II Galois Theory

Ishan Nath, Michaelmas 2023

Based on Lectures by Prof. Tom Fisher

November 28, 2023

Contents

1 Field Extensions

A *field* K is a ring (commutative, with a 1 and $0_K \neq 1_K$) in which every non-zero element has an inverse under multiplication. The *characteristic* of K is the least positive integer p (necessarily prime) such that $p \cdot 1_K = 0_K$. If no such p exists, $\text{char}(K) = 0$.

Then K contains a smallest subfield, either $\mathbb{F}_p$ if $\text{char}(K) = p \neq 0$, or $\mathbb{Q}$ if $\text{char}(K) = 0$.

Lemma 1.1. *Let K be a field, $0 \neq f \in K[X]$. Then f has at most $\deg(f)$ roots in K.*

Proof: We induct on $\deg(f) = n$. If f has degree 0, i.e. is constant, then it has no roots as $f \neq 0$. Otherwise, let $\deg(f) > 0$, and assume f has a root α otherwise the result is trivial.

Then $f(X) = (X - \alpha)g(X)$, where $g \in K[X]$, by polynomial division. Now $\deg(g) = n - 1$, so g has at most $n - 1$ roots. Then f has at most n roots; the roots of g, plus possibly α if it is not a root of g. Hence f has at most n roots, as desired.

Definition 1.1. Let L be a field and $K \subset L$ a subfield. Then L is an *extension* of K, written L/K.

Note that $\text{char}(K) = \text{char}(L)$.

Example 1.1. (Field extension)

(i) $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$.

(ii) Let K be a field, and $f \in K[X]$ an irreducible polynomial. As $K[X]$ is an ED, it is a PID. Now I claim (f) is a maximal ideal, as if $(f) \subset (g) \subset K[X]$, then $g \mid f$, a contradiction.

So $L = K[X]/(f)$ is a field, and moreover it is a field extension of K. If we let $\alpha = X + (f) \in L$, then α is a root of f in L.

Let L/K be a field extension. Then addition in L and multiplication by elements in K make L into a K-vector space.

Definition 1.2. Let L/K be a field extension. We say L/K is *finite* if L is finite dimensional as a K-vector space, in which case we write $[L : K] = \dim_K L$, which

we call the *degree* of the extension. If not, we say L/K is an *infinite extension*, and write $[L : K] = \infty$.

Example 1.2. (Degree of extensions)

(i) $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$.

(ii) If $L = K[X]/(f)$ for f irreducible, then $[L : K] = \deg(f)$. Indeed, if $\alpha \in L$ is as before, then $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of L.

Let K, L be field s and $\phi : K \to L$ a ring homomorphism. Then $\ker(\phi)$ is an ideal of K, but as K is a field this means either $\ker(\phi) = \{0\}$ or K.

However as ϕ is a ring homomorphism, $1_K \mapsto 1_L$, so $1_K \notin \ker(\phi)$. Hence $\ker(\phi) = \{0\}$, and so ϕ is injective.

We call such ϕ an *embedding* of K in L. We may use ϕ to identify K as a subfield of L, i.e. as an extension L/K.

1.1 Finite Fields

Taking $K = \mathbb{F}_2$, and $f = X^2 + X + 1 \in \mathbb{F}_2[X]$, then $L = K[X]/(f)$ gives a field with 4 elements. We will see how to construct all finite feels in this subsection.

Proposition 1.1. *Let K be a finite field of characteristic p. Then $|K| = p^n$, where $n = [K : \mathbb{F}_p]$.*

Proof: As $[K : \mathbb{F}_p] = n$, $K \cong \mathbb{F}_p^n$ as an $\mathbb{F}_p$-vector space. Hence $|K| = p^n$.

Later we will show there is exactly one field of order p^n for each such prime power.

The multiplicative group of a field is the set $K^\times = K \setminus \{0\}$, which is abelian under multiplication.

Proposition 1.2. *If K is a field, then any finite subgroup $G \subset K^\times$ is cyclic. In particular, if K is finite, then $K^\times$ is cyclic.*

Proof: By structure theorem and as G is abelian, G is a product of cyclic groups

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t},$$

where $1 \neq d_1 \mid d_2 \mid \cdots \mid d_t$. Moreover, if $t > 1$, then let $p | d_1$. We have that $C_p \times C_p$ is a subgroup of G, hence $X^p - 1$ has at least p^2 roots. However this

contradicts lemma 1.1.

Proposition 1.3. *Let R be a ring of characteristic p. Then*

$$\begin{aligned} \phi_p : R &\to R \\ x &\to x^p \end{aligned}$$

is a homomorphism from R to itself (the Frobenius endomorphism*).*

Proof: We need to show $\phi_p(1) = 1$, $\phi_p(xy) = \phi_p(x)\phi_p(y)$, and $\phi_p(x+y) = \phi_p(x) + \phi_p(y)$. The first two properties follow easily, and the last follows from binomial expansion:

$$\phi_p(x+y) = x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} + y^p = x^p + y^p = \phi_p(x) + \phi_p(y).$$

This can give a proof to Fermat's little theorem using induction.

Theorem 1.1 (Tower law)**.** *Let M/L and L/K be field extension. Then M/K is finite if and only if both M/L and L/K are finite. In this case,*

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

Proof: If M/K is finite, then any K-basis for M spans M as an L-vector space, and L is a K-vector subspace of M.

Now suppose that M/L and L/K are finite, say $v_1, \ldots, v_n$ is a K-basis for L, and $w_1, \ldots, w_m$ is a L-basis for M.

We claim that $\{v_i w_j \mid 1 \le i \le n, 1 \le j \le m\}$ is a K-basis for M:

(i) If $x \in M$, then $x = \sum_j \lambda_j w_j$ for some $\lambda_j \in L$, and $\lambda_j = \sum_i \mu_{ij} v_i$ for some $\mu_{ij} \in K$.

Then $x = \sum_{i,j} \mu_{ij} v_i w_j$, showing these are spanning.

(ii) Now suppose $\sum_{i,j} \mu_{ij} v_i w_j = 0$ for some $\mu_{ij} \in K$. Then

$$\sum_j \left(\sum_i \mu_{ij} v_i \right) w_j = 0.$$

As $w_1, \ldots, w_m$ are linearly independent over L, $\sum_i \mu_{ij} v_i = 0$ for all

j. As $v_1, \ldots, v_n$ are linearly independent over K, $\mu_{ij} = 0$ for all i, j. Hence these elements are linearly independent.

Definition 1.3. Let L/K be a field extension. Let $\alpha_1, \ldots, \alpha_n \in L$. Then

$$K[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[X_1, \ldots, X_n]\}.$$

This is the smallest subring of L to contain K and $\alpha_1, \ldots, \alpha_n$. Moreover let

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f, g \in K[X_1, \ldots, X_n], g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$

This is the smallest subfield of L to contain K and $\alpha_1, \ldots, \alpha_n$. It is also the field of fractions of $K[\alpha_1, \ldots, \alpha_n]$.

Example 1.3.

Note that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$.

Moreover $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1 + \sqrt{2}) = \mathbb{Q}(17/(3 - \sqrt{2}))$.

Moreover $K[\alpha_1, \ldots, \alpha_n]$ and $K(\alpha_1, \ldots, \alpha_n)$ are the intersections of the subrings (resp. subfields) of L that contain K and $\alpha_1, \ldots, \alpha_n$.

We can check that

$$K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K(\alpha_1)(\alpha_2, \ldots, \alpha_n).$$

Definition 1.4. A field extension L/K is a *simple extension* if $L = K(\alpha)$ for some $\alpha \in L$.

2 Algebraic Elements and Extensions

Let L/K be a field extension and $\alpha \in L$. Then there is a unique ring homomorphism $\phi : K[X] \to L$ such that $\phi(c) = c$ and $c \in K$, and $\phi(X) = \alpha$.

Indeed, we can let $\phi(\sum c_i X^i) = \sum c_i \alpha^i$, for $c_i \in K$. In this case ϕ is the "evaluation at α" map.

As $K[X]$ is a PID, $\ker(\phi) = (f)$ for some $f \in K[X]$.

Definition 2.1. α is *algebraic* over K if $f \neq 0$. In this case f is irreducible and unique up to multiplication by elements of $K^\times$. We scale f so that it is monic, and call it the *minimal polynomial* of α over K.

By the isomorphism theorem for rings,

$$\frac{K[X]}{(f)} \cong K[\alpha],$$

and as (f) is a maximal ideal, $K[\alpha]$ is a field. So $K(\alpha) = K[\alpha]$.

Moreover $[K(\alpha) : K] = \deg f$, since if $\deg f = n$, then $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a K-basis for $K(\alpha)$.

Example 2.1.

- If $x \in K$, then $m_{x,K} = T - x$.
- If p is prime, $d \geq 1$, then $T^d - p \in \mathbb{Q}[T]$ is irreducible (e.g Eisenstein's and Gauss' Lemma). So it is the minimum polynomial of $\sqrt[d]{p} = x \in \mathbb{R}$ over $\mathbb{Q}$.
- If $z = e^{2\pi i/p}$, then it is the root of $g(T) = T^{p-1} + \cdots + T + 1 \in \mathbb{Q}[T]$. This is irreducible by looking at $g(T+1)$ and applying Eisenstein's. Hence g is the minimal polynomial of z over $\mathbb{Q}$.

Let $\alpha \in L$ be algebraic over K with minimum polynomial f. Let $0 \neq \beta \in K(\alpha)$, and say $\beta = g(\alpha)$ for some $g \in K[X]$. Since f is irreducible and $\beta \neq 0$, we see that f and g are coprime

Running Euclid's algorithm gives $r, s \in K[X]$ such that $r(X)f(X) + s(X)g(X) = 1$. Hence plugging in α,

$$s(\alpha)g(\alpha) = r(\alpha)f(\alpha) + s(\alpha)g(\alpha) = 1,$$

so the inverse of β is simply $s(\alpha)$.

Definition 2.2. Let L/K be a field extension.

(i) $\alpha \in L$ is *transcendental* over K if it is not algebraic. In this case $K[\alpha] \cong K[X]$ and $K(\alpha) \cong K(X)$. Since $K[X]$ is not a field and $1, X, X^2, \ldots$ are linearly independent over K, $K[\alpha] \neq K(\alpha)$ and $[K(\alpha) : K] = \infty$.

(ii) L/K is *algebraic* if every $\alpha \in L$ is algebraic over K.

Remark.

(i) We have
$$[K(\alpha) : K] < \infty \iff \alpha \text{ is algebraic over } K.$$

(ii) If $[L : K] < \infty$, then for any $\alpha \in L$ we certainly have $[K(\alpha) : K] < \infty$. So any finite extension is algebraic. Note that the converse is not true: take $K = \mathbb{Q}$ and $L = \bigcup \mathbb{Q}(\sqrt[2^n]{2})$. This is a union of nested sequences of fields, and so is a field.

Then $[L : K] = \infty$ as $[\mathbb{Q}(\sqrt[2^n]{2}) : \mathbb{Q}] = 2^n$ is unbounded, but every $\alpha \in L$ belongs to a finite extension of $\mathbb{Q}$, and so is algebraic over $\mathbb{Q}$.

(iii) Classically $\alpha \in \mathbb{C}$ is called algebraic or transcendental, if it is algebraic or transcendental over $\mathbb{Q}$. However note every $\alpha \in \mathbb{C}$ is transcendental over $\mathbb{R}$.

2.1 Algebraic Numbers in $\mathbb{R}$ and $\mathbb{C}$

Traditionally, $x \in \mathbb{C}$ is algebraic if it is algebraic over $\mathbb{Q}$, otherwise it is transcendental. We have seen that $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$, and is not equal to $\mathbb{C}$, as $\mathbb{Q}[T]$ is countable, so the number of possible roots is countable. However, even though 'most' numbers are transcendental, it is harder to write one explicitly, or show a specific number isn't algebraic.

Liouville first provided a transcendental number,

$$\sum_{n \geq 1} \frac{1}{10^{n!}}.$$

He did this by showing that algebraic numbers can't be approximated very well by rationals, while his number is.

Later, Hermite and Lindemann showed that e and π are transcendental, and in the 20th century, the following theorem was proven:

Theorem 2.1 (Gelfond-Schneider theorem)**.** *If x, y are algebraic, where $x \neq 0, 1$, then x^y is algebraic if and only if $y \in \mathbb{Q}$.*

This gives results such as $\sqrt{2}^{\sqrt{3}}$ and $e^{\pi} = (-1)^{-i/2}$ are transcendental.

Example 2.2.

Some examples of calculating degrees of extensions.

1. Let $f(X) = X^d - n$, $d \geq 2, n \neq 0$. Suppose there exists a prime p such that when we write $n = p^e m$ with $p \nmid m$, then $(d, e) = 1$.

   We claim that f is irreducible in $\mathbb{Q}[X]$. Equivalently, we show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, where $\alpha = \sqrt[d]{n}$. By Euclid's algorithm, there exist $r, s \in \mathbb{Z}$ such that $rd + se = 1$.

   Then $p^{dr} n^s = p^{dr}(p^e m)^s = pm^s$. We put $\beta = p^r \alpha^s$, so that $\beta^d = pm^s$. Then β is a root of $g(X) = X^d - pm^s$, which is irreducible in $\mathbb{Z}[X]$ by Eisenstein's criterion. Hence it is irreducible in $\mathbb{Q}[X]$ by Gauss' lemma, so $[\mathbb{Q}(\beta) : \mathbb{Q}] = d$.

   But $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq \deg f = d$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, as required.

2. Let p be an odd prime, and $\zeta_p = e^{2\pi i/p}$, and $\alpha = 2\cos(2\pi/p) = \zeta_p + \zeta_p^{-1}$. Let's compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Note that ζ_p is a root of

   $$f(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X^2 + X + 1.$$

   This is irreducible by Eisenstein's criterion applied to $f(X + 1)$, so $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. ζ_p is a root of

   $$g(X) = (X - \zeta_p)(X - \zeta_p^{-1}) = X^2 - \alpha X + 1 \in \mathbb{Q}(\alpha)[X].$$

   Hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\alpha)] \leq \deg g = 2$. But $\alpha \in \mathbb{R}$ and $\zeta_p \notin \mathbb{R}$, hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\alpha)] = 2$. By the tower law, we thus have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = (p - 1)/2$.

3. Suppose m, n and mn are not perfect squares. Let $\alpha = \sqrt{m} + \sqrt{n}$. We will compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Clearly $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Conversely, we have

   $$m = (\alpha - \sqrt{n})^2 = \alpha^2 - 2\alpha\sqrt{n} + n \implies \sqrt{n} = \frac{\alpha^2 - m + n}{2\alpha} \in \mathbb{Q}(\alpha).$$

   Similarly $\sqrt{m} \in \mathbb{Q}(\alpha)$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Now $[\mathbb{Q}(\sqrt{n}) : \mathbb{Q}] = 2$, and we are just left to find $[\mathbb{Q}(\sqrt{m}, \sqrt{n}) : \mathbb{Q}(\sqrt{n})]$. Note it is less than 2, as $\sqrt{m}$ is a root of $X^2 - m$.

Suppose it is 1, so $\sqrt{m} \in \mathbb{Q}(\sqrt{n})$. Then $\sqrt{m} = r + s\sqrt{n}$ for some $r, s \in \mathbb{Q}$. Squaring both sides,

$$m = r^2 + 2rs\sqrt{n} + s^2 n.$$

Since $\sqrt{n} \notin \mathbb{Q}$, we must have $rs = 0$. If $r = 0$, then mn is a square. But if $s = 0$, then m is a square, hence we have a contradiction.

Therefore the degree is 2, and by tower law, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Lemma 2.1. *Let L/k be a field extension and $\alpha_1, \ldots, \alpha_n \ni L$. Then*

$$\alpha_1, \ldots, \alpha_n \text{ algebraic over } K \iff [K(\alpha_1, \ldots, \alpha_n) : K] < \infty.$$

Proof: The case $n = 1$ was a remark in the previous lecture.

The forwards direction is done by induction on n, using the tower law.

The reverse direction is clear since $K(\alpha_i) \subseteq K(\alpha_1, \ldots, \alpha_n)$.

Corollary 2.1. *Let L/K be any field extension. Then the set*

$$\{\alpha \in L \mid \alpha \text{ is algebraic over } K\}$$

is a subfield of L.

Proof: If α, β are algebraic over K, then by the previous lemma $K(\alpha, \beta)$ is a finite extension of K. Let γ be one of $\alpha \pm \beta$, or $\alpha\beta$, or (if $\alpha \neq 0$) α^{-1}.

Then $\gamma \in K(\alpha, \beta)$, so $K(\alpha, \beta, \gamma) = K(\alpha, \beta)$ is a finite extension of K, hence γ is algebraic.

Example 2.3.

Taking $K = \mathbb{Q}$ and $L = \mathbb{C}$, we see that $\overline{\mathbb{Q}}$, which are the algebraic numbers, is a field.

Since $\overline{\mathbb{Q}} \supset \mathbb{Q}(\sqrt[d]{2})$, and $[\mathbb{Q}(\sqrt[d]{2}) : \mathbb{Q}] = d$ for all d, we see that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Proposition 2.1. *Let $M/L/K$ be field extensions.*

Then M/K is algebraic if and only if M/L and L/K are algebraic.

Proof: For the forwards direction, every element of M is algebraic over K, hence algebraic over L, so M/L is algebraic. Moreover as $L \subset M$, L is algebraic over K.

