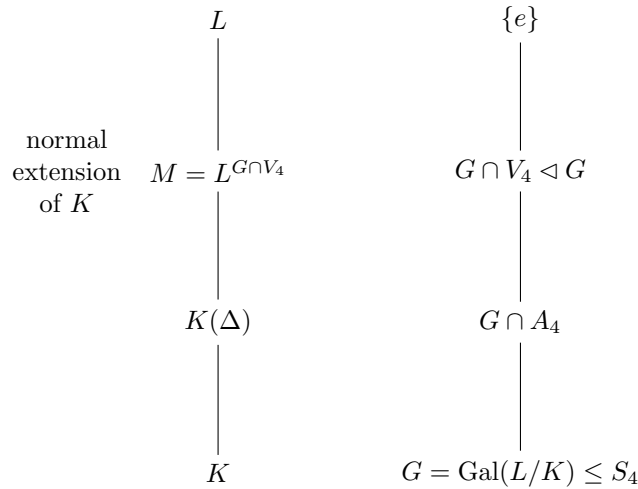
$$\alpha'_1 = \frac{1}{3}(\beta + \gamma), \quad \alpha'_2 = \frac{1}{3}(\omega^2\beta + \omega\gamma), \quad \alpha'_3 = \frac{1}{3}(\omega\beta + \omega^2\gamma).$$

#### 4.4 Quartics

As with the cubics by making a substitution of the form  $\alpha'_i = \alpha_i + \frac{a}{4}$  we may assume the sum of the roots to be zero, and so the  $t^3$  term is zero.

$$\begin{aligned} f(t) &= t^4 + bt^2 + ct + d \quad \text{monic irreducible} \\ &= (t - \alpha_1)(t - \alpha_2)(t - \alpha_3)(t - \alpha_4) \end{aligned}$$

Let  $L = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$  be the [splitting field](#) for  $f(t)$  over  $K$  and set  $M = L^{G \cap V_4}$ . The [Fundamental Theorem of Galois Theory](#) gives  $\text{Gal}(M/K) \cong \frac{G}{G \cap V_4}$ .



Take  $\theta : S_4 \rightarrow S_3$  with  $\ker \theta = V_4$ , so  $S_4/V_4 \cong S_3$ . Consider  $\theta|_G : G \rightarrow S_3$ , so  $\ker \theta|_G = G \cap V_4$ , and  $\frac{G}{G \cap V_4} \cong \text{im } \theta|_G \leq S_3$ .

We therefore go looking for a cubic for which  $M$  is the splitting field, called the resolvent cubic.

Set  $x = \alpha_1 + \alpha_2$ ,  $\gamma = \alpha_1 + \alpha_3$ ,  $z = \alpha_1 + \alpha_4$  and so

$$\alpha_1 = \frac{1}{2}(x + y + z), \alpha_2 = \frac{1}{2}(x - y - z), \alpha_3 = \frac{1}{2}(-x + y - z), \alpha_4 = \frac{1}{2}(-x - y + z).$$

Thus  $K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = K(x, y, z)$ .

$$x^2 = (\alpha_1 + \alpha_2)^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$

$$y^2 = (\alpha_1 + \alpha_3)^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$

$$z^2 = (\alpha_1 + \alpha_4)^2 = -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

These are distinct, e.g. if  $y^2 = z^2$  then  $y = \pm z$  and so either  $\alpha_3 = \alpha_4$  or  $\alpha_1 = \alpha_2$ . The  $x^2, y^2, z^2$  are permuted by  $G$  and are fixed by  $G \cap V_4$  by observation. So  $K(x^2, y^2, z^2) \leq M = L^{G \cap V_4}$ .

**Claim:** We have equality  $M = K(x^2, y^2, z^2)$ . Consider the **resolvent cubic**  $g(t) = (t - x^2)(t - y^2)(t - z^2) \in K[t]$ . Note that its coefficients are fixed by  $G$  and so lie in  $K$ .

Observe  $D(f) = D(g)$ , (check on example sheet). So  $K(\Delta) \leq K(x^2, y^2, z^2)$ . Now observe that  $\text{Gal}(L/K(x^2, y^2, z^2)) = \text{Gal}(K(x, y, z)/K(x^2, y^2, z^2))$ .

$$K(x^2, y^2, z^2) \leq K(x, y^2, z^2) \leq K(x, y, z^2) \leq K(x, y, z)$$

where each extension is degree 1 or 2. So  $|K(x, y, z) : K(x^2, y^2, z^2)|$  divides 8. So, the elements of  $\text{Gal}(L/K(x^2, y^2, z^2))$  have order dividing 8. But  $\text{Gal}(L/K(x^2, y^2, z^2)) \leq G \cap A_4$ , so  $\text{Gal}(L/K(x^2, y^2, z^2)) \leq G \cap V_4$ . By the [Fundamental Theorem of Galois Theory](#),  $M = K(x^2, y^2, z^2)$ .  $\square$

Consider the coefficients of  $g(t)$ :  $x^2, y^2, z^2$  are permuted by  $G$  and so the coefficients of  $g(t)$  are fixed by  $G$  and therefore in  $K$ .

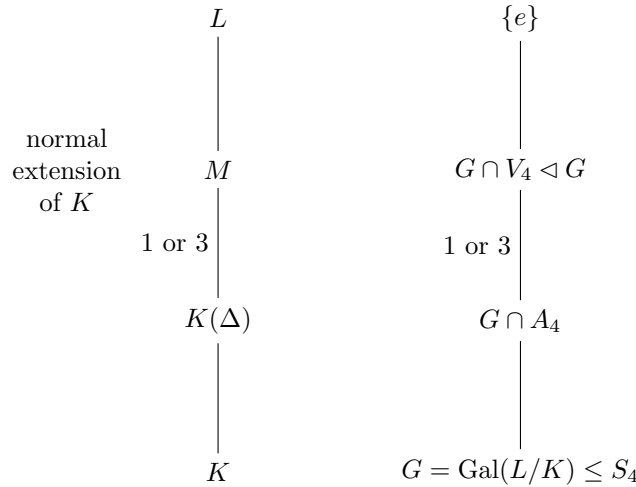
$$x^2 + y^2 + z^2 = -2b,$$

$$x^2y^2 + x^2z^2 + y^2z^2 = b^2 - 4d,$$

$$xyz = -c, \quad x^2y^2z^2 = c^2,$$

$$\text{So } g(t) = t^3 + 2bt^2 + (b^2 - 4d)t - c^2$$

We know how to solve cubics and so we can solve for  $x^2, y^2, z^2$ . Then we can solve for  $x, y, z$ . Then use the formulae from earlier to find  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ .



**Example.** For  $f(t) = t^4 + 4t^2 + 2$ , we have  $g(t) = t^3 + 8t^2 + 8t$  reducible.

## 4.5 Solubility by radicals

Now suppose we have a [Galois extension](#)  $K \leq L$  with

$$K = L_0 \leq L_1 \leq \cdots \leq L_m = L$$

such that  $L_i \leq L_{i+1}$  is either [cyclotomic](#) or [Kummer](#) extension.

Let  $G = \text{Gal}(L/K)$ . There is a corresponding chain of subgroups of  $G$

$$G = G_0 \geq G_1 \geq \cdots \geq G_m = \{e\}$$

with  $G_i = \text{Gal}(L/L_i)$ ,  $L_i = L^{G_i}$  from [Theorem 3.2](#).

However each extension  $L_i \leq L_{i+1}$  is Galois and we know

$$G_{i+1} = \text{Gal}(L/L_{i+1}) \triangleleft \text{Gal}(L/L_i) = G_i$$

hence  $G_i/G_{i+1} \cong \text{Gal}(L_{i+1}/L_i)$ , which is abelian if  $L_i \leq L_{i+1}$  is [cyclotomic](#) and cyclic if  $L_i \leq L_{i+1}$  is [Kummer](#).

**Definition 4.15** (Soluble group). A group is **soluble** if there is a chain of subgroups

$$\{e\} = G_m \triangleleft G_{m-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$$

with  $G_i/G_{i+1}$  abelian.

**Example.**

- $S_3$  is [soluble](#):  $\{e\} \triangleleft \langle (123) \rangle \triangleleft S_3$ .
- $S_4$  is soluble:  $\{e\} \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$  and  $A_4/V_4 \cong C_3$ ,  $S_4/A_4 \cong C_2$ .
- $A_5$  is simple, and therefore any normal subgroup is  $A_5$  and so any chain would have a non-abelian quotient. So,  $A_5$  is not soluble.

**Lemma 4.16.** A finite group  $G$  is [soluble](#) if and only if we have

$$\{e\} = G_m \triangleleft G_{m-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$$

with  $G_i/G_{i+1}$  cyclic.

*Proof.*  $(\Leftarrow)$  is immediate.  $(\Rightarrow)$ . We know about the structure of finite abelian groups. If  $A$  abelian then there is a chain

$$\{e\} = A_r \triangleleft A_{r-1} \triangleleft \cdots \triangleleft A_0 = A$$

with  $A_r/A_{r+1}$  cyclic. Thus if we have a chain with abelian factors  $G_i/G_{i+1}$  we can refine it to have cyclic factors.  $\square$

**Definition 4.17** (Derived subgroup). The **derived subgroup**  $G'$  of a group  $G$  is the subgroup generated by all the commutators  $g_1 g_2 g_1^{-1} g_2^{-1}$  for  $g_1, g_2 \in G$ .