For the other direction, let $\alpha \in M$. We must show that α is algebraic over K. Since M/L is algebraic, α is a root of some polynomial

$$f(X) = c_n X^n + \cdots + c_1 X + c_0 \in L[X].$$

Let $L_0 = K(c_0, c_1, \ldots, c_n)$. Each $c_i \in L$, hence is algebraic. Lemma (2.1) implies $[L_0 : K] < \infty$. But f has coefficients in L_0, so $[L_0(\alpha) : L_0] \leq \deg f < \infty$.

By the tower law, $[L_0(\alpha) : K] < \infty$, hence α is algebraic over K.

3 Ruler and Compass Constructions

We use our results on field extensions to show that certain classical problems concerning ruler and compass constructions cannot be solved.

Let $S \subset \mathbb{R}^2$ be a finite set of points. In plane geometry constructions, we are given three basic operations:

1. Draw a straight line through any 2 distinct points in S.
2. Draw a circle with centre at any point in S, and radius the distance between two points in S.
3. Enlarge S by adjoining any point of intersection of two distinct lines or circles.

Say $(x, y) \in \mathbb{R}^2$ is *constructible* from S if we can enlarge S to contain (x, y) by a finite sequence of the above operations.

Say $x \in \mathbb{R}$ is constructible if $(x, 0)$ is constructible from $(0, 0)$ and $(1, 0)$. It is easy to show every $x \in \mathbb{Q}$ and $\sqrt{2}$ is constructible.

We will relate this notion to the following algebraic notion:

Definition 3.1. Let $K \subset \mathbb{R}$ be a subfield. Say K is *constructible* if there exists $n \geq 0$ and fields $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n \subset \mathbb{R}$ such that:

(i) $K \subset F_n$,

(ii) $[F_i : F_{i-1}] = 2$.

Remark. By the tower law, $K/\mathbb{Q}$ is a finite extension and $[K : \mathbb{Q}]$ is a power of 2.

Theorem 3.1. *If $x \in \mathbb{R}$ is constructible, then $K = \mathbb{Q}(x)$ is constructible.*

Proof: Suppose $S \subset \mathbb{R}^2$ is a finite set of points, all of whose coordinates belong to a constructible field K.

It suffices to show that if we adjoin $(x, y) \in \mathbb{R}^2$ to S, then $K(x, y)$ is also constructible.

The lines and circles in (i) and (ii) have equations of the form

$$ax + by = c, \qquad (x - a)^2 + (y - b)^2 = c,$$

with $a, b, c \in K$. If (x, y) is the intersection of two such lines or circles, then

$$x = r + s\sqrt{v}, y = t + u\sqrt{v}$$

for $r, s, t, u, v \in K$. Hence $(x, y) \in K(\sqrt{v}) \subset F_n(\sqrt{v})$, Since $[F_n(\sqrt{v}) : F_n]|2$, it follows that $K(x, y)$ is constructible.

Remark. It is not hard to show that the converse is true, that is, if $\mathbb{Q}(x)$ is a constructible extension of $\mathbb{Q}$, then x is constructible by ruler and compass.

Corollary 3.1. *If $x \in \mathbb{R}$ is constructible, then x is algebraic over $\mathbb{Q}$, and $[\mathbb{Q}(x) : \mathbb{Q}]$ is a power of 2.*

This resolves the following classical problems:

1. 'Squaring the circle' - constructing a square whose area is that of a given circle; this is equivalent to constructing $\sqrt{\pi}$. But since π is transcendental, therefore $\sqrt{\pi}$ is transcendental, so such a square isn't constructible
2. 'Duplicating the cube' - constructing a cube with volume twice that of a given cube; this is equivalent to constructing $\sqrt[3]{2}$. But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, so $\mathbb{Q}(\sqrt[3]{2})$ (and thus $\sqrt[3]{2}$) isn't constructible.
3. 'Trisecting the angle' - let's say we are trying to trisect $2\pi/3$, which is certainly constructible. So if we can trisect $2\pi/3$, the angle $2\pi/9 = \theta$ is constructible, implying the real numbers $\sin\theta$, $\cos\theta$ are constructible. Using the triple angle formula,
$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta,$$
which implies $\cos\theta$ is a root of $8X^3 - 6X + 1$, and $2\cos\theta$ is a root of $X^3 - 3X + 1$, which is irreducible as it has no rational roots. So $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 3$, implying $\cos\theta$ is not constructible.

In fact, we will later generalise this result:

Theorem 3.2 (Gauss)**.** *A regular polygon is constructible if and only if n is the product of a power of 2 and distinct primes of the form $2^{2^k} + 1$.*

4 Splitting Fields

Pick a field K, and $f \in K[T]$ be non-constant. We want to find an extension L/K, as small as possible, such that f has a root, or an extension in which f can be written as a product of linear polynomials in $L[T]$.

For example, if $K \subset \mathbb{C}$, the Fundamental Theorem of Algebra says we can factor a monic $f \in \mathbb{C}[T]$ as a product of linear factors

$$f = \prod (T - x_i),$$

$x_i \in \mathbb{C}$. However the best L would be $K(x_1, \ldots, x_n)$.

Definition 4.1. Let L/K and M/K be extensions of K. A *K-homomorphism* from L to M is a field homomorphism $L \to M$ which is the identity on K. It is also called a K-embedding.

Theorem 4.1. *Let $L = K(\alpha)$, where α is algebraic over K with minimal polynomial f. Let M/K be any field extension. Then there is a bijection*

$$\{K\text{-homomorphisms } L \to M\} \leftrightarrow \{\text{roots of } f \text{ in } M\},$$
$$\tau \mapsto \tau(\alpha).$$

In particular, the number of K-homomorphisms is less than $\deg f$.

Proof: Write

$$f = \sum_{i=0}^{d} c_i X^i,$$

where $c_i \in K$. Let $\tau : L \to M$ be a K-homomorphism. Then,

$$f(\tau(\alpha)) = \sum_i c_i \tau(\alpha)^i = \tau\left(\sum_i c_i \alpha^i\right) = \tau(f(\alpha)) = 0,$$

hence $\tau(\alpha)$ is a root of f. But as $L = K(\alpha)$, any K-homomorphism is determined uniquely by $\tau(\alpha)$, so this map is injective.

Now we saw earlier that the evaluation at α gives an isomorphism

$$\frac{K[X]}{(f)} \xrightarrow{\phi} L, \qquad X + (f) \mapsto \alpha.$$

Now let $\beta \in M$ be a root of f. Since f is irreducible, it is the minimal

polynomial for β over K. Then evaluation at β gives a ring homomorphism

$$\frac{K[X]}{(f)} \xrightarrow{\psi} M, \qquad X + (f) \mapsto \beta.$$

Since ϕ, ψ are K-homomorphisms and ϕ is an isomorphism, it follows that

$$\tau = \psi \circ \phi^{-1} : L \to M$$

is a K-homomorphism with $\tau(\alpha) = \beta$.

Example 4.1.

There are exactly 2 $\mathbb{Q}$-homomorphisms $\mathbb{Q}(\sqrt{2}) \to \mathbb{R}$, given by

$$a + b\sqrt{2} \mapsto a + b\sqrt{2},$$

$$a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Note for future proofs we will need a slight variant of the above theorem. The proof is the exact same, but the generality will be useful in inductive proofs.

Definition 4.2. Let L/K, M/K' be field extensions. Let $\sigma : K \to K'$ be a field homomorphism. If $\tau : L \to M$ is a homomorphism such that $\tau(x) = \sigma(x)$ for all $x \in K$, we say τ is a *σ-homomorphism* from L to L'.

We also say τ extends σ, or that σ is the restriction of τ to K, and write $\sigma = \tau|_K$.

Taking $K' = K$ and $\sigma = \mathrm{id}$, then we recover the definition of a K-homomorphism.

Theorem 4.2. *Let $L = K(\alpha)$ where α is algebraic over K, with minimum polynomial f. Let $\sigma : K \to K'$ be a field embedding, and M/K' be any field extension. Then there is a bijection*

$$\{\sigma\text{-homomorphisms } L \to M\} \leftrightarrow \{\text{roots of } \sigma f \text{ in } M\},$$
$$\tau \mapsto \tau(\alpha).$$

In particular, the number of σ-homomorphisms is at most $\deg f$.

Example 4.2.

Let $K = \mathbb{Q}(\sqrt{2})$, and $L = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{1 + \sqrt{2}}$.

Then there are exactly two K-embeddings $L \to \mathbb{R}$ given by $\alpha \mapsto \pm\sqrt{1 + \sqrt{2}}$.

However if $\sigma : K \to K$ by $a+b\sqrt{2} \mapsto a-b\sqrt{2}$, then there are no σ-embedding $L \to \mathbb{R}$, since $1 - \sqrt{2} < 0$.

Definition 4.3. Let K be a field. Let $0 \neq f \in K[X]$. An extension L/K is a *splitting field* of f over K if:

(i) f splits into linear factors over L.

(ii) $L = K(\alpha_1, \ldots, \alpha_n)$, where a_i are the roots of f.

The second condition is equivalent to saying that f does not split into linear factors over any subfield of L containing K. Moreover it implies $[L : K] < \infty$.

Theorem 4.3. *let $0 \neq f \in K[X]$. Then there exists a splitting field for f over K.*

Proof: The proof is by induction on $\deg f$. If $\deg f \leq 1$, then $L = K$.

Now assume that every polynomial of degree $< \deg f$ has a splitting field. Let g be an irreducible factor of f. Let

$$K_1 = \frac{K[X]}{(g)}, \qquad \alpha_1 = X + (g) \in K_1.$$

Then $f(\alpha_1) = 0$, so $f(X) = (X - \alpha_1)f_1(X)$ for some $f_1 \in K_1[X]$ with $\deg f_1 < \deg f$. By the induction hypothesis, there exists a splitting field L for f_1 over K_1. Say that $L = K_1(\alpha_2, \ldots, \alpha_n)$ where $\alpha_2, \ldots, \alpha_n$ are the roots of f_1 in L.

We claim that L is a splitting field for f over K. Since f_1 splits in L, so does $f(X) = (X - \alpha_1)f_1(X)$.

Moreover $L = K_1(\alpha_2, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n)$ and $\alpha_1, \ldots, \alpha_n$ are the roots of f, hence L satisfies both conditions.

Theorem 4.4 (Uniqueness of Splitting Fields)**.** *Let $0 \neq f \in K[X]$, and let L be a splitting field of f over K. Let $\sigma : K \to M$ be any field embedding such that $\sigma f \in M[X]$ splits. Then,*

(i) *There exists a σ-embedding $\tau : L \to M$.*

(ii) *If M is a splitting field for σf over σK, then any τ as above is an isomorphism.*

In particular, any two splitting fields for f over K are K-isomorphic.

Proof:

(i) We will prove this by induction on $n = [L : K]$. If $n = 1$ then $L = K$ and there is nothing to prove. So suppose $n > 1$ and let $g \in K[X]$ be an irreducible factor of f, of degree at least 1.

Let $\alpha \in L$ be a root of g, and let $\beta \in M$ be a root of σg. Hence σ extends to an embedding $\sigma_1 : K(\alpha) \to M$, where $\alpha \mapsto \beta$. Also $[L : K(\alpha)] < [L : K]$.

As L is a splitting field of f over $K(\alpha)$, and $\sigma_1 f = \sigma f$ splits in M, by the induction hypothesis σ_1 extends to an embedding $\tau : L \to M$.

(ii) Pick any $\tau : L \to M$ as in (i). Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in L. Then the roots of σf in M are $\tau\alpha_1, \ldots, \tau\alpha_n$. So if M is a splitting field for σf over σK, then

$$\begin{aligned} M &= \sigma K(\tau\alpha_1, \ldots, \tau\alpha_n) \\ &= \tau(K(\alpha_1, \ldots, \alpha_n)) \\ &= \tau(L). \end{aligned}$$

Hence τ is surjective, so τ is an isomorphism.

For the final statement, suppose L/K and M/K are splitting fields for f over K, and let $\sigma : K \to M$ be the inclusion map. Then combining (i) and (ii), we get a K-isomorphism $L \to M$.

Example 4.3.

If $K \subset \mathbb{C}$, then by the fundamental theorem of algebra, our splitting field for f over K is the subfield $K(\alpha_1, \ldots, \alpha_n) \subset \mathbb{C}$ where $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ are the roots of f.

(i) If $f(X) = X^3 - 2 \in \mathbb{Q}[X]$, then

$$f(X) = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \omega^2\sqrt[3]{2}),$$

so $\mathbb{Q}(\omega, \sqrt[3]{2})$ is a splitting field for f over $\mathbb{Q}$. Now $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, so as $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] \leq 6$ and is divisible by both 2 and 3, it must be 6.

(ii) Let p be an odd prime, and

$$\begin{aligned} f(X) &= \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X^2 + X + 1 \in \mathbb{Q}[X] \\ &= \prod_{r=1}^{p-1} (X - \zeta_p^r), \end{aligned}$$

where $\zeta_p = e^{2\pi i/p}$. Then f has splitting field $\mathbb{Q}(\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}) = \mathbb{Q}(\zeta_p)$. So in this case, the splitting field is obtained by just adjoining one root.

(iii) Let $f(X) = X^3 - 2 \in \mathbb{F}_7[X]$. Then f is irreducible as it has no roots. Let

$$L = \frac{\mathbb{F}_7[X]}{(f)},$$

so $L = \mathbb{F}_7(\alpha)$ with $\alpha^3 = 2$. But then as $2^3 = 4^3 = 1$, we can factor

$$f(X) = (X - \alpha)(X - 2\alpha)(X - 4\alpha).$$

So $L = \mathbb{F}_7(\alpha)$ is a splitting field for f over $\mathbb{F}_7$.

Definition 4.4. A field K is *algebraically closed* if every nonconstant polynomial in $K[X]$ has a root in K, equivalently every irreducible polynomial in $K[X]$ is linear.

From the fundamental theorem of algebra, $\mathbb{C}$ is algebraically closed.

Lemma 4.1. *Let K be a field. The following are equivalent:*

(i) *K is algebraically closed.*

(ii) *If L/K is a field extension and $\alpha \in L$ is algebraic over K, then $\alpha \in K$.*

(iii) *If L/K is algebraic then $L = K$.*

(iv) *If L/K is finite then $L = K$.*

Proof: (i) $\implies$ (ii) as the minimal polynomial of α over K is irreducible hence linear. So $\alpha \in K$.

Note that (ii) $\implies$ (iii) $\implies$ (iv) is clear. Now to show that (iv) $\implies$ (i), let $f \in K[X]$ be an irreducible polynomial.

Then $L = K[X]/(f)$ is a finite extension of K, with $[L : K] = \deg f$. But by

(iv) we have $L = K$, so f is linear, and hence every irreducible polynomial is linear, so if α is algebraic then $\alpha \in K$.

Definition 4.5. If L/K is algebraic and L is algebraically closed, then we say that L is an *algebraic closure* of K.

Lemma 4.2. *Let L/K be an algebraic extension such that every polynomial in $K[X]$ splits into linear factors over L. Then L is algebraically closed, and hence an algebraic closure of K.*

Proof: If L is not algebraically closed, then there must exist M/L algebraic with $[M : L] > 1$. Both M/L and L/K are algebraic, hence M/K is algebraic.

Pick any $\alpha \in M$. Let f be the minimal polynomial for α over K. By our assumption, f splits over L, so $\alpha \in L$. Hence $M = L$.

Later we will show that every field K has an algebraic closure.

Theorem 4.5. *Suppose that:*

(i) *$K \subset \mathbb{C}$, or*

(ii) *K is countable.*

Then K has an algebraic closure.

Proof:

(i) If $K \subset \mathbb{C}$, then let

$$L = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } K\}.$$

Then L is a field, as we have proved, and L/K is clearly algebraic. If $f \in K[X]$, then we can write $f(X) = \prod(X - \alpha_i)$ for some $\alpha_i \in \mathbb{C}$.

By the definition of L, all α_i are in L, so f splits into linear factors over L. Hence L is algebraically closed by our previous lemma, so L is the algebraic closure of K.

(ii) If K is countable, then so is $K[X]$. Enumerate the monic irreducible polynomials $f_1, f_2, \ldots$. Let $L_0 = K$ and for each $i \geq 1$ let L_i be a splitting field for f_i over L_{i-1}. Then,

$$L_0 \subset L_1 \subset L_2 \subset \cdots$$

Then $L = \bigcup L_n$ is a field, with L/K algebraic and every polynomial in $K[X]$ splits over L. Hence L is algebraically closed, so L is an algebraic closure of K.

Remark. Taking $K = \mathbb{Q}$ in the proof of the above, we see that $\overline{\mathbb{Q}} \subset \mathbb{C}$ is algebraically closed.

5 Symmetric Polynomials

5.1 Motivation

Suppose we wish to find the roots of a cubic polynomial $f(X) = X^3+aX^2+bX+c \in \mathbb{Q}[X]$.

After substituting $X - \frac{a}{3}$ for X, we may assume $a = 0$. Writing

$$f(X) = (X - \alpha)(X - \beta)(X - \gamma)$$

and comparing coefficients, we get

$$\begin{aligned} \alpha + \beta + \gamma &= 0, \\ \alpha\beta + \beta\gamma + \gamma\alpha &= b, \\ \alpha\beta\gamma &= -c. \end{aligned}$$

Let $\omega = e^{2\pi i/3}$, and write

$$\alpha = \frac{1}{3}[(\alpha + \beta + \gamma) + (\alpha + \omega\beta + \omega^2\gamma) + (\alpha + \omega^2\beta + \omega\gamma)] = \frac{1}{3}(u + v),$$

where $u = \alpha + \omega\beta + \omega^2\gamma$, $v = \alpha + \omega^2\beta + \omega\gamma$. Then $u^3 + v^3$ and uv are unchanged under permuting α, β, γ.

After some calculations, we find that

$$\begin{aligned} u^3 + v^3 &= -27c, \\ uv &= -3b. \end{aligned}$$

Hence u^3 and v^3 are the roots of

$$X^2 + 27cX - 27b^3 = 0.$$

Solving this quadratic and taking cube roots gives a formula for the roots of a cubic, usually called Cardano's formula.

5.2 Formalising

Let S_n be the symmetric group on n letters.

Definition 5.1. Let R be a ring. A polynomial $f \in R[X_1, \ldots, X_n]$ is *symmetric* if

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n),$$

for all $\sigma \in S_n$. If f and g are symmetric, then so are $f + g$ and fg. Hence the symmetric polynomials form a subring of $R[X_1, \ldots, X_n]$.

Definition 5.2. The *elementary symmetric functions* are the polynomials $s_1, \ldots, s_n \in \mathbb{Z}[X_1, \ldots, X_n]$ such that

$$\prod_{i=1}^{n}(T + X_i) = T^n + s_1 T^{n-1} + \cdots + s_{n-1}T + s_n.$$

For example, for $n = 3$,

$$\begin{aligned} s_1 &= X_1 + X_2 + X_3, \\ s_2 &= X_1X_2 + X_2X_3 + X_3X_1, \\ s_3 &= X_1X_2X_3. \end{aligned}$$

In general,

$$s_r = \sum_{1 \le i_1 < \cdots < i_r \le n} X_{i_1}X_{i_2}\cdots X_{i_r}.$$

Theorem 5.1 (Symmetric function theorem)**.**

(i) *Every symmetric polynomial over R can be expressed as a polynomial in the elementary symmetric functions, with coefficients in R.*

(ii) *There are no nontrivial relations between the s_r.*

This says, if we consider the ring homomorphism

$$\begin{aligned} R[Y_1, \ldots, Y_n] &\xrightarrow{\theta} R[X_1, \ldots, X_n], \\ Y_i &\mapsto s_i, \end{aligned}$$

then $\mathrm{Im}(\theta)$ is the symmetric polynomials, and θ is injective.

Proof: Note we can write any $f \in R[X_1, \ldots, X_n]$ as $f = \sum f_d$, where f_d is homogeneous of degree d. Clearly f is symmetric if and only if all f_d are symmetric.

So for the proof of this theorem, it suffices to consider only symmetric and homogeneous polynomials. Define the *lexographic ordering* of monomials such that

$$X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} > X_1^{j_1}X_2^{j_2}\cdot X_n^{j_n}$$

if $i_1 = j_1, i_2 = j_2, \ldots, i_{r-1} = j_{r-1}, i_r > j_r$ for some $1 \le r \le n$. Then this is a total order.

Let $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ be the largest monomial to appear in f with non-zero

coefficient, say c. Then $X_{\sigma(1)}^{i_1} X_{\sigma(2)}^{i_2} \cdots X_{\sigma(n)}^{i_n}$ also appears in f for all $\sigma \in S_n$. Hence we must have $i_1 \geq i_2 \geq \cdots \geq i_n$.

Write

$$X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} = X_1^{i_1 - i_2} (X_1 X_2)^{i_2 - i_3} \cdots (X_1 X_2 \cdots X_n)^{i_n}.$$

Let $g = S_1^{i_1 - i_2} S_2^{i_2 - i_3} \cdots S_n^{i_n}$. Then f and g are both homogeneous of degree d and have the same largest monomial. So $f - cg$ is either 0, or it is a symmetric homogeneous polynomial of degree d whose leading monomial is smaller than that of f.

As there are only finitely many monomials of degree d, this process eventually terminates.

To prove part (ii), we will induct on n. Write $s_{r,n}$ instead of s_r to indicate the number of variables involved. Suppose we have $G \in R[Y_1, \ldots, Y_n]$ with $G(s_{1,n}, s_{2,n}, \ldots, s_{n,n}) = 0$. We must prove that $G = 0$.

The case for $n = 1$ is clear. Write $G = Y_n^k H$ with $Y_n \nmid H$, $k \geq 0$. Since $s_{n,n} = X_1 X_2 \ldots X_n$, it is not a zero divisor in $R[X_1, \ldots, X_n]$, we have $H(s_{1,n}, \ldots, s_{n,n}) = 0$.

So we may assume that G, if non-zero, is not divisible by Y_n. Replacing X_n by 0 gives

$$s_{r,n}(X_1, \ldots, X_{n-1}, 0) = \begin{cases} s_{r,n-1}(X_1, \ldots, X_{n-1}) & r < n, \\ 0 & r = n. \end{cases}$$

Therefore, $G(s_{1,n-1}, s_{2,n-1}, \ldots, s_{n-1,n-1}, 0)$. By the induction hypothesis, we get $G(Y_1, \ldots, Y_{n-1}, 0) = 0$. Hence $Y_n \mid G$, so $G = 0$.

Example 5.1.

Consider the symmetric polynomial

$$f = \sum_{i \neq j} X_i^2 X_j.$$

The leading term is $X_1^2 X_2 = X_1 (X_1 X_2)$. Hence looking at

$$s_1 s_2 = \sum_i \sum_{j<k} X_i X_j X_k = \sum_{i \neq j} X_i^2 X_j + 3 \sum_{i<j<k} X_i X_j X_k.$$

Hence we can subtract $3s_3$ to get $f = s_1 s_2 - 3s_3$.

Example 5.2.

Let $f(X) = \prod(X - \alpha_i)$ be a monic polynomial with roots $\alpha_1, \ldots, \alpha_n$. The *discriminant* of f is

$$\mathrm{Disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

By the symmetric function theorem, we can write $\mathrm{Disc}(f)$ as a polynomial in the coefficients of f. For example, if $n = 2$, then

$$f(X) = X^2 + bx + c = (X - \alpha_1)(X - \alpha_2).$$

Then the discriminant is

$$\mathrm{Disc}(f) = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c.$$

It is clear from the definition that

$$\mathrm{Disc}(f) = 0 \iff f \text{ has repeated roots.}$$

6 Normal and Separable Extensions

Definition 6.1. An extension L/K is *normal* if it is algebraic and the minimal polynomial of every $\alpha \in L$ splits into linear factors over L.

Equivalently, if $f \in K[X]$ is irreducible and has a root in L, then it splits into linear factors.

We can think of these as trade unions.

Theorem 6.1. *Let $[L : K] < \infty$. Then,*

$$L/K \text{ is normal} \iff L \text{ is a splitting field for some } f \in K[X].$$

Proof: As $[L : K] < \infty$, we can write $L = K(\alpha_1, \ldots, \alpha_n)$. Let f_i be the minimal polynomial of α_i over K. Then,

$$\begin{aligned} L/K \text{ normal} &\implies f_i \text{ splits into linear factors over } L \\ &\implies L \text{ is a splitting field for } \prod f_i. \end{aligned}$$

For the other way round, let L be the splitting field of $f \in K[X]$ over K. Let $\alpha \in L$ have minimal polynomial g over K.

Let M/L be a splitting field for g. We must show that whenever $\beta \in M$ is a root of g, then in fact $\beta \in L$. We know that $L = L(\alpha)$ is a splitting field for f over $K(\alpha)$, and $L(\beta)$ is a splitting field for f over $K(\beta)$.

But as α and β have the same minimal polynomial g over K, $K(\alpha)$ and $K(\beta)$ are K-isomorphic.

By the uniqueness of splitting fields, $L(\alpha)$ and $L(\beta)$ are K-isomorphic, so $[L : K] = [L(\beta) : K]$. By the tower law, this means $L(\beta) = L$, and so $\beta \in L$.

6.1 Separability

Over $\mathbb{R}$ or $\mathbb{C}$, we know from calculus that a polynomial f has a repeated root α if and only if

$$f(\alpha) = f'(\alpha) = 0.$$

To work over arbitrary fields, we proceed purely algebraically.

Definition 6.2. The formal derivative of

$$f = \sum_{i=0}^{d} c_i X^i \in K[X]$$

is

$$f' = \sum_{i=1}^{d} i c_i X^{i-1}.$$

This definition follows the Leibniz properties.

Lemma 6.1. *Let $f \in K[X]$ and $\alpha \in K$ a root of f. Then α is a simply root if and only if $f'(\alpha) = 0$.*

Proof: Write $f(X) = (X - \alpha)g(X)$ for some $g \in K[X]$. Then

$$\begin{aligned} \alpha \text{ is a simple root of } f &\iff X - \alpha \text{ is not a factor of } g \\ &\iff g(\alpha) \neq 0. \end{aligned}$$

But

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

By the gcd of polynomials $f, g \in K[X]$, not both zero, we mean the unique monic polynomial $\gcd(f, g)$ which generates the ideal $(f, g) \subset K[X]$.

This is the unique monic polynomial which divides both f and g, and can be written as $af + bg$ for some $a, b \in K[X]$.

We can compute $\gcd(f, g)$, together with a, b using Euclid's algorithm.

Lemma 6.2. *Let $f, g \in K[X]$ and let L/K be any field extension. Then* $\gcd(f, g)$ *is the same computed in $K[X]$ and in $L[X]$.*

Proof: Running Euclid's algorithm in $f, g \in K[X]$ gives the same answer whether we work in $K[X]$ or $L[X]$.

Definition 6.3. An irreducible polynomial $f \in K[X]$ is *separable* if it splits into distinct linear factors in a splitting field.

The convention in this course is that we use the same definition for any $0 \neq f \in K[X]$.

Anything which is not separable is called *inseparable*.

Lemma 6.3. *Let $0 \neq f \in K[X]$. Then*

$$f \text{ is separable} \iff \gcd(f, f') = 1.$$

Proof: Let L be a splitting field of f, for f separable. Then, then

$$\begin{aligned} f \text{ separable} &\iff f \text{ and } f' \text{ have no common roots in } L \\ &\iff \gcd(f, f') = 1 \text{ in } L[X] \\ &\iff \gcd(f, f') = 1 \text{ in } K[X]. \end{aligned}$$

Theorem 6.2. *Let $f \in K[X]$ be irreducible. Then f is separable unless* $\mathrm{char}(K) = p > 0$ *and $f(X) = g(X^p)$ for some $g \in K[X]$.*

Proof: Assume f is monic. Since f is irreducible, $\gcd(f, f') = 1$ or f. If $f' \neq 0$, then since $\deg f' < \deg f$, we have $\gcd(f, f') \neq f$, hence $\gcd(f, f') = 1$ and f is separable.

Now suppose that $f' = 0$. If

$$f = \sum_{i=0}^{d} c_i X^i \implies f' = \sum_{i=1}^{d} i c_i X^{i-1},$$

so $f' = 0 \implies ic_i = 0$. If $\mathrm{char}(K) = 0$, then this implies $c_i = 0$ for all $1 \leq i \leq d$. So f is constant, hence irreducible.

If $\mathrm{char}(K) = p > 0$, then we still get $c_i = 0$ for all i with $p \nmid i$. Hence $f(X) = g(X^p)$ for some $g \in K[X]$.

Definition 6.4. Let L/K be a field extension.

(a) $\alpha \in L$ is separable over K if it is algebraic over K and its minimal polynomial is separable.

(b) L/K is separable if every $\alpha \in L$ is separable. In particular, L/K is algebraic.

Theorem 6.3 (Primitive Element)**.** *If L/K is finite and separable, then $L = K(\theta)$ for some $\theta \in L$.*

Proof: Write $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in L$. We must show that $L = K(\theta)$ for some $\theta \in L$.

It suffices to prove the case $n = 2$, since the general case follows by induction on n. Write $L = K(\alpha, \beta)$ and let f be the minimal polynomial of α over K, and g the minimal polynomial of β over K.

Let M be the splitting field for fg over L. Then if we write

$$f(X) = \prod_{i=1}^{r}(X - \alpha_i), \qquad g(X) = \prod_{i=1}^{s}(X - \beta_i),$$

for $\alpha_i, \beta_j \in M$ and $\alpha_1 = \alpha$, $\beta_1 = \beta$, then

$$L/K \text{ separable} \implies \beta \text{ separable over } K \implies \beta_1, \ldots, \beta_s \text{ distinct.}$$

We pick some $c \in K$ and let $\theta = \alpha + c\beta$. Let

$$F(X) = f(\theta - cX) \in K(\theta)[X].$$

Then,

$$F(\beta) = f(\theta - c\beta) = f(\alpha) = 0,$$

and also $g(\beta) = 0$, so if $\beta_2, \ldots, \beta_s$ are not roots of F, then

$$\begin{aligned} &\gcd(F, g) = X - \beta \text{ in } M[X] \\ \implies &\gcd(F, g) = X - \beta \text{ in } K(\theta)[X] \\ \implies &\beta \in K(\theta). \end{aligned}$$

But then $\alpha = \theta - c\beta \in K(\theta)$, so $K(\alpha, \beta) \subset K(\theta)$. But clearly $K(\theta) \subset K(\alpha, \beta)$, so $K(\alpha, \beta) = K(\theta)$.

We are done unless $F(\beta_j) = 0$ for some $2 \leq j \leq s$. But then $f(\theta - c\beta_j) = 0$, so

$$\alpha + c\beta = \alpha_i + c\beta_j$$

for some $1 \leq i \leq r$, $2 \leq j \leq s$. If $|K| = \infty$, then since $\beta \notin \{\beta_2, \ldots, \beta_s\}$, we can pick $c \in K$ such that this never happens.

If $|K| < \infty$, then $|L| < \infty$ and hence $L^\times$ is cyclic generated by θ, so $L = K(\theta)$.

Example 6.1.

We saw in a previous example that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Remark. The above theorems show that if $[K : \mathbb{Q}] < \infty$, then $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$.

Our aim is to show that if L/K is a field extension, and $\alpha_1, \ldots, \alpha_n \in L$, then

$$\alpha_1, \ldots, \alpha_n \text{ separable over } K \iff K(\alpha_1, \ldots, \alpha_n)/K \text{ is separable.}$$

For L/K, M/K field extensions, we write $\mathrm{Hom}_K(L, M)$ to denote the number of K-embeddings from L into M.

Lemma 6.4. *Let $[L : K] < \infty$. Suppose $L = K(\alpha)$, and f is the minimal polynomial of α over K. Let M/K be any field extension. Then*

$$|\mathrm{Hom}_K(L, M)| \leq [L : K],$$

with equality if and only if f splits into distinct linear factors over M.

Proof: We know from before that

$$|\mathrm{Hom}_K(L, M)| = |\{\text{roots of } f \text{ in } M\}| \leq \deg f = [L : K],$$

with equality if and only if f splits into distinct linear factors over M.

Theorem 6.4. *Let $[L : K] < \infty$. Write $L = K(\alpha_1, \ldots, \alpha_n)$ and let f_i be the minimal polynomial of α_i over K. Let M/K be any field extension. Then,*

$$|\mathrm{Hom}_K(L, M)| \leq [L : K],$$

with equality if and only if f_i splits into distinct linear factors over M.

We can easily extend this theorem as follows:

Theorem 6.5. *Let $\sigma : K \to M$ be an embedding. Then*

$$|\{\sigma\text{-homomorphisms } L \to M\}| \leq [L : K],$$

with equality if and only if each $\sigma(f_i)$ splits into distinct linear factors over M.

We will use this variant in the induction argument.

Proof: We will prove this by induction on n. The case $n = 1$ has already been proven, so suppose $n > 1$.

Let $K_1 = K(\alpha_1)$. Then from the above lemma,

$$|\mathrm{Hom}_K(K_1, M)| \leq [K_1 : K]. \tag{1}$$

Let $\sigma \in \mathrm{Hom}_K(K_1, M)$. Then by the induction hypothesis, the number of

σ-homomorphisms

$$|\{\sigma\text{-homomorphisms } L = K_1(\alpha_2, \ldots, \alpha_n) \to M\}| \leq [L : K_1]. \qquad (2)$$

Hence the number of homomorphisms is

$$|\mathrm{Hom}_K(L, M)| \leq [L : K_1][K_1 : K] = [L : K].$$

Note if equality holds then equality holds in both inequalities above. (1) gives that f_1 splits into distinct linear factors over M. But reordering α_i gives the same conclusion for all the f_i.

Conversely, if each f_i splits into distinct linear factors, then we get equality in (1).

Moreover, for $2 \leq i \leq n$ the minimal polynomial of α_i over K_1 divides the minimal polynomial of α_i over K, hence f_i splits into distinct linear factors over M.

By the induction hypothesis, this gives equality everywhere.

Corollary 6.1. *Let $[L : K] < \infty$, and write $L = K(\alpha_1, \ldots, \alpha_n)$. Let f_i be the minimal polynomial of α_i over K. Let M/K be any field extension in which $\prod f_i$ splits as a product of linear factors. Then the following are equivalent:*

(i) *L/K is separable.*

(ii) *Each α_i is separable over K.*

(iii) *Each f_i splits into distinct linear factors over M.*

(iv) $|\mathrm{Hom}_K(L, M)| = [L : K]$.

Proof: (i) $\implies$ (ii) $\implies$ (iii) by definition, and (iii) $\implies$ (iv) as we have just shown.

To show (iv) $\implies$ (i), let $\beta \in L$. Then applying this theorem to $L = K(\alpha_1, \ldots, \alpha_n, \beta)$ shows that β is separable over K.

(iv) is a useful characterisation of separable extensions.

Example 6.2.