**Lemma 4.18.** Let  $K \triangleleft G$ . Then  $G/K$  abelian  $\iff G' \leq K$ .



*Proof.*

$$\begin{aligned}
G/K \text{ abelian} &\iff Kg_1Kg_2Kg_1^{-1}Kg_2^{-1} = K \quad \forall g_1, g_2 \in G \\
&\iff g_1g_2g_1^{-1}g_2^{-1} \in K \\
&\iff G' \leq K.
\end{aligned}$$

□

**Remark.**

- (1) Next term in Representation Theory, we will prove Burnside's theorem: If  $|G| = p^a q^b$  for  $p, q$  distinct primes then  $G$  is [soluble](#).
- (2) The Feit-Thompson theorem says that if  $|G|$  is odd, then  $G$  is [soluble](#).
- (3) There's an analogue of Sylow's theorems due to Philip Hall. For all  $|G| = mn$  with  $m, n$  coprime there is a subgroup of order  $m$  iff  $G$  is [soluble](#).

**Definition 4.19** (Derived series). The **derived series**  $\{G^{(m)}\}$  of  $G$  is defined inductively:

$$\begin{aligned}
G^{(0)} &= G \\
G^{(1)} &= G' \\
G^{(2)} &= (G')' \\
G^{(j+1)} &= (G^{(j)})'
\end{aligned}$$

Thus  $G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \dots$  with  $G^{(j)}/G^{(j+1)}$  abelian.

**Lemma 4.20.** For  $G$  finite,  $G$  is [soluble](#)  $\iff G^{(m)} = \{e\}$  for some  $m$ .

*Proof.* If  $G^{(m)} = \{e\}$  then the derived series gives a chain in the definition of solubility.

Conversely if there is such a chain

$$G \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_m = \{e\}$$

with  $G_i/G_{i+1}$  abelian then an easy induction shows that  $G^{(j)} \leq G_j$  and so  $G^{(m)} = \{e\}$ . □

**Lemma 4.21.**

- (i) Let  $H \leq G$ ,  $G$  [soluble](#). Then  $H$  soluble.
- (ii) Let  $H \triangleleft G$ , then  $G$  soluble  $\iff H$  and  $G/H$  both soluble.

*Proof.*

- (i)  $G$  soluble  $\implies G^{(m)} = \{e\}$  by [Lemma 4.20](#). But  $H^{(m)} \leq G^{(m)}$  and so  $H$  soluble by [Lemma 4.20](#).
- (ii) Let  $H \triangleleft G$ , then  $G$  soluble  $\implies H$  soluble by (i).  $G$  soluble  $\implies G^{(m)} = \{e\}$ , say. Observe that

$$\left(\frac{G}{H}\right)' = \frac{G'H}{H} \leq \frac{G}{H}.$$

Similarly,

$$\left(\frac{G}{H}\right)^{(j)} = \frac{G^{(j)}H}{H} \leq \frac{G}{H}.$$

Thus  $(G/H)^{(m)} = H/H$ , a trivial subgroup of  $G/H$  and so  $G/H$  soluble.

Now consider the converse. Suppose that  $H$  and  $G/H$  are soluble.  $H^{(r)} = \{e\}$  and  $(G/H)^{(s)} = H/H$ . But

$$\left(\frac{G}{H}\right)^{(s)} = \frac{G^{(s)}H}{H}$$

so  $G^{(s)}H = H$  thus  $G^{(s)} \leq H$ . Hence  $G^{(r+s)} \leq H^{(r)} = \{e\}$ . Thus  $G$  is soluble by Lemma 4.20.

□

**Example.**  $S_5$  is not soluble since its subgroup  $A_5$  is not soluble.

**Theorem 4.22.** Let  $K$  be a field and  $f(t) \in K[t]$ . Assume  $\text{char } K = 0$ . Then  $f(t)$  is soluble by radicals over  $K \iff \text{Gal } f$  over  $K$  is soluble.

**Remark.** We don't need to restrict to  $\text{char } K = 0$ . What we need to do for a particular  $f(t)$  is to avoid a finite number of bad characteristics (avoid characteristics  $\leq \deg f(t)$ ).

**Corollary 4.23.** If  $f(t)$  is a monic irreducible polynomial  $\in K[t]$  with  $\text{Gal}(f) \cong A_5$  or  $S_5$  then  $f(t)$  is not soluble by radicals (with  $\text{char } K = 0$ ).