Let K be any field. The polynomial $T^n - Y \in K[Y, T]$ is irreducible:

It suffices to consider factorizations of the form $f(T)(g(T) + Yh(T))$, where $f, g, h \in K[T]$. Since $K[Y]$ is a UFD with field of fractions $K(Y)$, it follows by Gauss' lemma that

$$T^n - Y \in K(Y)[T]$$

is irreducible. The field extension $K(X)/K(X^n)$ is generated by X which is a root of $T^n - X^n \in K(X^n)[T]$. Putting $Y = X^n$ in this shows it is irreducible, and $[K(X) : K(X^n)] = n$.

Now take $K = \mathbb{F}_p$ and $n = p$. We claim that $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$ is an inseparable extension of degree p. Indeed, the minimal polynomial of X over $\mathbb{F}_p(X^p)$ is

$$f(T) = T^p - X^p \in \mathbb{F}_p(X^p)[T],$$

which is inseparable since

$$f(T) = (T - X)^p.$$

7 Galois Extensions

Definition 7.1. An *automorphism* of a field L is a bijective homomorphism $\sigma : L \to L$. We write $\mathrm{Aut}(K)$ for the group of automorphisms of L under composition.

Note if σ is a homomorphism, then so is σ^{-1}.

Definition 7.2. Let L/K be a field extension. A *K-automorphism* of L is an automorphism $\sigma \in \mathrm{Aut}(L)$, whose restriction to K is the identity map.

The K-automorphisms of L form a subgroup $\mathrm{Aut}(L/K) < \mathrm{Aut}(L)$.

Remark.

(i) $\mathrm{Aut}(\mathbb{Q})$ and $\mathrm{Aut}(\mathbb{F}_p)$ are both trivial, as $\mathrm{Aut}(L) = \mathrm{Aut}(L/K)$, where K is the prime subfield of L.

(ii) If $[L : K] < \infty$, then any K-embedding $L \to L$ is surjective, i.e. $\mathrm{Hom}_K(L, L) = \mathrm{Aut}(L/K)$.

Lemma 7.1. *Let L/K be a finite extension. Then*

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

Proof: Take $M = L$ in theorem (6.4).

Definition 7.3. If $S \subset \mathrm{Aut}(L)$ is any subset, we define the *fixed field* of S to be

$$L^S = \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in S\}.$$

This is a subfield of L.

Definition 7.4. A field extension L/K is *Galois* if it is algebraic and

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

In essence, the automorphisms which fix K don't fix anything else.

Example 7.1.

(i) $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$, where τ is complex conjugation.

If $z \in \mathbb{C}$, then

$$z \in \mathbb{R} \iff \tau(z) = z.$$

Hence $\mathbb{C}/\mathbb{R}$ is Galois.

(ii) Let $L = \mathbb{Q}(\sqrt{2})$, $f(X) = X^2 - 2$. Then

$$\mathrm{Aut}(L/\mathbb{Q}) \leftrightarrow \{\text{roots of } f \text{ in } L\},$$

hence $\mathrm{Aut}(L/\mathbb{Q}) = \{1, \tau\}$, where

$$\tau(a + b\sqrt{2}) = a - b\sqrt{2},$$

for $a, b \in \mathbb{Q}$. Then $L^\tau = \mathbb{Q}$, so $L/\mathbb{Q}$ is Galois.

(iii) Let $L = \mathbb{Q}(\sqrt[3]{2})$, and $f(X) = x^3 - 2$. Then $\mathrm{Aut}(L/\mathbb{Q})$ corresponds with the number of roots of f in L.

But since $L \subset \mathbb{R}$, we have $\mathrm{Aut}(L/\mathbb{Q}) = 1$, so $L/\mathbb{Q}$ is not Galois.

(iv) Let $K/\mathbb{F}_p$ be a finite extension, and let $\phi : K \to K$ be $x \mapsto x^p$.

Then $\phi \in \mathrm{Aut}(K/\mathbb{F}_p)$, so $K^\phi = \{x \in K \mid \phi(x) = x\} = \{\text{roots of } X^p - x \text{ in } K\} \supset \mathbb{F}_p$. So $K/\mathbb{F}_p$ is Galois.

Theorem 7.1. *Let $[L : K] < \infty$, and $G = \mathrm{Aut}(L/K)$. The following are equivalent:*

(i) *L/K is Galois.*

(ii) *L/K is normal and separable.*

(iii) *L is the splitting field of a separable polynomial over K.*

(iv) *$|G| = [L : K]$.*

Proof: To show (i) $\implies$ (ii), let $\alpha \in L$ and $\{\sigma(\alpha) \mid \sigma \in G\} = \{\alpha_1, \ldots, \alpha_m\}$, with $\alpha_1, \ldots, \alpha_m$ distinct. Then let

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i).$$

We let $\sigma \in G$ act on $L[X]$ by

$$\sigma\left(\sum c_i X^i\right) = \sum \sigma(c_i) X^i.$$

Since G permutes the α_i, we have $\sigma f = f$ for all $\sigma \in G$.

Hence if L/K Galois, then $f \in K[X]$. So let g be the minimal polynomial of α over K. Since $f(\alpha) = 0$, we have $g|f$, but as $g(\sigma(\alpha)) = \sigma(g(\alpha)) = 0$ for all $\sigma \in G$, every root of f is a root of g.

By construction, f is separable and monic, so $f = g$. Hence the minimal polynomial of α over K splits into distinct linear factors over L. Since $\alpha \in L$ was arbitrary, this shows that L/K is normal and separable.

For (ii) $\implies$ (iii), theorem 6.1 says that L is the splitting field of some $f \in K[X]$. Hence write

$$f = \prod_{i=1}^{m} f_i^{e_i},$$

where the $f_i \in K[X]$ are distinct irreducibles, and $e_i \geq i$. Then, L/K separable implies each f_i is separable. Moreover, as $\gcd(f_i, f_j) = 1$ in $K[X]$, then $\gcd(f_i, f_j) = 1$ in $L[X]$, so

$$g = \prod_{i=1}^{m} f_i$$

is separable, and L is a splitting field for g over K.

To show (iii) $\implies$ (iv), let L be the splitting field of a separable polynomial $f \in K[X]$. Then $L = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of f.

The minimal polynomial f_i of each α_i divides f, and so splits into distinct linear factors over L.

Taking $M = L$ in theorem 6.4 gives $|\mathrm{Aut}(L/K)| = [L : K]$.

Finally, to show (iv) $\implies$ (i), note that

$$G \leq \mathrm{Aut}(L/L^G) \leq \mathrm{Aut}(L/K) = G,$$

hence $G = \mathrm{Aut}(L/L^G)$. Therefore,

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

which gives

$$[L : L^G][L^G : K] \leq [L : L^G],$$

so $L^G = K$.

Definition 7.5. If L/K is a Galois extension, then we write $\mathrm{Gal}(L/K)$ for $\mathrm{Aut}(L/K)$. This is called the *Galois group* of L over K.

Remark. We saw in this proof that if L/K is Galois and $\alpha \in L$, then the minimal polynomial of α over K is

$$\prod_{i=1}^{m}(X - \alpha_i),$$

where $\alpha_1, \ldots, \alpha_m$ are the distinct elements of $\{\sigma(\alpha) \mid \sigma \in G\}$.

Theorem 7.2 (Fundamental Theorem of Galois Theory)**.** *Let L/K be a finite Galois extension, $G = \mathrm{Gal}(L/K)$.*

(i) *Let F be an intermediate field, $K \subset F \subset L$. Then L/F is Galois and $\mathrm{Gal}(L/F)$ is a subgroup of G.*

(ii) *There is an inclusion reversing bijection from the intermediate fields to subgroups of G, by*

$$\begin{aligned} F &\mapsto \mathrm{Gal}(L/F) \\ L^H &\hookleftarrow H. \end{aligned}$$

(iii) *Let F be an intermediate field. Then,*

$$\begin{aligned} F/K \text{ Galois} &\iff \sigma F = F \text{ for all } \sigma \in G \\ &\iff H = \mathrm{Gal}(L/F) \text{ is a normal subgroup of } G. \end{aligned}$$

In this case, the restriction map

$$\begin{aligned} G &\to \mathrm{Gal}(F/K) \\ \sigma &\mapsto \sigma|_F \end{aligned}$$

is surjective with kernel H, and so

$$\mathrm{Gal}(F/K) \cong G/H.$$

Proof: (i). By theorem 7.1, L is the splitting field of some separable polynomial $f \in K[X]$.

Then L is the splitting field of f over F, so L/F is Galois, and $\mathrm{Gal}(L/F)$ is a subgroup of $\mathrm{Gal}(L/K)$ since any automorphism of L acting as the identity on F also acts as the identity on K.

(ii) To show we have a bijection, we need to check that both compositions are the identity.

First, note that $F = L^{\mathrm{Gal}(L/F)}$. This holds as L/F is Galois, so by our previous theorem we are done.

Then it suffices to prove that $\mathrm{Gal}(L/L^H) = H$. We certainly have $H \leq \mathrm{Gal}(L/L^H)$, so it suffices to show that

$$|\mathrm{Gal}(L/L^H)| \leq |H|.$$

Let $F = L^H$. As L/F is finite and separable, the theorem of the primitive element tells us that $L = F(\alpha)$ for some $\alpha \in L$.

Then α is a root of

$$f(X) = \prod_{\sigma \in H} (X - \sigma(\alpha)),$$

which has coefficients in $L^H = F$. Therefore,

$$|\mathrm{Gal}(L/L^H)| = [L : L^H] = [F(\alpha) : F] \leq \deg f = |H|,$$

as required. Now if $F_1 \subset F_2$, then $\mathrm{Gal}(L/F_2) \subset \mathrm{Gal}(L/F_1)$, so the bijection reverses inclusions.

(iii). We first show that F/K is Galois if and only if $\sigma F = F$ for all $\sigma \in G$.

$\implies$ For the forwards direction, let $\alpha \in F$ have minimal polynomial f over K. Then for any $\sigma \in G$, $\sigma(\alpha)$ is a root of f.

Since F/K is normal, we have $\sigma(\alpha) \in F$. Hence $\sigma(F) \subset F$. As $[\sigma F : K] = [F : K]$, it follows that $\sigma F = F$.

$\impliedby$ Now for the backwards direction. Assume that $\sigma F = F$. Let $\alpha \in F$, then its minimum polynomial over K is

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i),$$

where $\{\alpha_1, \ldots, \alpha_m\}$ are the distinct elements of $\{\sigma(\alpha) \mid \sigma \in G\}$. The assumption that $\sigma(F) = F$ tells us that $\alpha_1, \ldots, \alpha_m \in F$, hence F/K is normal.

But also as L/K is Galois, L/K is separable, hence F/K is separable. So F/K is normal and separable, hence it is Galois.

Now suppose $H \leq G$ corresponds to $F = L^H$. Then for $\sigma \in G$, we have

$$\begin{aligned} L^{\sigma H \sigma^{-1}} &= \{x \in L \mid \sigma\tau\sigma^{-1}(x) = x \text{ for all } \tau \in H\} \\ &= \{x \in L \mid \tau\sigma^{-1}(x) = \sigma^{-1}(x) \text{ for all } \tau \in H\} \\ &= \{x \in L \mid \sigma^{-1}(x) \in L^H = F\} \\ &= \sigma F, \end{aligned}$$

hence as $\sigma F = F$ for all $\sigma \in G$, $L^{\sigma H \sigma^{-1}} = L^H$ for all $\sigma \in G$, hence $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$, so $H \leq G$ is a normal subgroup.

Now for the third part. Consider the restriction map res. Then

$$\begin{aligned} \mathrm{Ker}(\mathrm{res}) &= \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) = x \text{ for all } x \in F\} \\ &= \mathrm{Gal}(L/F) = H, \end{aligned}$$

so $G/H \cong \mathrm{Im}(\mathrm{res}) \leq \mathrm{Gal}(L/K)$. But,

$$|G/H| = \frac{|G|}{|H|} = \frac{[L:K]}{[L:H]} = [F:K] = |\mathrm{Gal}(F/K)|,$$

so res is surjective, and $\mathrm{Gal}(F/K) = G/H$.

Example 7.2.

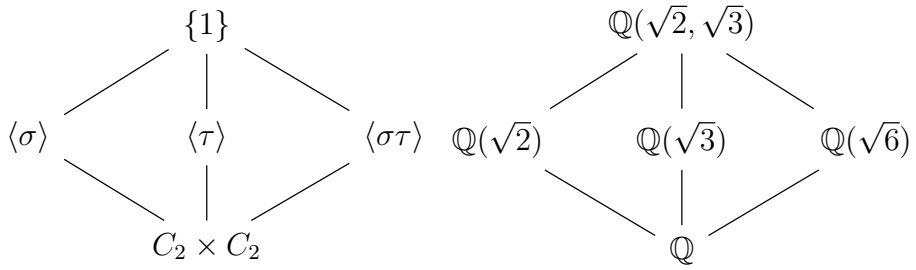
Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $K/\mathbb{Q}$ is the splitting field of the polynomial $(X^2 - 2)(X^2 - 3)$. So $K/\mathbb{Q}$ is normal, and hence Galois.

Now if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then it is uniquely determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$. Since $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(\sqrt{3}) = \pm\sqrt{3}$, we have $|\mathrm{Gal}(K/\mathbb{Q})| \leq 4$.

But we saw before that $[K : \mathbb{Q}] = 4$, hence $|\mathrm{Gal}(K/\mathbb{Q})| = 4$, so letting

$$\begin{aligned} \sigma &: \sqrt{2} \mapsto \sqrt{2}, & \sqrt{3} &\mapsto -\sqrt{3}, \\ \tau &: \sqrt{2} \mapsto -\sqrt{2}, & \sqrt{3} &\mapsto \sqrt{3}, \end{aligned}$$

then $\sigma^2 = \tau^2 = \mathrm{id}$, and $\sigma\tau = \tau\sigma$, so $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2$.



Example 7.3.

Let $K = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{2+\sqrt{2}}$. Then $(\alpha^2-2)^2 = 2$, so α is a root of $f(X) = X^4 - 4X^2 + 2$.

This is irreducible in $\mathbb{Z}[X]$ by Eisenstein's criterion with $p = 2$, hence is irreducible in $\mathbb{Q}[X]$ by Gauss' lemma, so $[K : \mathbb{Q}] = 4$.

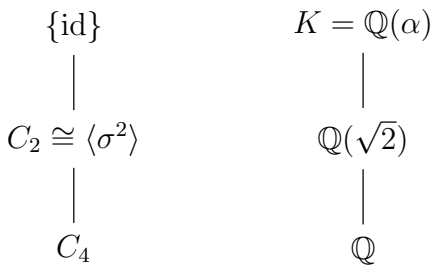
Now $(2+\sqrt{2})(2-\sqrt{2}) = 2$, so f has roots $\pm a$ and $\pm\sqrt{2}/\alpha$. Hence K is a splitting field for f over $\mathbb{Q}$, so $K/\mathbb{Q}$ is both normal and Galois.

So $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is uniquely determined by $\sigma(\alpha)$, but $\sigma(\alpha) = \{\pm\alpha, \pm\sqrt{2}/\alpha\}$ and $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 4$, so all possibilities must occur.

Fix $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ with $\sigma(\alpha) = \sqrt{2}/\alpha$. Then $\sigma(\alpha^2) = 2/\alpha^2$, hence $\sigma(2+\sqrt{2}) = 2-\sqrt{2}$, and $\sigma(\sqrt{2}) = -\sqrt{2}$.

Hence $\sigma^2(\alpha) = \sigma(\sqrt{2}/\alpha) = -\sqrt{2}/(\sqrt{2}/\alpha) = -\alpha$, so $\sigma^2 \neq \mathrm{id}$, but $\sigma^4 = \mathrm{id}$.

Hence $\mathrm{Gal}(K/\mathbb{Q}) \cong C_4$.



Definition 7.6. Let L_1, L_2 be subfields of a field M. The *composite* L_1L_2 is the smallest subfield of M to contain both L_1 and L_2.

This exists, as the intersection of any collections of subfield is a subfield.

Theorem 7.3. *Let $[M : K] < \infty$, and let L_1, L_2 be intermediate field.*

(i) *If L_1/K is Galois, then L_1L_2/L_2 is Galois and there is an injective group homomorphism*

$$\mathrm{Gal}(L_1L_2/L_2) \hookrightarrow \mathrm{Gal}(L_1/K).$$

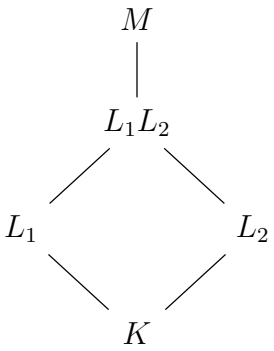
This is surjective if and only if $L_1 \cap L_2 = K$.

(ii) *If L_1/K and L_2/K are both Galois, then L_1L_2/K is Galois, and there is an injective group homomorphism*

$$\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K).$$

This is surjective if and only if $L_1 \cap L_2 = K$.

Proof: Let's draw a diagram.



(i) First L_1/K is Galois implies L_1 is the splitting field of some separable polynomial $f \in K[X]$. Then L_1L_2 is the splitting field for f over L_2, so L_1L_2/L_2 is Galois.

Now if $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$, then $\sigma|_K = \mathrm{id}$, and since L_1/K is Galois, we have $\sigma(L_1) = L_1$.

We consider the group homomorphism

$$\begin{aligned} \mathrm{Gal}(L_1L_2/L_2) &\to \mathrm{Gal}(L_1/K) \\ \sigma &\mapsto \sigma|_{L_1}. \end{aligned}$$

It is injective, since if $\sigma|_{L_1} = \mathrm{id}$, then σ acts trivially on both L_1 and L_2, hence on L_1L_2.

Now suppose $L_1 \cap L_2 = K$. Then L_1/K is finite and separable, so $L_1 = K(\alpha)$ for some $\alpha \in L_1$. Let $f \in K[X]$ be the minimal polynomial of α over K.

Suppose $f = gh$ for some $g, h \in L_2[X]$. Then as f splits into linear factors over L_1, g and h have coefficients in $L_1 \cap L_2 = K$, which is a contradiction to f irreducible over K. So f is irreducible in $L_2[X]$, and

$$[L_1 : K] = \deg f = [L_1L_2 : L_2].$$

So the map res is an isomorphism. Conversely, $\mathrm{Im}(\mathrm{res}) \leq \mathrm{Gal}(L_1/L_1 \cap L_2) \leq \mathrm{Gal}(L_1/K)$, so if res is surjective, then $L_1 \cap L_2 = K$.

(ii) Note if L_i/K is Galois, then L_i is a splitting field of some separable polynomial $f_i \in K[X]$.

Then L_1L_2 is the splitting field of the separable polynomial $\mathrm{lcm}(f_1, f_2)$, so L_1L_2/K is Galois.

If $\sigma \in \mathrm{Gal}(L_1L_2/K)$, then $\sigma|_K = \mathrm{id}$ and since L_i/K is normal, $\sigma(K_i) = K_i$. Now consider the group homomorphism

$$\begin{aligned} \mathrm{Gal}(L_1L_2/K) &\to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \\ \sigma &\mapsto (\sigma|_{L_1}, \sigma_{L_2}) \end{aligned}$$

This is injective, since if both $\sigma|_{L_1} = \mathrm{id}$ and $\sigma|_{L_2} = \mathrm{id}$, then σ acts trivially on L_1L_2.

Moreover,

$$\begin{aligned} \text{map is surjective} &\iff [L_1L_2 : K] = [L_1 : K][L_2 : L] \\ &\iff [L_1L_2 : L_2][L_2 : K] = [L_1 : K][L_2 : K] \\ &\iff [L_1L_2 : L_2] = [L_1 : K] \\ &\iff L_1 \cap L_2 = K. \end{aligned}$$

Theorem 7.4. *Let L/K be finite and separable. Then there exists finite extension M/L such that:*

(i) *M/K is Galois.*

(ii) *If $L \subset M' \subset M$ and M'/K is Galois, then $M' = M$.*

We say M/K is a Galois closure *of L/K.*

Proof: By the theorem of the primitive element, $L = K(\alpha)$ for some $\alpha \in L$. Let f be the minimal polynomial of α over K.

Then as L/K is separable, f is separable. Let M be a splitting field for f over K. Then since $L = K(\alpha)$ where α is a root of f, it follows that M is a splitting field of f over K.

Hence by theorem 7.1, M/K is Galois. Now let M' be intermediary and Galois. As $\alpha \in M'$ and M'/K is normal, f splits into linear factors over M'. Hence $M' = M$.

Example 7.4.

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has Galois closure $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$, where $\omega = e^{2\pi i/3}$.

8 Trace and Norm

Let L/K be a finite extension, say $[L:K] = n$. For $\alpha \in L$, the map $m_\alpha : x \mapsto \alpha x$ is K-linear endomorphism of L, hence it has a trace and determinant.

Definition 8.1. The *trace* and *norm* of α are:

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}(m_\alpha), \qquad N_{L/K}(\alpha) = \det(m_\alpha).$$

Concretely, if L has K-basis $v_1, \ldots, v_n$ and $A = (a_{ij})$ is the unique $n \times n$ matrices with entries in K such that

$$\alpha(v_j) = \sum_{i=1}^{n} a_{ij} v_i,$$

then $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}\, A$ and $N_{L/K}(\alpha) = \det A$.

Example 8.1.

Let $K = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$. If $\alpha = x + y\sqrt{d}$, then L has K-basis $1, \sqrt{d}$ and in this basis we can compute

$$\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) = \mathrm{tr} \begin{pmatrix} x & dy \\ y & x \end{pmatrix} = 2x,$$
$$N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) = \det \begin{pmatrix} x & dy \\ y & x \end{pmatrix} = x^2 - dy^2.$$

Lemma 8.1.

(i) $\mathrm{Tr}_{L/K} : L \to K$ *is a* K*-linear map.*

(ii) $N_{L/K} : L \to K$ *is multiplicative.*

(iii) *If* $\alpha \in K$, *then* $\mathrm{Tr}_{L/K}(\alpha) = [L:K]\alpha$, $N_{L/K}(\alpha) = \alpha^{[L:K]}$.

(iv) *If* $\alpha \in L$, *then*

$$N_{L/K}(\alpha) = 0 \iff \alpha = 0.$$

Proof: (i) and (ii) follow from the corresponding statements for traces and determinants.

(iii) If $\alpha \in K$, then m_α is represented by αI_n, which has trace and determinant as indicated.

(iv) $N_{L/K}(\alpha) \neq 0 \iff m_\alpha$ is invertible $\iff \alpha \neq 0$.

Lemma 8.2. *Let $M/L/K$ be field extensions, and $\alpha \in L$. Then*

$$\mathrm{Tr}_{M/K}(\alpha) = [M : L] \mathrm{Tr}_{L/K}(\alpha), \qquad N_{M/K}(\alpha) = N_{L/K}(\alpha)^{[M:L]}.$$

Proof: If A represents m_α with respect to some basis for L/K, and B represents m_α with respect to some basis for M/K picked by following the proof of the tower law, then

$$B = \begin{pmatrix} A & & & 0 \\ & A & & \\ & & \ddots & \\ 0 & & & A \end{pmatrix}.$$

Here A is $[L : K] \times [L : K]$, and B is $[M : K] \times [M : K]$. Then $\mathrm{tr}(B) = [M : L] \mathrm{tr}(A)$, and $\det(B) = \det(A)^{[M:L]}$.

Theorem 8.1. *Let $[L : K] < \infty$, and let $\alpha \in L$. Let f be the minimal polynomial of α over K, and say*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots a_1 X + a_0,$$

for $a_i \in K$.

Then $\mathrm{Tr}_{L/K}(\alpha) = -ma_{n-1}$, where $m = [L : K(\alpha)]$, and $N_{L/K}(\alpha) = ((-1)^n a_0)^m$.

Proof: By lemma 8.2, without loss of generality let $L = K(\alpha)$. If A represents m_α with respect to basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, then

$$A = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ 0 & & & 1 & -a_{n-1}, \end{pmatrix}$$

which has trace $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}(A) = -a_{n-1}$, and norm $N_{L/K}(\alpha) = \det(A) = (-1)^n a_0$.

Example 8.2.

Let $K = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt{d})$. If $\alpha = x + y\sqrt{d}$, then $(\alpha - x)^2 - dy^2$, so α is a root of

$$T^2 - 2xT + x^2 - dy^2 = 0.$$

This gives the same trace and norm from before.

Theorem 8.2 (Transitivity of Trace and Norm)**.** *Let $M/L/K$ be finite extensions and $\alpha \in M$. Then*

$$\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)),$$
$$N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha)).$$

Proof: Just a sketch - this proof is non-examinable.

By lemma 8.2, without loss of generality let $M = L(\alpha)$. Let f be the minimum polynomial of α over L, say

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0,$$

for $a_i \in L$. Then suppose L/K has basis $v_1, \ldots, v_m$, and M/L has basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

If A_i represents m_{a_i} with respect to $v_1, \ldots, v_m$ and B represents m_α with respect to $(v_i\alpha^{j-1})$, then

$$B = \begin{pmatrix} 0 & & & & -A_0 \\ I & 0 & & & -A_1 \\ 0 & I & \ddots & & \vdots \\ & & \ddots & 0 & \vdots \\ 0 & & & I & -A_{n-1} \end{pmatrix},$$

where A_i is $m \times m$ and B is $mn \times mn$. We compute

$$\mathrm{Tr}_{M/K}(\alpha) = \mathrm{tr}(B) = -\mathrm{tr}(A_{n-1}) = \mathrm{Tr}_{L/K}(-a_{n-1}) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)),$$

$$N_{M/K}(\alpha) = \det(B) = (-1)^{mn}\det(A_0) = N_{L/K}((-1)^n a_0) = N_{L/K}(N_{M/L}(\alpha)).$$

Theorem 8.3. *Let L/K be a finite Galois extension with $G = \mathrm{Gal}(L/K)$. Let*

$\alpha \in L$. *Then*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha), \qquad N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

Proof: Note that the minimal polynomial of α over K is

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i),$$

where $\{\alpha_1, \ldots, \alpha_n\} = \{\sigma(\alpha) \mid \sigma \in G\}$. Let $m = [L : K(\alpha)] = |\mathrm{Stab}_G(\alpha)|$. Then

$$\mathrm{Tr}_{L/K}(\alpha) = m \sum_{i=1}^{n} \alpha_i = \sum_{\sigma \in G} \sigma(\alpha),$$
$$N_{L/K}(\alpha) = \left(\prod_{i=1}^{n} \alpha_i \right)^m = \prod_{\sigma \in G} \sigma(\alpha).$$

Example 8.3.

Once again take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{d})$. Then L/K is Galois and $\mathrm{Gal}(L/K) = \{1, \sigma\}$, where $\sigma(\sqrt{d}) = \sqrt{d}$. For $\alpha = x + y\sqrt{d}$, we have

$$\mathrm{Tr}_{L/K}(\alpha) = (x + y\sqrt{d}) + (x - y\sqrt{d}) = 2x,$$

$$N_{L/K}(\alpha) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

We can actually generalise the above theorem to L/K separable. Let $\bar{K}$ be an algebraic closure of K.

Corollary 8.1. $|\mathrm{Hom}_K(L, \bar{K})| = [L : K]$.

Theorem 8.4. *Let L/K be a finite separable extension of degree d. Let $\sigma_1, \ldots, \sigma_d$ be the K-embeddings $L \hookrightarrow \bar{K}$, and let $\alpha \in L$. Then,*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha), \qquad N_{L/K}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha).$$

Proof: Let f be the minimal polynomial of α over K. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\bar{K}$. By theorem 4.2,

$$\begin{aligned} \mathrm{Hom}_K(K(\alpha), \bar{K}) &\leftrightarrow \{\alpha_1, \ldots, \alpha_n\} \\ \sigma &\mapsto \sigma(\alpha). \end{aligned}$$

Since $L/K(\alpha)$ is separable, each K-embedding $K(\alpha) \hookrightarrow \bar{K}$ extends to an embedding $L \hookrightarrow \bar{K}$ in exactly $m = [L : K(\alpha)]$ ways. Hence

$$\begin{aligned} \mathrm{Tr}_{L/K}(\alpha) &= m \sum_{j=1}^{n} \alpha_j = \sum_{i=1}^{d} \sigma_i(\alpha), \\ N_{L/K}(\alpha) &= \left(\prod_{j=1}^{n} \alpha_j \right)^m = \prod_{i=1}^{d} \sigma_i(\alpha_i). \end{aligned}$$

9 Finite Fields

Fix p a prime number. Recall that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In this section we describe all finite fields of characteristic p and their Galois theories. Recall the following:

Proposition 9.1.

(i) *If K is a finite field of characteristic p, then $|K| = p^n$, where $n = [K : \mathbb{F}_p]$.*

(ii) *$K^\times$ is cyclic of order $p^n - 1$.*

(iii) *$\phi : K \to K$, $\phi(x) = x^p$ is a ring homomorphism, which is an automorphism in finite fields.*

Theorem 9.1. *Let $q = p^n$ for some $n \geq 1$.*

(i) *There exists a field with q elements.*

(ii) *Any field with q elements is a splitting field of $X^q - X$ over $\mathbb{F}_p$.*

In particular, any two finite fields with the same order are isomorphic.

Proof:

(i) Let L be a splitting field of $f(X) = X^q - X$ over $\mathbb{F}_p$. Let $K \subset L$ be the fixed field of $\phi^n : x \mapsto x^q$. Then

$$K = \{\alpha \in L \mid \phi^n(\alpha) = \alpha\} = \{\alpha \in L \mid f(\alpha) = 0\}.$$

But $f'(X) = -1$, so $\gcd(f, f') = 1$, hence f is separable, and so $|K| = q$.

(ii) Suppose K is a field with $|K| = q$. Then from Lagrange's theorem $\alpha^{q-1} = 1$ for all $\alpha \in K^\times$, hence $\alpha^q = \alpha$ for all $\alpha \in K$. So we can factor

$$f(X) = X^q - X = \prod_{\alpha \in K} (X - \alpha),$$

hence f splits over K. Moreover it cannot split over any proper subfield due to size constraints, so K is the splitting field of f.

In the following, write $\mathbb{F}_q$ for any field with q elements. By the above theorem, any two such fields are isomorphic, although there is no canonical choice of isomorphism.

Theorem 9.2. *$\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ cyclic of order n, generated by the Frobenius map $\phi : x \to x^p$.*

Proof: Let $L = \mathbb{F}_{p^n}$, and let $G \subset \mathrm{Aut}(L/\mathbb{F}_p)$ be the subgroup generated by ϕ. Then

$$|L^G| = |L^\phi| = |\{\alpha \in L \mid \alpha^p - \alpha = 0\} \leq p.$$

But as $\mathbb{F}_p \subset L^G$, $L^G = \mathbb{F}_p$. hence

$$\mathbb{F}_p \subset L^{\mathrm{Aut}(L/\mathbb{F}_p)} \subset L^G = \mathbb{F}_p.$$

The first equality shows that $L/\mathbb{F}_p$ is Galois, and the second shows that $\mathrm{Aut}(L/\mathbb{F}_p) = G$. Therefore $\mathrm{Gal}(L/\mathbb{F}_p) = G = \langle\phi\rangle$, and it has order $[L : \mathbb{F}_p] = n$.

Corollary 9.1. *Let L/K be any extension of finite fields with $|K| = q$. Then L/K is Galois with $\mathrm{Gal}(L/K)$ cyclic and generated by the q-power Frobenius map $x \mapsto x^q$.*

Proof: Let $L = \mathbb{F}_{p^n}$. We have $\mathbb{F}_p \subset K \subset L$. We have seen that $L/\mathbb{F}_p$ is Galois with

$$G = \mathrm{Gal}(L/\mathbb{F}_p) = \langle\phi\rangle \cong C_n.$$

Hence from the fundamental theorem of Galois theory, L/K is Galois and

$$H = \mathrm{Gal}(L/K) \leq G.$$

Since $G = \langle\phi\rangle \cong C_n$, we have $H = \langle\phi^m\rangle$ for some $m \mid n$. Then

$$[K : \mathbb{F}_p] = \frac{[L : \mathbb{F}_p]}{[L : K]} = \frac{|G|}{|H|} = (G : H) = m,$$

so $q = |K| = p^m$, and $\phi^m : x \mapsto x^q$.

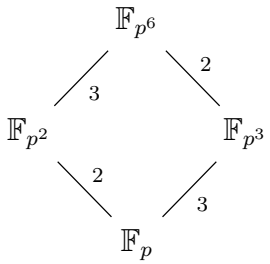
Corollary 9.2. *$\mathbb{F}_{p^n}$ has a unique subfield of order p^m for each $m \mid n$, and no others.*

Proof: Apply the fundamental theorem of Galois theory. The subgroups of $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\phi\rangle \cong C_n$ are the subgroup $H = \langle\phi^m\rangle$ for $m \mid n$.

If $K = (\mathbb{F}_{p^n})^H$, then $H = \mathrm{Gal}(\mathbb{F}_{p^n}/K)$, and $[K : \mathbb{F}_p] = (G : H) = m$, so $|K| = p^m$.

Example 9.1.

Let's look at $\mathbb{F}_{p^6}$. The lattice of subfields looks like this:



All extensions are Galois, with cyclic Galois group of order indicated.

10 Galois Group of a Polynomial

Let $f \in K[X]$ be a separable polynomial of degree n. Let L be a splitting field for f over K. Then action of $G = \mathrm{Gal}(L/K)$ on the roots $\alpha_1, \ldots, \alpha_n$ of f determines an injective group homomorphism $\iota : G \to S_n$.

Its image is the *Galois group* of f over K, written $\mathrm{Gal}(f)$ or $\mathrm{Gal}(f/K)$.

Lemma 10.1. *Let $f \in K[X]$ be a separable polynomial. Then*

$$f \text{ irreducible} \iff \mathrm{Gal}(f/K) \text{ transitive.}$$

Proof: $\Longleftarrow$ Assume $\mathrm{Gal}(f/K)$ transitive. If $f = gh$ for $g, h \in K[X]$, and $\deg g, \deg h > 0$, then $\mathrm{Gal}(f/K)$ sends roots of g to roots of g, and so cannot act transitively on the roots of f.

$\Longrightarrow$ Without loss of generality assume f is monic. Let $\alpha \in L$ be a root of f. Then f is the minimal polynomial of α over K. Then the roots of f are precisely $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L/K)\}$.

Hence $\mathrm{Gal}(L/K)$ acts transitively on $\alpha_1, \ldots, \alpha_n$, and so $\mathrm{Gal}(f/K) \leq S_n$ is a transitive subgroup.

Remark. Alternatively, by theorem 4.2, there exists a K-isomorphism $K(\alpha_i) \cong K(\alpha_j)$, by $\alpha_i \mapsto \alpha_j$.

This extends to an automorphism of L by uniqueness of splitting fields.