**Example.** In Example 3.9, we considered  $f(t) = t^5 - 6t + 3 \in \mathbb{Q}[t]$ .  $\text{Gal}(f)$  over  $\mathbb{Q}$  is  $S_5$ , and so  $f$  is not soluble by radicals.

**Lemma 4.24.** If  $K \leq N$  is an extension by radicals then  $\exists N'$  with  $N \leq N'$  with  $K \leq N'$  is an extension by radicals, with  $K \leq N'$  a Galois extension.

*Proof of Theorem 4.22.* Suppose  $f(t)$  is soluble by radicals. Thus if  $L$  is the splitting field of  $f(t)$  over  $K$  then  $L$  lies in an extension of  $K$  by radicals

$$K = L_0 \leq L_1 \leq \cdots \leq L_m$$

with each  $L_i \leq L_{i+1}$  cyclotomic or Kummer.

With Lemma 4.24, we may assume  $L_m$  is Galois over  $K$ . By Fundamental Theorem of Galois Theory there is a corresponding chain of subgroups of  $\text{Gal}(L_m/K)$ . Our previous discussion at the beginning of this section (before Lemma 4.13) we know that  $\text{Gal}(L_m/K)$  is soluble.

But  $F \leq L \leq L_m$  with  $K \leq L$  Galois. By the Fundamental Theorem of Galois Theory,  $\text{Gal}(L/K) \cong \text{Gal}(L_m/K) / \text{Gal}(L_m/L)$ .

But quotients of soluble groups are soluble, so  $\text{Gal}(L/K)$  is soluble. □

*Proof of Lemma 4.24.* We have  $K = L_0 \leq L_1 \leq \cdots \leq L_m$  with each  $L_i \leq L_{i+1}$  cyclotomic or Kummer, and we want to embed this into a Galois extension of the same form.

Assume  $\text{char } K = 0$ . By the Primitive Element Theorem,  $L_m = K(\alpha_1)$  for some  $\alpha_1$ . Let  $g(t)$  be the minimal polynomial of  $\alpha_1$  over  $K$  with splitting field  $M$ . Thus  $M = K(\alpha_1, \alpha_2, \dots, \alpha_n)$  where  $\alpha_1, \dots, \alpha_n$  are roots of  $g(t)$ .

There are  $K$ -homomorphisms

$$\begin{aligned}\phi_i : M &\longrightarrow M \\ \alpha_1 &\longmapsto \alpha_i\end{aligned}$$

extending the  $K$ -homs  $K(\alpha_1) \rightarrow K(\alpha_i) \leq M$ .

The tower  $K \leq \phi_i(K) \leq \phi_i(L_1) \leq \cdots \leq \phi_i(L_m) = K(\alpha_i)$  with cyclotomic or Kummer extensions as before, Consider  $L_m = K(\alpha_1) \leq \phi_2(L_1)(\alpha_1) \leq \phi_2(L_2)(\alpha_1) \leq \cdots \leq \phi_2(L_m)(\alpha_1) = K(\alpha_1, \alpha_2)$ .

Consider the extension  $\phi_2(L_j)(\alpha_1) \leq \phi_2(L_{j+1})(\alpha_1)$ :

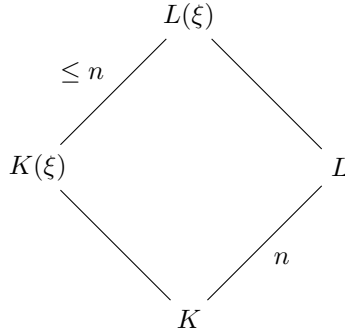
**if  $L_j \leq L_{j+1}$  is cyclotomic** then all the roots of unity adjoined are now in  $L_m = K(\alpha_1)$  and so  $\phi_2(L_j)(\alpha_1) = \phi_2(L_{j+1})(\alpha_1)$ .

**if  $L_j \leq L_{j+1}$  is Kummer** then we obtain  $L_{j+1}$  by adjoining roots of an element of  $L_j$  and so we obtain  $\phi_2(L_{j+1})$  by adjoining roots of an element in  $\phi_2(L_j)$ . Hence we get from  $\phi_2(L_j)(\alpha_1)$  to  $\phi_2(L_{j+1})(\alpha_1)$  by adjoining roots of an element of  $\phi_2(L_j)$ . So it's a Kummer extension.

Now continue to get suitable chain  $K(\alpha_1, \alpha_2) \leq \cdots \leq K(\alpha_1, \alpha_2, \alpha_3)$ .