Let $f \in K[X]$ be monic and separable, with roots $\alpha_1, \ldots, \alpha_n$ in a splitting field L. Recall that

$$\mathrm{Disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Lemma 10.2. *Assume* $\mathrm{char}\, K \neq 2$. *Let* $\triangle = \mathrm{Disc}(f)$. *The fixed field of* $\mathrm{Gal}(f/K) \cap A_n$ *is* $K(\sqrt{\triangle})$

In particular, $\mathrm{Gal}(f/K) \leq A_n \iff \triangle$ *is a square in* K.

Proof: The sign of a permutation $\pi \in S_n$ is defined so that

$$\prod_{i<j} (X_{\pi(i)} - X_{\pi(j)}) = \mathrm{sgn}(\pi) \prod_{i<j} (X_i - X_j).$$

Define the quantity

$$\delta = \prod_{i<j}(\alpha_i - \alpha_j),$$

so $\delta^2 = \triangle$. Hence if $\sigma \in G = \mathrm{Gal}(f/K) = \mathrm{Gal}(L/K)$, then

$$\sigma(\delta) = \mathrm{sgn}(\sigma)\delta.$$

As f is separable and $\mathrm{char}\, K \neq 2$, $\delta = -\delta$. Hence

$$G \cap A_n = \{\sigma \in G \mid \mathrm{sgn}(\sigma) = 1\} = \{\sigma \in G \mid \sigma(\delta) = \delta\} = \mathrm{Gal}(L/K(\delta)).$$

So $L^{G\cap A_n} = K(\delta) = K(\sqrt{\triangle})$. In particular, $G \leq A_n \iff G \cap A_n = G \iff K(\sqrt{\triangle}) = K \iff \triangle$ is a square in K.

Remark. $G = \mathrm{Gal}(f/K) \leq S_n$ is really only defined up to conjugacy, since if we reorder $\alpha_1, \ldots, \alpha_n$ using $\sigma \in S_n$. Then G changes to $\sigma G \sigma^{-1}$.

However we can distinguish $\langle (1\,2), (3\,4)\rangle$ and $\langle (1\,2)(3\,4), (1\,3)(2\,4)\rangle$ even though they are both isomorphic to $C_2 \times C_2$.

Hence we want to look at $G \hookrightarrow S_n$ up to conjugacy.

- For $n = 2$, the only transitive subgroup of S_2 is itself.
- For $n = 3$, the transitive subgroups of S_3 are S_3 and $A_3 \cong C_3$.

So if $f \in K[X]$ is irreducible, then $\mathrm{Gal}(f/K) = A_3$ or S_3. Then $\mathrm{Gal}(f/K) = A_3 \iff \mathrm{Disc}(f)$ is a square in K.

Taking $n = 3$ in the discriminant formula proved in example sheet 2 gives

$$\mathrm{Disc}(X^3 + aX + b) = -4a^3 - 27b^2.$$

Example 10.1.

Let $f(X) = X^3 - 3X + 1$. Then $\mathrm{Disc}(f) = -4(-3)^3 - 27 = 81 = 9^2$, so $\mathrm{Gal}(f/\mathbb{Q}) = 1$ or A_3.

However f is irreducible, so $\mathrm{Gal}(f/\mathbb{Q}) = A_3$.

For $n = 4$, the transitive subgroups of S_4 are S_4, A_4, D_8, C_4 and $V \cong C_2 \times C_2$.

Of these S_4, A_4 and V are normal subgroups. There are 3 conjugate copies of each of C_4 and D_8.

Let S_4 act on $V \setminus \{\mathrm{id}\}$ by conjugation. As $g(1\,2)(3\,4)g^{-1} = (g(1)\,g(2))(g(3)\,g(4))$, it would be equivalent to let S_4 act on the set of ways of partitioning $\{1,2,3,4\}$ into two subsets of size 2.

The corresponding permutation representation is a group homomorphism $\pi : S_4 \to S_3$.

If $H = \{\sigma \in S_4 \mid \sigma(1) = 1\} = \langle (2\,3\,4), (2\,3)\rangle \leq S_4$, then $\pi|_H : H \to S_3$ is an isomorphism.

So π is surjective, and $|\ker \pi| = 4$. As V is abelian, $V \leq \ker \pi$, hence $V = \ker \pi$.

If $G \leq S_4$, then applying the isomorphism theorem to $\pi|_G$ gives

$$G/G \cap V \cong \pi(G) \leq S_3.$$

Here is the subgroup in S_3 associated to each transitive subgroup of S_4.

$G \leq S_4$	$\pi(G) \leq S_3$
S_4	S_3
A_4	A_3
C_4, D_8	C_2
V	1

Let

$$f(X) = \prod_{i=1}^{4}(X - \alpha_i)$$

be a monic quartic polynomial. Define

$$\begin{aligned}\beta_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4),\\ \beta_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),\\ \beta_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).\end{aligned}$$

Definition 10.1. The *resolvent cubic* is

$$g(X) = \prod_{i=1}^{3}(X - \beta_i).$$

Theorem 10.1. *Let f, g be as above.*

(i) *If $f \in K[X]$, then $g \in K[X]$.*

(ii) *If f is separable, then g is separable.*

(iii) *If both hold, then*

$$\pi(\mathrm{Gal}(f/K)) = \mathrm{Gal}(g/K).$$

In particular if $f \in K[X]$ is irreducible, then $\mathrm{Gal}(g/K)$ determines $\mathrm{Gal}(f/K)$ up to ambiguity between C_4 and D_8 when $|\mathrm{Gal}(g/K)| = 2$.

Proof:

(i) More generally, each coefficient of g is a symmetric polynomial in $\mathbb{Z}[\beta_1, \beta_2, \beta_3]$, hence a symmetric polynomial in $\mathbb{Z}[\alpha_1, \ldots, \alpha_4]$, and so by the symmetric function theorem is a $\mathbb{Z}$-coefficient polynomial in the coefficients of f.

(ii) Note that if we expand:

$$\begin{aligned}\beta_1 - \beta_2 &= \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 \\ &\quad - \alpha_1\alpha_2 - \alpha_1\alpha_4 - \alpha_2\alpha_3 - \alpha_3\alpha_4 \\ &= (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2).\end{aligned}$$

Hence if f is separable, then $\alpha_1, \ldots, \alpha_4$ are distinct, so $\beta_1 \neq \beta_2$. The same calculation show that $\beta_1, \beta_2, \beta_3$ are distinct. Thus g is separable.

(iii) Let M be a splitting field of f over K. Let $\alpha_1, \ldots, \alpha_4 \in M$ be the roots of f. Then

$$L = K(\beta_1, \beta_2, \beta_3) \subset M$$

is a splitting field for g over K.

If an element of $\mathrm{Gal}(M/K)$ permutes $\alpha_1, \ldots, \alpha_4$ according to $\sigma \in S_4$, then it restrict to an element of $\mathrm{Gal}(L/K)$ permuting $\beta_1, \beta_2, \beta_3$ according to $\pi(\sigma) \in S_3$.

In other words, there is a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(M/K) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(L/K) \\ \downarrow{\scriptstyle \iota_4} & & \downarrow{\scriptstyle \iota_3} \\ S_4 & \xrightarrow{\pi} & S_4 \end{array}$$

By theorem 6.4(c)? the map $\mathrm{res} : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ is surjective, hence

$$\pi(\mathrm{Im}\,\iota_4) = \mathrm{Im}(\iota_3) \implies \pi(\mathrm{Gal}(f/K)) = \mathrm{Gal}(g/K).$$

Proposition 10.1. *Let f be a monic quartic polynomial with resolvent cubic g. Then:*

(i) $\mathrm{Disc}(f) = \mathrm{Disc}(g)$.

(ii) *If $f(X) = X^4 + pX^2 + qX + r$, then $g(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2$.*

Proof:

(i) Exercise. Use the fact that $\beta_1 - \beta_2 = (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2)$.

(ii) We must show that:

$$\beta_1 + \beta_2 + \beta_3 = 2p, \tag{1}$$
$$\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1 = p^2 - 4r, \tag{2}$$
$$\beta_1\beta_2\beta_3 = -q^2. \tag{3}$$

For the proof of (1), note that

$$\beta_1 + \beta_2 + \beta_3 = 2\sum_{i<j} \alpha_i\alpha_j = 2p.$$

Now let's try doing (3). Since $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, we have

$$\begin{aligned}\beta_1 &= -(\alpha_1 + \alpha_2)^2,\\ \beta_2 &= -(\alpha_1 + \alpha_3)^2,\\ \beta_3 &= -(\alpha_1 + \alpha_4)^2.\end{aligned}$$

Now notice that

$$(\alpha_1 + \alpha_2 + \alpha_3) = \alpha_1^2(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) + \sum_{i<j<k} \alpha_i\alpha_j\alpha_k,$$
$$\implies \beta_1\beta_2\beta_3 = -q^2.$$

This proves (3). Now (2) is just a further calculation (omitted as it is kinda cringe).

Example 10.2.

Let $f(X) = X^4 - 4X^2 + 2$. Then $g(X) = X(X^2 + 8X + 8)$.

Now $\mathrm{Disc}(f) = \mathrm{Disc}(g) = 8^2\,\mathrm{Disc}(X^2 + 8X + 8) = 2^1 1$. Now as $\mathrm{Gal}(g/\mathbb{Q}) =$

C_2, we have $\mathrm{Gal}(f/\mathbb{Q}) = C_4$ or D_8.

But note that $f(X) = (X^2 - 2 + \sqrt{2})(X^2 - 2 - \sqrt{2})$, $\mathrm{Gal}(f/\mathbb{Q}(\sqrt{2})) = \mathrm{Gal}(f/\mathbb{Q}) \cap A_4$ is not a transitive subgroup of S_4.

This implies $\mathrm{Gal}(f/\mathbb{Q}) \cong C_4$.

Let's see how we can use this to determine the roots of a quartic polynomial. We do it step-by-step.

(i) Replace $f(X)$ by $f(X + c)$ such that f has no X^3 term.

(ii) Find the roots $\beta_1, \beta_2, \beta_3$ of the resolvent cubic using the method of symmetric polynomials.

(iii) Then as $\beta_i = -(\alpha_1 + \beta_{i+1})^2$, we have $\frac{1}{2}(\sqrt{-\beta_1} + \sqrt{-\beta_2} + \sqrt{-\beta_3}) = \alpha_1$, where we choose square roots such that

$$\sqrt{-\beta_1}\sqrt{-\beta_2}\sqrt{-\beta_3} = -q.$$

Recall that $\sigma \in S_n$ has cycle type $(n_1, \ldots, n_r)$ if, when written as a product of disjoint cycles, these cycles have length $n_1, \ldots, n_r$.

Lemma 10.3. *Let $f \in \mathbb{F}_p[X]$ be a separable polynomial with irreducible factors of degrees $n_1, \ldots, n_r$. Then $\mathrm{Gal}(f/\mathbb{F}_p) \leq S_n$ is generated by a single element of cycle type $(n_1, \ldots, n_r)$.*

In particular, $\mathrm{Gal}(f/\mathbb{F}_p)$ is cyclic with order $\mathrm{lcm}(n_1, \ldots, n_r)$.

Proof: Let L be a splitting field of f over $\mathbb{F}_p$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in L. Then theorem 9.2 tells us that $G = \mathrm{Gal}(L/\mathbb{F}_p)$ is cyclic generated by the Frobenius map $\phi : x \mapsto x^p$.

Write $f = \prod f_i$, where $f_i \in \mathbb{F}_p[X]$ is irreducible of degree n. Since G permutes the roots of each f_i transitively, the action of ϕ on the roots of f_i is given by a single n_i cycle.

Theorem 10.2 (Reduction mod p)**.** *Let $f \in \mathbb{Z}[X]$ be a monic separable polynomial of degree n. Let p be a prime and suppose the reduction of f mod p, say $\bar{f} \in \mathbb{F}_p[X]$ is also separable.*

Then $\mathrm{Gal}(\bar{f}/\mathbb{F}_p) \leq \mathrm{Gal}(f/\mathbb{Q})$ as a subgroup of S_n, up to conjugacy.

Corollary 10.1. *With the same assumptions, suppose $\bar{f} = g_1 g_2 \cdots g_r$, where $g_i \in \mathbb{F}_p[X]$ is irreducible of degree n_i. Then $\mathrm{Gal}(f/\mathbb{Q}) \leq S_n$ contains an element with cycle type $(n_1, n_2, \ldots, n_r)$.*

Proof: Combine the above lemma and theorem.

Example 10.3.

Let $f(X) = X^4 - 3X + 1$. Then looking mod 2,

$$\bar{f} = X^4 + X + 1 \in \mathbb{F}_2[X]$$

is irreducible. Then looking mod 5,

$$\bar{f} = (X+1)(X^3 - X^2 + X + 1) \in \mathbb{F}_5[X],$$

where the latter polynomial is irreducible in $\mathbb{F}_5[X]$. Hence $\mathrm{Gal}(f/\mathbb{Q})$ contains a 3-cycle and a 4-cycle, hence must be S_4.

Now let's prove the above theorem.

Proof: Let $f \in K[X]$ be a monic separable polynomial of degree n with splitting field L and roots $\alpha_1, \ldots, \alpha_n \in L$. Let

$$F(T_1, \ldots, T_n, X) = \prod_{\sigma \in S_n} (X - (\alpha_1 T_{\sigma(1)} + \cdots + \alpha_n T_{\sigma(n)})) \in K[T_1, \ldots, T_n, X].$$

Indeed, the coefficients of this polynomial are in L, and are fixed by $\mathrm{Gal}(L/K)$, hence are in K.

We define an action σ of S_n on $K[T_1, \ldots, T_n, X]$ by permuting the T_i, i.e.

$$(\sigma * h)(T_1, \ldots, T_n, X) = h(T_{\sigma(1)}, \ldots, T_{\sigma(n)}, X).$$

We note that $\sigma * F = F$ for all $\sigma \in S_n$. Let's take a quick detour.

Lemma 10.4. *Let $F_1 \in K[T_1, \ldots, T_n, X]$ be an irreducible factor of F. Then* $\mathrm{Gal}(f/K) \leq S_n$ *is conjugate to* $\mathrm{Stab}(F_1) = \{\tau \in S_n \mid \tau * F_1 = F_1\}$.

Proof: Without loss of generality, assume F_1 is monic in X. Replacing F_1 by $\tau * F_1$ for suitable $\tau \in S_n$, we may suppose it has a factor

$$X - (\alpha_1 T_1 + \cdots + \alpha_n T_n).$$

Then for each $\sigma \in G = \mathrm{Gal}(f/K)$ it has a factor

$$X - (\alpha_{\sigma(1)}T_1 + \cdots + \alpha_{\sigma(n)}T_n).$$

Now notice that

$$\prod_{\sigma \in G}(X - (\alpha_{\sigma(1)}T_1 + \cdots + \alpha_{\sigma(n)}T_n))$$

has coefficients in K, and divides F_1, hence is equal to F_1.

For $\tau \in S_n$, we have

$$\begin{aligned}
\tau * F_1 &= \prod_{\sigma \in G}(X - (\alpha_{\sigma(1)}T_{\tau(1)} + \cdots + \alpha_{\sigma(n)}T_{\tau(n)})) \\
&= \prod_{\sigma \in G}(X - (\alpha_{\sigma\tau^{-1}(1)}T_1 + \cdots + \alpha_{\sigma\tau^{-1}(n)}T_n)) \\
&= \prod_{\sigma \in G\tau^{-1}}(X - (\alpha_{\sigma(1)}T_1 + \cdots + \alpha_{\sigma(n)}T_n)).
\end{aligned}$$

So $\tau * F_1 = F_1 \iff G = G\tau^{-1} \iff \tau \in G$.

Let's go back to the proof we just interjected.

Proof: By the symmetric function theorem, the coefficients of F are $\mathbb{Z}$-coefficient polynomials in the coefficients of f. So if $f \in \mathbb{Z}[X]$, then $F \in \mathbb{Z}[T_1, \ldots, T_n, X]$.

Let $\bar{f} \in \mathbb{F}_p[X]$ and $\bar{F} = \mathbb{F}_p[T_1, \ldots, T_n, X]$ be the polynomials obtained by reducing all the coefficients modulo p.

We may equally construct $\bar{F}$ from $\bar{f}$ in the same way we construct F from f.

Write $F = F_1F_2 \cdots F_s$ for $F_i \in \mathbb{Z}[T_1, \ldots, T_n, X]$ distinct irreducibles, and $\bar{F} = \Phi_1\Phi_2 \cdots \Phi_t$, for $\Phi_i \in \mathbb{F}_p[T_1, \ldots, T_n, X]$ distinct irreducibles.

Without loss of generality assume that $\Phi_1 \mid \bar{F}_1$. Then $\Phi_1 \nmid \bar{F}_j$ for all $j > 1$. Then

$$\{\tau \in S_n \mid \tau * \Phi_1 = \Phi_1\} \subseteq \{\tau \in S_n \mid \tau * F_1 = F_1\}.$$

Hence the previous lemma shows that, up to conjugacy,

$$\mathrm{Gal}(\bar{f}/\mathbb{F}_p) \leq \mathrm{Gal}(f/\mathbb{Q}).$$

11 Cyclotomic and Kummer Extensions

Let K be a field and $n \geq 1$ an integer. We suppose that $\operatorname{char} K \nmid n$.

Let L/K be a splitting field of $f(X) = X^n - 1$. Since $f'(X) = nX^{n-1}$ and $n \cdot 1_K \neq 0$, we have $\gcd(f, f') = 1$, and so f is separable.

Hence L/K is Galois. Let $\mu_n = \{x \in L \mid x^n = 1\}$ be the group of n'th roots of unity. This is a subgroup of L^* of order n.

Definition 11.1. $\zeta_n \in \mu_n$ is a *primitive n'th root of unity* if it has order exactly n in L^*. For example if $K \subset \mathbb{C}$, then we can take $\zeta_n = e^{2\pi i/n}$.

Then $\mu_n = \langle \zeta_n \rangle = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ and $L = K(1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}) = K(\zeta_n)$.

Definition 11.2. $K(\zeta_n)/K$ is called a *cyclotomic extension*.

Recall that $(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$ is a group under multiplication, and it has order $\phi(n)$.

Let K be a field with $\operatorname{char} K \nmid n$, and let ζ_n be a primitive n'th root of unity.

Theorem 11.1. *There is an injective group homomorphism*

$$\operatorname{Gal}(K(\zeta_n)/K) \overset{\chi}{\hookrightarrow} (\mathbb{Z}/n\mathbb{Z})^*.$$

In particular, $\operatorname{Gal}(K(\zeta_n)/K)$ *is abelian, and* $[K(\zeta_n) : K]$ *divides* $\phi(n)$.

Proof: Let $G = \operatorname{Gal}(K(\zeta_n)/K)$. If $\sigma \in G$, then ζ_n and hence also $\sigma(\zeta_n)$ are roots of $X^n - 1$, so $\sigma(\zeta_n) = \zeta_n^a$ for some $\alpha \in \mathbb{Z}$.

Moreover, since ζ_n is a primitive n'th root of unity, the value of a is unique mod n. We define $\chi : G \to \mathbb{Z}/n\mathbb{Z}$ by $\sigma \mapsto a$.

Now let $\sigma, \tau \in G$ with $\sigma(\zeta_n) = \zeta_n^a$ and $\tau(\zeta_n) = \zeta_n^b$. Then

$$\sigma\tau(\zeta_n) = \sigma(\zeta_n^b) = \zeta_n^{ab},$$

so $\chi(\sigma\tau) = ab = \chi(\sigma)\chi(t)$. In particular, $\chi(\sigma)\chi(\sigma^{-1}) = \chi(1) = 1$, so $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$.

Moreover, χ is a group homomorphism. Since any $\sigma \in G$ is uniquely determined by $\sigma(\zeta_n)$, it is clear that χ is injective.

Remark. If $\chi(\sigma) = a$, then $\sigma(\zeta) = \zeta^a$ for all $\zeta \in \mu_n$. So the definition of χ does not depend on the choice of ζ_n.

Example 11.1.

Let p be a prime with $p \equiv 4 \pmod 5$. Let $K = \mathbb{F}_p$, $L = \mathbb{F}_{p^2}$ and $n = 5$. Since $5 \mid (p^2 - 1)$, there is $\zeta_5 \in L$ a primitive 5'th root of unity, but as $5 \nmid p - 1$, $\zeta_5 \notin K$.

Hence we get $L = K(\zeta_5)$. Therefore,

$$C_2 \cong \mathrm{Gal}(L/K) \overset{\chi}{\hookrightarrow} (\mathbb{Z}/5\mathbb{Z})^*,$$

hence $\mathrm{Im}(\chi) = \{\pm 1\} \leq (\mathbb{Z}/5\mathbb{Z})^*$.

Corollary 11.1. *Let $K = \mathbb{F}_p$ and suppose $p \nmid n$. Then $[K(\zeta_n) : K]$ equals the order of p in $(\mathbb{Z}/n\mathbb{Z})^*$.*

Proof: $\mathrm{Gal}(K(\zeta_n)/K)$ is generated by the Frobenius ϕ which sends $\zeta_n \mapsto \zeta_n^p$, so

$$\begin{aligned}[K(\zeta_n) : K] &= \text{order of } \phi \text{ in } \mathrm{Gal}(K(\zeta_n)/K) \\ &= \text{order of } \chi(\phi) \text{ in } (\mathbb{Z}/n\mathbb{Z})^*.\end{aligned}$$

Definition 11.3. Let $\zeta_n = e^{2\pi i/n}$. The *n'th cyclotomic polynomial* is

$$\Phi_n(X) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \zeta_n^a).$$

Its roots are the primitive n'th roots of unity. As $\mathrm{Gal}(\mathbb{Q}/(\zeta_n)/\mathbb{Q})$ permutes these, we have $\Phi_n \in \mathbb{Q}[X]$, and clearly we have

$$\zeta^n = 1 \iff \zeta \text{ is a primitive } d\text{'th root of unity for some } d \mid n.$$

Hence we get

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

It follows by induction on n that $\Phi_n \in \mathbb{Z}[X]$.

Let's look at some small cases. We have

$$\begin{aligned}\Phi_1 &= X - 1, \\ \Phi_p &= \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-1} + \cdots + X^2 + X + 1, \\ \Phi_4 &= X^2 + 1.\end{aligned}$$

In general, $\deg \Phi_n = \phi(n)$.

Theorem 11.2. *If $K = \mathbb{Q}$, then the group homomorphism χ is an isomorphism. In particular, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, and $\Phi_n \in \mathbb{Q}[X]$ is irreducible.*

Proof: Let p be a prime with $p \nmid n$. We show that $\operatorname{Im}\chi$ contains p mod n. If this is true, then $\operatorname{Im}\chi$ contains a mod n for every a coprime to n, hence χ is surjective as required.

Let $f, g \in \mathbb{Q}[X]$ be the minimal polynomials of ζ_n and ζ_n^p over $\mathbb{Q}$. If $f = g$, then as $\operatorname{Gal}(f/\mathbb{Q})$ is transitive, there exists $\sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $\sigma(\zeta_n) = \zeta_n^p$.

If not, then f, g are distinct irreducibles dividing $X^n - 1$. So $f, g \in \mathbb{Z}[X]$ and $fg \mid (X^n - 1)$.

As ζ_n is a root of $g(X^p)$, we have $f(X) \mid g(X^p)$. Reducing mod p gives

$$\bar{f}(X) \mid \bar{g}(X^p) = \bar{g}(X)^p.$$

Both $\bar{f}$ and $\bar{g}$ divide the separable polynomial $X^n - 1 \in \mathbb{F}_p[X]$, so $\bar{f}(X) \mid \bar{g}(X)$. Hence

$$\bar{f}(X)^2 \mid \bar{f}(X)\bar{g}(X) \mid X^n - 1,$$

which is a contradiction to $X^n - 1$ separable.

Using this we can tie up a loose end from earlier.

Theorem 11.3. *Let $n \geq 3$. A regular n-gon is constructible by ruler and compass if and only if $\phi(n)$ is a power of 2.*

Proof: Let $\zeta_n = e^{2\pi i/n}$ and $\alpha = \zeta_n + \zeta_n^{-1} = 2\cos(\frac{2\pi}{n})$.

Since $\alpha \in \mathbb{R}$, $\zeta_n \notin \mathbb{R}$ and ζ_n is a root of $X^2 - \alpha X + 1 \in \mathbb{Q}(\alpha)[X]$, we have that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$.

If a regular n-gon can be constructed, then α can be constructible. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2. Therefore,

$$\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2[\mathbb{Q}(\alpha) : \mathbb{Q}]$$

is a power of 2.

For the converse, we can use the converse of the theorem in the relevant section. It remains to show that if $\phi(n)$ is a power of 2, then there exists a sequence of fields

$$\mathbb{Q} = K_m \subset K_{m-1} \subset \cdots \subset K_1 \subset K_0 = \mathbb{Q}(\zeta_n),$$

where $[K_i : K_{i+1}] = 2$ for all i, and $K_1 = \mathbb{Q}(\alpha)$. By the fundamental theorem of Galois theory, it suffices to construct subgroups

$$\{1\} = H_0 < H_1 < \cdots < H_{m-1} < H_m = (\mathbb{Z}/n\mathbb{Z})^*,$$

where $(H_i : H_{i-1}) = 2$ for all i, and $H_1 = \{\pm 1\}$.

Assuming $H_0, H_1, \ldots, H_j$ have been constructed, and $H_j \neq G$, we note that G/H_j has order a power of 2 and is non-trivial, so it contains an element gH_j of order 2. Then set $H_{j+1} = \langle H_j, g\rangle$ and repeat.

Corollary 11.2. *A regular n-gon is constructible by ruler and compass if and only if n is a power of 2 times a product of distinct primes of the form $F_k = 2^{2^k} + 1$.*

Proof: Note that:

$$n = \prod_i p_i^{\alpha_i} \implies \phi(n) = \prod_i p_i^{\alpha_i - 1}(p_i - 1).$$

If $\phi(n)$ is a power of 2 $\iff$ n is a product of a power of 2 and distinct odd primes of the form $2^m + 1$.

Now if $2^m + 1$ is a prime, then m must be a power of 2. Indeed, if $m = ab$ with $b > 1$ odd, then putting $x = 2^a$,

$$2^m + 1 = 2^{ab} + 1 = x^b + 1 = (x+1)(x^{b-1} - x^{b-2} + \cdots - x + 1).$$

The next question is for what k is F_k actually prime. Indeed, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ are all prime. However $F_5 = 641 \times 6700417$.

Many Fermat numbers have been proved composite and no more have been shown to be prime.

Theorem 11.4. *Let K, L be fields and $\sigma_1, \ldots, \sigma_n : K \hookrightarrow L$ be distinct field embeddings. If $\lambda_1, \ldots, \lambda_n \in L$ satisfy*

$$\lambda_1\sigma_1(x) + \lambda_2\sigma_2(x) + \cdots + \lambda_n\sigma_n(x) = 0$$

for all $x \in K$, then $\lambda_1 = \lambda_1 = \cdots = \lambda_n = 0$.

Proof: We induct on n. This is trivially true for $n = 1$, so assume $n \geq 2$ and

$$\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0 \tag{1}$$

for all $x \in K$. Pick $y \in K$ such that $\sigma_1(y) \neq \sigma_2(y)$. Replacing x by xy in (1) gives

$$\lambda_1\sigma_1(x)\sigma_1(y) + \cdots + \lambda_n\sigma_n(x)\sigma_n(y) = 0 \tag{2}$$

for all $x \in K$. Taking $\sigma_1(y) \times (1) - (2)$ gives a new relation with only $n-1$ terms, hence it must be a trivial relation. Thus by the induction hypothesis,

$$\sigma_1(y)\lambda_i = \sigma_i(y)\lambda_i$$

for $2 \leq i \leq n$. Since $\sigma_1(y) \neq \sigma_2(y)$, we have $\lambda_2 = 0$. Thus (1) has only $n-1$ terms, so by the induction hypothesis, all $\lambda_i = 0$.

11.1 Kummer Theory

We continue to assume $\operatorname{char} K \nmid n$, but now further assume that $\mu_n \subset K$, that is K contains a primitive n'th root of unity ζ_n.

Lat $a \in K^*$. Let L/K be a splitting field of $f(X) = X^n - a$. Since $f'(X) = nX^{n-1}$ and $n \neq 0$, f is separable. Hence L/K is Galois.

Let $\alpha \in L$ be a root of f in L. Then

$$f(X) = \prod_{j=0}^{n-1}(X - \zeta_n^j\alpha).$$

Hence we know

$$L = K(\alpha), \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha) = K(\alpha).$$

We sometimes write $\sqrt[n]{a}$ for this α.

Definition 11.4. $K(\sqrt[n]{a})/K$ is called a *Kummer extension*.

Theorem 11.5. *Assume $\mu_n \subset K$ and $a \in K^*$. There is an injective group homomorphism*

$$\operatorname{Gal}(K(\sqrt[n]{a})/K) \overset{\theta}{\hookrightarrow} \mu_n.$$

In particular $\operatorname{Gal}(K(\sqrt[n]{a})/K)$ *is a cyclic group and* $[K(\sqrt[n]{a}) : K]$ *divides* n.

Proof: Let $G = \operatorname{Gal}(K(\sqrt[n]{a})/K)$. If $\sigma \in G$, then $\sqrt[n]{(a)}$ and hence also $\sigma(\sqrt[n]{a})$ are roots of $X^n - a$, so $\sigma(\sqrt[n]{a}) = \zeta_n^r\sqrt[n]{a}$ for some $0 \leq r < n$. Now

define

$$\begin{aligned}\theta : G &\to \mu_n \\ \sigma &\mapsto \zeta_n^r.\end{aligned}$$

Let $\sigma, \tau \in G$ be such that $\sigma(\sqrt[n]{(a)} = \zeta_n^r \sqrt[n]{(a)}$, $\tau(\sqrt[n]{a}) = \zeta_n^s \sqrt[n]{(a)}$. Then

$$\sigma\tau(\sqrt[n]{a}) = \sigma(\zeta_n^s \sqrt[n]{a}) = \zeta_n^{r+s} \sqrt[n]{a}.$$

Hence

$$\theta(\sigma\tau) = \zeta_n^{r+s} = \theta(\sigma)\theta(\tau),$$

so θ is a group homomorphism.

Since any $\sigma \in G$ is uniquely determined by $\sigma(\sqrt[n]{(a)}$, it is clear that θ is injective.

Remark. The definition of θ does not depend on the choice of $\sqrt[n]{a}$. Indeed, if $\alpha^n = \beta^n = 1$, then $\frac{\alpha}{\beta} \in \mu_n \subset K$. Therefore

$$\sigma\left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta} \implies \frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(\beta)}{\beta}.$$

We denote

$$(K^*)^n = \{x^n \mid x \in K^*\} \subset K^*.$$

Corollary 11.3. *Assume $\mu_n \subset K$ and $a \in K^*$. Then,*

$$[K(\sqrt[n]{a}) : K] = \text{ order of } a \text{ in } K^*/(K^*)^n.$$

In particular, $X^n - a$ is irreducible in $K[X]$ if and only if a is not a d'th power in K for any $1 < d \mid n$.

Proof: Let $\alpha \in \sqrt[n]{a}$ and $G = \mathrm{Gal}(K(\alpha)/K)$. Then

$$\begin{aligned} a^m \in (K^*)^n &\iff \alpha^m \in K^* \text{ (where we use } \mu_n \subset K) \\ &\iff \sigma(\alpha^m) = \alpha^m \text{ for all } \sigma \in G \\ &\iff \theta(\sigma)^m = 1 \text{ for all } \sigma \in G \\ &\iff \mathrm{Im}\,\theta \subset \mu_m \\ &\iff [K(\alpha) : K] = |\mathrm{Im}(\theta)| \text{ divides } m. \end{aligned}$$

Hence $[K(\alpha) : K]$ is the least m such that $a^m \in (K^*)^n$. Now onto the second

part:

$$\begin{aligned} X^n - a \text{ irreducible in } K[X] &\iff [K(\alpha) : K] = n \\ &\iff a \text{ has order } n \text{ in } K^*/(K^*)^n \\ &\iff \nexists\, m \mid n, m < n \text{ such that } a^m \in (K^*)^n \\ &\iff \nexists\, 1 < d \mid n \text{ with } a \in (K^*)^d. \end{aligned}$$

For the last iff, we put $n = md$ and use the fact that $\mu_n \subset K$.

As a special case, let $n = 2$ and $\operatorname{char} K \neq 2$. Then $[K(\sqrt{a}) : K] = 2$ provided $a \notin (K^*)^2$.

Theorem 11.6 (Kummer's theorem)**.** *Assume* $\operatorname{char} K \nmid n$ *and* $\mu_n \subset K$*. Then every degree* n *Galois extension* L/K *with cyclic Galois group is of the form* $L = K(\sqrt[n]{a})$ *for some* $a \in K$*.*

Proof: Write $\operatorname{Gal}(L/K) = \{\sigma^i \mid 0 \leq i < n\}$. Then by the linera independence of field embeddings, there exists $x \in L$ such that

$$\sum_{j=0}^{n-1} \zeta_n^j \sigma^j(x) \neq 0.$$

This value α is known as the *Lagrange resolvent*. Then

$$\sigma(\alpha) = \sum_{j=0}^{n-1} \zeta_n^j \sigma^{j+1}(x) = \sum_{j=0}^{n-1} \zeta_n^{j-1} \sigma^j(x) = \zeta_n^{-1}\alpha.$$

The Galois conjugates $\sigma^j(\alpha) = \zeta_n^{-j}\alpha$ are distinct, so the minimal polynomial of α has degree at least n. But then as $[L : K] = n$, we get $[K(\alpha) : K] = n$, and $L = K(\alpha)$.

Finally $\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta_n^{-1}\alpha)^n = \alpha^n$, hence $\alpha^n \in K$.

Now let K be a field with $\operatorname{char} K = 0$. Let $f \in K[X]$ be a polynomial.

Definition 11.5. f is *soluble by radicals* over K if there exists fields

$$K = K_0 \subset K_1 \subset K_2 \cdots \subset K_m,$$

such that f has a root in K_m, and for each $1 \leq i \leq m$, $K_i = K_{i-1}(\alpha_i)$ with $\alpha_i^{d_i} \in K_{i-1}$ for some $d_i \geq 1$.

Definition 11.6. A finite group G is *soluble* if there exists subgroups

$$\{1\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_m = G,$$

such that for each $1 \leq i \leq m$, $H_{i-1} \lhd H_i$ and H_i/H_{i-1} is abelian.

Remark. The definition is unchanged if we replace "abelian" by "cyclic", or "cyclic with prime order".

Example 11.2.