Thus we get a suitable chain from  $K$  to  $K(\alpha_1, \dots, \alpha_n) = M$ . Observe that  $K \leq M$  is Galois.  $\square$

*Converse of Theorem 4.22.* Suppose  $G = \text{Gal}(f)$  over  $K$  is soluble (and  $\text{char } K = 0$ ). Let  $L$  be the splitting field of  $f(t)$  over  $K$  and so  $|G| = |L : K| = n$ . Set  $m = n!$  and let  $\xi$  be a primitive root of unity and consider  $L(\xi)$ .



Our proof is similar to that used for cubics. Observe that  $|L(\xi) : K(\xi)| \leq n$ . By the **Primitive Element Theorem**  $L = K(\alpha)$  for some  $\alpha$  with **minimal polynomial**  $g(t)$  say of degree  $n$ . Then  $L(\xi) = K(\xi)(\alpha)$  and the minimal polynomial of  $\alpha$  over  $K(\xi)$  divides  $g(t)$  and so is of degree  $\leq n$ .

Then  $\text{Gal}(L(\xi)/K)$  is soluble since  $\text{Gal}(L(\xi)/L)$  is soluble and  $\text{Gal}(L/K) \cong \frac{\text{Gal}(L(\xi)/K)}{\text{Gal}(L(\xi)/L)}$  soluble by **Fundamental Theorem of Galois Theory** and **Lemma 4.21**. Then the subgroup  $\text{Gal}(L(\xi)/K(\xi)) \leq \text{Gal}(L(\xi)/K)$  is soluble by **Lemma 4.21**.

Thus there is a chain of subgroups

$$\text{Gal}(L(\xi)/K(\xi)) = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{e\},$$

with  $G_i/G_{i+1}$  cyclic (using **Lemma 4.16**).

Now use the [Fundamental Theorem of Galois Theory](#) to get a corresponding chain of fields  $K(\xi) \leq K_1 \leq \cdots \leq K_m = L(\xi)$ , with each  $K_i \leq K_{i+1}$  [Galois](#), with [cyclic](#) Galois group. By [Theorem 4.11](#), all these extensions are Kummer (not all the extensions are of degree  $\leq n$  and so we have the appropriate roots of unity). Thus we've embedded  $L$  in an [extension of  \$K\$  by radicals](#).  $\square$

**Example.**

- (1) Take  $f(t) = t^4 + 4t^2 + 2$ , irreducible over  $\mathbb{Q}$  by [Eisenstein's criterion](#), and it has roots  $\pm\sqrt{-2 \pm \sqrt{2}}$  (two conjugate pairs). Complex conjugation gives double transposition. The resolvent cubic is  $g(t) = t^3 + 8t^2 + 8t$  which is reducible with roots  $0, -4 \pm 2\sqrt{2}$ . We have  $L = K(\sqrt{-4 + 2\sqrt{2}}, \sqrt{-4 - 2\sqrt{2}})$ , and  $M = K(-4 + 2\sqrt{2}, -4 - 2\sqrt{2}) = K(\sqrt{2})$ . So  $|L : K| = 8$ , and the Galois group is dihedral.
- (2)  $f(t) = t^4 + 2t + 2$  is irreducible over  $\mathbb{Q}$  by Eisenstein's criterion. Its discriminant is  $101 \cdot 4^2$ , not a square, and the resolvent cubic is  $g(t) = t^3 - 8t - 4$ , irreducible since it is  $t^3 + 2t + 1 \pmod{5}$ , irreducible. So there is a 3-cycle in the [Galois group](#).  $\text{Gal}(f)$  is a transitive subgroup of  $S_4$  and not of  $A_4$  containing a 3-cycle, so  $\text{Gal}(f)$  is  $S_4$ .
- (3)  $f(t) = t^5 - t - 1$  is irreducible over  $\mathbb{Q}$  since it is irreducible mod 5, and so the Galois group contains a 5-cycle and is a transitive subgroup of  $S_5$ . Mod 2, it factorises as a product of an irreducible cubic and quadratic:  $(t^3 + t^2 + 1)(t^2 + t + 1)$ . So  $\text{Gal}(\bar{f})$  is generated by an element of cycle type 3, 2, so  $\text{Gal}(f)$  contains an element of cycle type 3, 2, so  $g^3$  is a transposition. A subgroup of  $S_5$  containing a 5-cycle and a transposition must be  $S_5$  itself. So  $\text{Gal}(f) = S_5$  over  $\mathbb{Q}$ .

## 5 Final Thoughts

### 5.1 Algebraic closure

**Definition 5.1** (Algebraically closed). A field  $L$  is **algebraically closed** if any  $f(t) \in L[t]$  **splits** into a product of linear factors in  $L[t]$ .

**Remark.** This is equivalent to saying that any  $f(t) \in L[t]$  has a root in  $L$ , or that any algebraic extension of  $L$  is  $L$  itself.

**Definition 5.2** (Algebraic closure). An extension  $K \leq L$  is an algebraic closure of  $K$  if  $K \leq L$  is **algebraic** and  $L$  is **algebraically closed**.

**Lemma 5.3.** If  $K \leq L$  is **algebraic** and every polynomial in  $K[t]$  **splits** completely over  $L$ , then  $L$  is an **algebraic closure** of  $K$ .

*Proof.* We need to show  $L$  is **algebraically closed**. Suppose  $L \leq L(\alpha)$  is a **finite extension**, and  $f_\alpha(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$  is the **minimal polynomial** of  $\alpha$  over  $L$ . Let  $M = K(a_0, a_1, \dots, a_{n-1})$ . Then  $M \leq M(\alpha)$  is a finite extension. But each  $a_i$  is **algebraic** over  $K$  and so  $|M : K| < \infty$ . Hence  $|M(\alpha) : K| < \infty$  by **Tower law** and so  $\alpha$  is algebraic over  $K$ . The minimal polynomial over  $K$  must split over  $L$ , and so  $\alpha \in L$ . Thus any algebraic extension of  $L$  is  $L$  itself.  $\square$

**Example.**  $\mathbb{A} = \{ \alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q} \}$  It is a subfield of  $\mathbb{C}$ : If  $\alpha, \beta$  are **algebraic** over  $\mathbb{Q}$  then  $|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}| < \infty$  so if  $\gamma = \alpha + \beta, \alpha - \beta, \alpha\beta$  or  $\alpha/\beta$  (if  $\beta \neq 0$ ) we get  $\mathbb{Q}(\gamma) \leq \mathbb{Q}(\alpha, \beta)$  and so  $|\mathbb{Q}(\gamma) : \mathbb{Q}| < \infty$ . So  $\gamma$  is algebraic over  $\mathbb{Q}$  so  $\gamma \in \mathbb{A}$ . Therefore  $\mathbb{A} = \overline{\mathbb{Q}}$  is an **algebraic closure** of  $\mathbb{Q}$ .

If we want to prove existence and uniqueness of algebraic closures in general then we need to appeal to Zorn's Lemma. This appears in Logic and Set Theory, and it's equivalent to the Axiom of Choice and to the Well Ordering Principle.

**Definition 5.4** (Partial order).  $(\mathcal{S}, \leq)$  is a **partial order** on  $\mathcal{S}$  if

- (i)  $\forall x \in \mathcal{S} \ x \leq x$
- (ii)  $x \leq y$  and  $y \leq z \implies x \leq z$ .
- (iii) if  $x \leq y$  and  $y \leq x$  then  $x = y$ .

$\mathcal{S}$  is **totally ordered** if for any  $x, y \in \mathcal{S}$  either  $x \leq y$  or  $y \leq x$ . A **chain** is a partially ordered set  $(\mathcal{S}, \leq)$  that is a totally ordered subset.

**Lemma 5.5** (Zorn's Lemma). Let  $(\mathcal{S}, \leq)$  be a non-empty **partially ordered** set. Suppose that any **chain** has an upper bound in  $\mathcal{S}$ . Then  $\mathcal{S}$  has a maximal element.

**Lemma 5.6.** Let  $R$  be a ring. Then  $R$  has a maximal ideal.

*Proof.* Let  $\mathcal{S}$  be the set of proper ideals of  $R$ . This is non-empty, since  $(0)$  is proper. Partially order  $\mathcal{S}$  by inclusion. Any ideal  $I$  is proper  $\iff 1 \notin I$ . Any chain of proper ideals has an upper bound in  $\mathcal{S}$ , namely the union of the chain. **Zorn's Lemma** gives that  $\mathcal{S}$  has a maximal element, i.e. a maximal ideal of  $R$ .  $\square$

**Theorem 5.7** (Existence of algebraic closures). For any field  $K$  there is an **algebraic closure**.

*Proof.* Let

$$\mathcal{S} = \{ (f(t), j) \mid f(t) \text{ irreducible, monic in } K[t], 1 \leq j \leq \deg f \}$$

For each pair  $s = (f(t), j) \in \mathcal{S}$  we introduce an indeterminate  $X_s = X_{f,j}$ . Consider the polynomial ring  $K[X_s : s \in \mathcal{S}]$  and set

$$\tilde{f}(t) = f(t) - \prod_{j=1}^{\deg g} (t - X_{f,j}) \in K[X_s : s \in \mathcal{S}][t].$$

Let  $I \triangleleft K[X_s : s \in \mathcal{S}]$  generated by all the coefficients of all the  $\tilde{f}(t)$ . Denote the coefficients of  $\tilde{f}(t)$  by  $a_{f,l}$  for  $0 \leq l \leq \deg f$ .

Claim:  $I \neq K[X_s : s \in \mathcal{S}]$ . Proof: Suppose  $1 \in I$  and aim for a contradiction.

$$b_1 a_{f_1, l_1} + \cdots + b_N a_{f_N, l_N} = 1 \quad \text{in } K[X_s : s \in \mathcal{S}]. \quad (+)$$

Let  $L$  be a [splitting field](#) for  $f_1(t) \cdots f_N(t)$ .

For each  $i$ ,  $f_i$  splits over  $L$ .  $f_i(t) = \prod_{j=1}^{\deg f_i} (t - a_{ij})$ . Define a  $K$ -linear ring homomorphism, identity on  $K$ ,

$$\begin{aligned} \theta : K[X_s : s \in \mathcal{S}] &\longrightarrow L \\ X_{f_i, j} &\longmapsto \alpha_{ij} \\ X_s &\longmapsto 0 \quad \text{otherwise.} \end{aligned}$$

This induces a map  $K[X_s : s \in \mathcal{S}] \rightarrow L[t]$ . Then

$$\begin{aligned} \theta(\tilde{f}_i(t)) &= \theta(f_i(t)) - \prod_{j=1}^{\deg f_i} \theta(t - X_{f_i, j}) \\ &= f_i(t) - \prod_{j=1}^{\deg f_i} (t - \alpha_{i, j}) = 0. \end{aligned}$$

But then  $\theta(a_{f_i, j}) = 0$  since  $a_{f_i, j}$  are the coefficients of  $\tilde{f}_i(t)$ . But applying  $\theta$  to  $(+)$  we get  $0 = 1$ .

Then  $I$  is a proper ideal of  $K[X_s : s \in \mathcal{S}]$ . By [Zorn's Lemma](#) there is a maximal ideal  $P$  of  $K[X_s : s \in \mathcal{S}]$  containing  $I$ . Set  $L_1 = K[X_s : s \in \mathcal{S}]/P$ , a field. Thus we have a field extension  $K \leq L_1$ .

Claim:  $L_1$  is an [algebraic](#) closure of  $K$ . First show  $K \leq L_1$  is [algebraic](#):  $L_1$  is generated by the maps  $x_{f,j}$  of the  $X_{f,j}$ . However  $\tilde{f}(t)$  has coefficients in  $I$  and so its image  $L_1[t]$  is the zero polynomial. Thus in  $L_1[t]$ ,

$$f(t) = \prod (t - x_{f,j}) \quad (*)$$

and so  $f(x_{f,j}) = 0$ . Thus the  $x_{f,j}$  are algebraic.

Any element of  $L_1$  involves only finitely many of the  $x_{i,j}$  and so is [algebraic](#) over  $K$ . Moreover from  $(*)$  any  $f(t) \in K[t]$  splits completely over  $L_1$ .

The result follows from [Lemma 5.3](#).  $\square$

**Theorem 5.8.** Suppose  $\theta : K \rightarrow L$  is a ring homomorphism and  $L$  is algebraically closed. Suppose  $K \leq M$  is an algebraic extension. Then  $\theta$  can be extended to a homomorphism  $\theta : M \rightarrow L$  (i.e.  $\phi|_K = \theta$ ).

*Proof.* Let

$$\xi = \{ (N, \phi) \mid K \leq N \leq M, \phi \text{ a homomorphism } N \rightarrow L \text{ extending } \theta \}.$$

Partially order  $\xi$  with  $(N_1, \phi_1) \leq (N_2, \phi_2)$  if  $N_1 \leq N_2$  and  $\phi_2|_{N_1} = \phi_1$ .  $\xi$  is non-empty since  $(K, \theta) \in \xi$ .

If there is a chain  $(N_1, \phi_1) \leq \dots$  then set  $N = \bigcup N_\lambda$ . This is a subfield of  $M$ , and we can define  $\psi : N \rightarrow L$  as follows: if  $\alpha \in N$  then  $\alpha \in N_\lambda$  for some  $\lambda$  and we set  $\psi(\alpha) = \phi_\lambda(\alpha)$ . This is well defined.

Then  $(N, \psi)$  is an upper bound for our chain  $\xi$ .

Zorn's Lemma applies and gives a maximal element of  $\xi$ ,  $(N, \phi)$ . We now show  $N = M$ . Given  $\alpha \in M$ , it is algebraic over  $K$ , and hence over  $N$ . Let  $f_\alpha(t)$  be its minimal polynomial over  $N$ . But  $\phi f(t)$  is in  $L[t]$  and so splits completely over  $L$ , since  $L$  is algebraically closed.

So  $\phi f(t) = (t - \beta_1) \cdots (t - \beta_r)$ , say. Since  $\phi f(B_\gamma) = 0$  then there is a map

$$N(\alpha) \cong \frac{N[t]}{(f_\alpha(t))} \longrightarrow L$$

$$\alpha \longmapsto \beta_1 \quad \text{extending } \phi$$

Maximality of  $(N, \phi)$  implies that  $N(\alpha) = N$ . So  $\alpha \in N$ , so  $N = M$ .  $\square$

**Theorem 5.9** (Uniqueness of algebraic closures). If  $K \leq L_1$ ,  $L \leq L_2$  are two algebraic closures of  $K$  then there exists an isomorphism  $\phi : L_1 \rightarrow L_2$ .

*Proof.* By Theorem 5.8 there is a homomorphism  $\phi : L_1 \rightarrow L_2$  extending the embedding of  $K$  into  $L_2$ . Since  $K \leq L_2$  is algebraic, so too is  $\phi(L_1)$ . But  $L_1$  is algebraically closed and so  $\phi(L_1)$  is algebraically closed. So  $L_2 = \phi(L_1)$  and  $\phi$  is an isomorphism.  $\square$

## 5.2 Symmetric polynomials and invariant theory

In the buildup of the Fundamental Theorem of Galois Theory we met Artin's Theorem: Let  $K \leq L$  and  $H$  a finite group of  $\text{Aut}_K(L)$ . Let  $M = L^H$ . Then  $M \leq L$  is a Galois extension and  $H = \text{Gal}(L/M)$ .

**Example.**  $L = K(X_1, \dots, X_n)$ . Let  $S_n$  permute the variables. These permutations induce  $K$ -automorphisms of  $L$ . By Artin's Theorem, if  $M = L^{S_n} \leq L$  then it is Galois and  $\text{Gal}(L/M) = S_n$ . Thus  $S_n$  is a Galois group of some field extension.

We know that we can regard any finite group  $G$  as a subgroup of some  $S_n$ , and so we see that any finite group is a Galois group of some field extension (using Fundamental Theorem of Galois Theory). Let

$$\begin{aligned} f(t) &= (t - X_1)(t - X_2) \cdots (t - X_n) \in M[t] \\ &= t^n - s_1 t^{n-1} + s_2 t^{n-2} + \cdots + (-1)^n s_n. \end{aligned}$$

Thus  $s_1 = X_1 + \cdots + X_n$ ,  $s_2 = \sum_{i < j} X_i X_j$ , and  $s_n = X_1 X_2 \cdots X_n$ .

**Definition 5.10** (Elementary symmetric polynomials). These  $s_i$  are the elementary symmetric polynomials.

**Theorem 5.11.** The fixed field  $M = L^{S_n} = K(s_1, \dots, s_n)$  and the  $s_1, \dots, s_n$  are algebraically independent over  $K$  (in  $L$ ).

**Definition 5.12.**  $\alpha_1, \dots, \alpha_n$  are **algebraically independent** over  $K$  if the ring homomorphism  $K[Y_1, \dots, Y_n] \rightarrow K[\alpha_1, \dots, \alpha_n] \leq L$  is an isomorphism where  $K[Y_1, \dots, Y_n]$  is the polynomial ring in  $Y_1, \dots, Y_n$ .



# Index

- algebraic, 5
- algebraic closure, 45
  - existence, 45
  - uniqueness, 47
- algebraically closed, 45
- Artin's theorem, 25
- automorphism group, 22
  
- constructible, 7
- cyclotomic polynomial, 32
  
- degree, 3
- derived series, 41
- derived subgroup, 40
- discriminant, 28
  
- Eisenstein's criterion, 8
- elementary symmetric polynomials, 48
  
- field extension, 3
  - by radicals, 36
  - cyclic, 34
  - cyclotomic, 32
  - Kummer, 36
  - normal, 13
  - normally generated, 22
  - separable, 15
  - separably generated, 18
  - simple, 6
- finite field
  - existence, 31
  - uniqueness, 30
- fixed field, 24
- formal derivative, 14
- frobenius automorphism, 30
- fundamental theorem, 24
  
- Galois extension, 22
- Galois group, 22
  - of polynomial, 27
  
- $K$ -homomorphism, 10
  
- minimal polynomial, 5
  
- norm, 19
  
- poset, 45
- Primitive element theorem, 18
- primitive root, 32
  
- separable polynomial, 14
- soluble, 40
- splitting field, 10
  - existence, 12
  - uniqueness, 12
  
- tower law, 3
- trace, 19
  
- Zorn's lemma, 45