S_4 is soluble as

$$\{1\} \leq C_2 \leq V \leq A_4 \leq S_4,$$

with $V \cong C_2 \times C_2$, $A_4/V \cong C_3$ and $S_4/A_4 \cong C_2$.

Lemma 11.1. *If G is soluble, then so is every subgroup and quotient of G.*

This is an exercise.

Theorem 11.7. *Let $f \in K[X]$ be irreducible. Then*

$$f \text{ is soluble by radicals} \iff \mathrm{Gal}(f/K) \text{ is soluble.}$$

To show this we prove another lemma.

Lemma 11.2. *Let L/K be a finite Galois extension, with $\mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_m\}$. Let $a \in L^*$ and $n \geq 1$. Then*

$$M = L(\mu_n, \sqrt[n]{\sigma_1(a)}, \ldots, \sqrt[n]{\sigma_m(a)})$$

is a Galois extension of K.

Proof: Let

$$f(X) = \prod_{i=1}^{m} (X^n - \sigma_i(a)) \in K[X].$$

Then M is the splitting field of f over L, and moreover M is the composite of L and the splitting field of f over K, hence M/K is Galois.

Let's get back to proving this theorem.

Proof: $i \implies$ By definition, there exists fields $K = K_0 \subset K_1 \subset \cdots \subset K_m$, such that f has a root in K_m and for each $1 \leq i \leq m$, $K_i = K_{i-1}(\alpha_i)$ with

$\alpha_i^{d_i} \in K_{i-1}$ for some $d_i \geq 1$.

By repeatedly applying the previous lemma, we may assume that K_m/K is Galois. By adjoining suitable roots of unity first, we may further assume that each extension $K_i/K_{i=1}$ is either cyclotomic or Kummer. Hence $\mathrm{Gal}(K_i/K_{i-1})$ is abelian, so by the fundamental theorem of Galois theory, $\mathrm{Gal}(K_m/K)$ is soluble.

Since f has a root in K_m, and K_m/K is normal, we know that f splits in K_m. Hence $\mathrm{Gal}(f/K)$ is a quotient of $\mathrm{Gal}(K_m/K)$, so is soluble.

$\Longleftarrow$ By the Galois correspondence, there eixsts fields

$$K = K_0 \subset K_1 \subset \cdots \subset K_m$$

such that f has a root in K_m, and each K_i/K_{i-1} is Galois with cyclic Galois group. Let $n = \mathrm{lcm}[K_i : K_{i-1}]$. Then

$$K = K_0 \subset K_0(\zeta_n) \subset K_1(\zeta_n) \subset \cdots \subset K_m(\zeta_n).$$

By theorem 7.3, $K_i(\zeta_n)/K_{i-1}(\zeta_n)$ is Galois, and

$$\mathrm{Gal}(K_i(\zeta_n)/K_{i-1}(\zeta_n)) \hookrightarrow \mathrm{Gal}(K_i/K_{i-1}),$$

hence $\mathrm{Gal}(K_i(\zeta_n)/K_{i-1}(\zeta_n))$ is cyclic of order dividing n. Hence by Kummer's theorem, f is soluble by radicals.

Corollary 11.4. *If $f \in K[X]$ is a polynomial of degree $n \geq 5$ with Galois group A_n or S_n, then f is not soluble by radicals over K.*

Proof: A_5 is non-abelian and simple, hence is not soluble.

Hence as A_n and S_n contain A_5 as a subgroup, they are not soluble for all $n \geq 5$.

Example 11.3.

Let $K = \mathbb{Q}$, and $f(X) = X^5 - X + a$, where $a \in \mathbb{Z}$ and $\gcd(a, 10) = 1$.

Then mod 2, $f = X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$, so $\mathrm{Gal}(f/\mathbb{Q})$ contains an element σ with cycle type $(2, 3)$. So σ^3 is a transposition.

From example sheet 4 question 5, we get that $\bar{f} \in \mathbb{F}_5[X]$ is irreducible.

Now we know from example sheet 3 that a subgroup of S_p containing both a p-cycle and a transposition is S_p itself, so $\mathrm{Gal}(f/\mathbb{Q}) = S_5$, and f is not soluble by radicals.

12 Algebraic Closure

In this section we go back and try to prove the existence of algebraic closures for general fields. To do this, we need the following machinery:

Theorem 12.1 (Zorn's Lemma)**.** *Let S be a non-empty partially ordered set. If every chain in S has an upper bound, then S has a maximal element.*

Definition 12.1. A relation $\leq$ on a set S is a partial order if for all $x, y, z \in S$:

(i) $x \leq x$.

(ii) If $x \leq y$ and $y \leq z$, then $x \leq z$.

(iii) If $x \leq y$ and $y \leq x$, then $x = y$.

$(S, \leq)$ is called a *partially ordered set* or a *poset*. It is totally ordered if, moreover, for each $x, y \in S$, either $x \leq y$ or $y \leq x$.

Let $T \subset S$ be a subset.

- T is a *chain* if it is totally ordered by $\leq$.
- $x \in S$ is an upper bound for T if $t \leq x$ for all $t \in T$.
- $x \in S$ is maximal if there is no $y \in S$ with $x \leq y$ and $x \neq y$.

Let's look at ways to use Zorn's lemma.

Example 12.1.

Let V be a vector space and $(S, \leq)$ the set of linearly independent subsets of V, ordered by inclusion.

If $T \subset S$ is a chain, then let

$$Y = \bigcup_{X \in T} X.$$

It may be checked that Y is linearly independence, as linear dependence is a finite property. Hence Y is an upper bound for T. Therefore Zorn's lemma applies, and tells us that we have a maximal element B. Then,

(i) B is linearly independent, and

(ii) $B \cup \{v\}$ is not linearly independent for any $v \in V \setminus B$.

Hence this shows that B spans V, i.e. B is a basis for V.

Example 12.2.

Let R be a non-zero ring. Let $(S, \leq)$ be the set of all proper ideals of R, ordered by inclusion.

Then R nonzero $\implies \{0\} \in S \implies S$ is non-empty.

Now if $T \subset S$ is a chain, then let

$$J = \bigcup_{I \in T} I.$$

If $x, y \in J$, then $x \in I_1$ and $y \in I_2$ for some $I_1, I_2 \in T$. Since T is totally ordered, we have either $I_1 \subset I_2$ or $I_2 \subset I_1$. Thus $x + y \in J$. Also for all $r \in R$, $x \in J$, $rx \in J$.

So J is an ideal in R. Moreover it is a proper ideal since $1 \notin J$. Therefore $J \in S$ is an upper bound for T. Zorn's lemma then shows that S has a maximal element, hence R has a maximal ideal.

Theorem 12.2. *Let K be a field.*

(i) *There is an algebraic extension L/K such that every non-constant polynomial $f \in K[X]$ has a root in L.*

(ii) *K has an algebraic closure $\bar{K}$.*

Proof:

(i) Let S be the set of monic non-constant polynomials in $K[X]$. Ideally, we would like L to look like $K(\alpha_f \mid f \in S)$, where α_f is a root of f.

Let us expand this idea. Let $R = K[X_f \mid f \in S]$ be the polynomial ring in indeterminates $\{X_f \mid f \in S\}$. So the elements of R are finite K-linear combinations of monomials of the form

$$X_{f_1}^{d_1} X_{f_2}^{d_2} \cdots X_{f_r}^{d_r},$$

where $f_i \in S$ and $d_i \in \mathbb{N}$. Let $I \subset R$ be the ideal generated by $\{f(X_f) \mid f \in S\}$.

Now we need to show that $I \neq R$. If not, then $1 \in I$, i.e.

$$1 = \sum_{f \in T} g_f f(X_f), \qquad (*)$$

for some finite subset $T \subset S$ and polynomials $g_f \in R$.

Let L/K be a splitting field for $\prod_{f\in T} f$. Then for each $f \in T$, let $\alpha_f \in L$ be a root of f. We define a ring homomorphism

$$\phi : R \to L[X_f \mid f \in S \setminus T],$$
$$X_f \mapsto \begin{cases} \alpha_f & f \in T, \\ X_f & f \notin T, \end{cases}$$

and $\phi(c) = c$ for all $c \in K$. Applying ϕ to $(*)$ gives

$$1 = \sum_{f\in T} \phi(g_f) f(\alpha_f) = 0,$$

a contradiction. This proves the claim.

Since $I \neq R$, from the previous example R/I has a maximal ideal. Equivalently R has a maximal ideal J containing I.

Let $L = R/J$, and $\alpha_f = X_f + J \in L$. By construction, $f(\alpha_f) = 0$, since $f(X_j) \in I \subset J$. Since

$$L = \bigcup_{T\subset S \text{ finite}} K(\alpha_f \mid f \in T),$$

it follows that L/K is an algebraic extension.

(ii) Repeating the construction in (i) gives

$$K \subset K_1 \subset K_2 \subset \cdots$$

Each non-constant polynomial in $K_n[X]$ has a root in K_{n+1}. If $f \in K[X]$ has degree $n \geq 1$, then it has a root α_1 in K_1. Then $f(X)/(X-\alpha_1)$ has a root α_2 in K_2, and so on, so that f splits into linear factors in K_n. Then we can define

$$\bar{K} = \bigcup_{n\geq 1} K_n.$$

This is a field since it is a union of fields totally ordered by inclusion. Then every polynomial in $K[X]$ splits into linear factors over $\bar{K}$, and each element of $\bar{K}$ belongs to some K_n, so $\bar{K}$ is algebraic over K. Now we can apply lemma 4.2.

Now we try prove uniqueness of algebraic closure.

Proposition 12.1. *Let L/K be an algebraic extension and M/K a field extension with M algebraically closed. Then there exists a K-embedding $L \hookrightarrow M$.*

Proof: Let

$$S = \{(F, \sigma) \mid \sigma : F \hookrightarrow M \text{ a } K\text{-embedding}\},$$

with partial order $(F_1, \sigma_1) \leq (F_2, \sigma_2)$ if $F_1 \subset F_2$ and $\sigma_2|_{F_1} = \sigma_1$. Then $(S, \leq)$ is a poset, and it is non-empty as $(K, \mathrm{id}) \in S$.

Suppose $T = \{(F_i, \sigma_i) \mid i \in I\}$ be a chain, where I is some indexing set, and let

$$F = \bigcup_{i \in I} F_i,$$

be a field. Define

$$\begin{aligned} \sigma : F &\to M \\ x &\mapsto \sigma_i(x) \text{ if } x \in F_i. \end{aligned}$$

This is well-defined since σ_i and σ_j agree on $F_i \cap F_j$.

Then $(F, \sigma) \in S$ is an upper bound for T, hence by Zorn's lemma S has a maximal element (F, σ).

Let $\alpha \in L$. Then α is algebraic over K, hence algebraic over F. By theorem 4.2, we may extend $\sigma : F \hookrightarrow M$ to $\tau : F(\alpha) \hookrightarrow M$, using the fact that M is algebraically closed.

Then $(F, \sigma) \leq (F(\alpha), \tau)$. But (F, σ) maximal means $F(\alpha) \in F$, so $\alpha \in F$. Therefore $F = L$, and $\sigma : L \hookrightarrow M$ is a K-embedding as required.

Corollary 12.1. *Let K be a field, and L_1, L_2 be algebraic closures of K. Then there exists a K-isomorphism $\phi : L_1 \to L_2$.*

Note that in general, ϕ is not unique.

Proof: Since L_1/K is algebraic and L_2/K is a field extension with L_2 algebraically closed, using the previous proposition gives a K-embedding $\phi : L_1 \hookrightarrow L_2$.

Now any $\alpha \in L_2$ is algebraic over K, hence algebraic over $\phi(L_1)$. But

$\phi(L_1) \cong L_1$ is algebraically closed, hence $\alpha \in \phi(L_1)$.

This shows that ϕ is surjective.

13 Artin's Theorem and Invariant Theory

Theorem 13.1 (Artin's Theorem on Invariants)**.** *Let L be a field and $G \subset \mathrm{Aut}(L)$ be a finite subgroup. Then L/L^G is a finite Galois extension with Galois group G.*

In particular, $[L : L^G] = |G|$.

Remark. Let $K = L^G$. Then $G \leq \mathrm{Aut}(L/K)$, and

$$K \subset L^{\mathrm{Aut}(L/K)} \subset L^G = K,$$

so $K = L^{\mathrm{Aut}(L/K)}$. If we knew that L/K is algebraic, then it would follow that L/K is Galois.

Moreover if we knew that L/K is finite then

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

Proof: Let $K = L^G$. Pick any $\alpha \in L$, and let

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i),$$

where $\alpha_1, \ldots, \alpha_m$ are the distinct elements of $\mathrm{Orb}_G(\alpha) = \{\sigma(\alpha) \mid \sigma \in G\}$.

Then $\sigma f = f$ for all $\sigma \in G$, so $f \in K[X]$. Hence α is algebraic and separable over K, so L/K is algebraic and separable. We have also shown that $[K(\alpha) : K] \leq |G|$ for all $\alpha \in L$.

Now pick $\alpha \in L$ with $[K(\alpha) : K]$ maximal, and we will show that $L = K(\alpha)$.

Indeed, let $\beta \in L$, then $K(\alpha, \beta)/K$ is finite and separable. So by theorem 6.3, $K(\alpha, \beta) = K(\theta)$ for some $\theta \in L$.

By our choice of α, we have $[K(\theta) : K] \leq [K(\alpha) : K]$, but as $K(\alpha) \subset K(\theta)$ this gives $K(\alpha) = K(\theta)$.

Hence $\beta \in K(\alpha)$. This proves the claim.

Note $|\mathrm{Aut}(L/K)| \leq [L : K] = [K(\alpha) : K] \leq |G|$, but since $G \subset \mathrm{Aut}(L/K)$ it follows that these are all equalities, and hence $|\mathrm{Aut}(L/K)| = [L : K]$ so L/K is Galois, and $G = \mathrm{Gal}(L/K)$.

Example 13.1.

Let $L = \mathbb{C}(X_1, X_2)$ and define $\sigma, \tau \in \mathrm{Aut}(L)$ by

$$(\sigma f)(X_1, X_2) = f(iX_1, -iX_2),$$
$$(\tau f)(X_1, X_2) = f(X_2, X_1).$$

Let $G = \langle \sigma, \tau \rangle \cong D_8$. Our aim is then to compute L^G.

We spot that X_1X_2 and $X_1^4 + X_2^4 \in L^G$. We want to show that $L^G = \mathbb{C}(X_1X_2, X_1^4 + X_2^4)$.

To show this, note that $L = \mathbb{C}(X_1X_2, X_1^4 + X_2^4)(X_1)$. So it suffices to show that this has the appropriate degree. Let

$$f(T) = (T^4 - X_1^4)(T^4 - X_2^4) = T^8 - (X_1^4 + X_2^4)T^4 + (X_1X_2)^4 \in \mathbb{C}(X_1X_2, X_1^4 + X_2^4)[T].$$

Hence $[L : \mathbb{C}(X_1X_2, X_1^4 + X_2^4)] \leq 8$. But by Artin's theorem, $[L : L^G] = |G| = 8$, so by the tower law $L^G = \mathbb{C}(X_1X_2, X_1^4 + X_2^4)$.

Let R be a ring and $G \subset \mathrm{Aut}(R)$ a subgroup. *Invariant theory* seeks to describe the rings

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

This topic was studied extensively in the 19th century, and was the motivation for Hilbert's basis theorem.

It is also important in modern algebraic geometry for describing the quotient of an algebraic variety by a group action.

Example 13.2.

Let K be a field, and $L = K(X_1, \ldots, X_n)$ be the field of rational functions in n variables, i.e. the field of fractions of $R = K[X_1, \ldots, X_n]$.

Let $G = S_n$ act on L by permuting the X_i's. Our aim is to compute L^G.

Note that L^G contains the elementary symmetric polynomials s_i. Moreover, by the symmetric function theorem,

$$R^G = K[s_1, \ldots, s_n],$$

and there are no polynomial relations satisfied by the s_i.

Now we claim that $L^G = K(s_1, \dots, S_n)$. Indeed, suppose that $\frac{f}{g} \in L^G$, where $f, g \in R$ are coprime.

Then $\frac{\sigma(f)}{\sigma(g)} = \frac{f}{g}$ for all $\sigma \in G$. Since R is a UFD and the units of R are just $K^\times$, we have $\sigma(f) = c_0 f$, and $\sigma(g) = c_0 g$ for some $c_0 \in K^\times$.

But G has finite order, so say $|G| = N$. Then $f = \sigma^N(f) = c_0^N f$, so $c_0^N = 1$. Hence fg^{N-1} and $g^N \in R^G = K(s_1, \dots, s_n)$, so

$$\frac{f}{g} = \frac{fg^{N-1}}{g^N} \in K(s_1, \dots, s_n).$$

For another proof, let

$$f(T) = \prod_{i=1}^{n} (T - X_i) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n.$$

Then $f \in K(s_1, \dots, s_n)[T]$ is a polynomial of degree n, and L is a splitting field for f over $K(s_1, \dots, s_n)$.

From example sheet 1, $[L : K(s_1, \dots, s_n)] \leq n!$. But also $[L : L^G] = n!$ by Artin's theorem, so $L^G = K(s_1, \dots, s_n)$.

Remark. We have shown that the Galois group of a generic monic polynomial of degree n is S_n.

It can be shown that for any finite group G, there exists a finite Galois extension L/K with Galois group G. This may not be possible if we specify K, for example if $K = \mathbb{C}$ or $K = \mathbb{F}_p$.

When $K = \mathbb{Q}$, this is an open problem (the inverse Galois problem).

Corollary 13.1. *Let S_n act on $L = K(X_1, \dots, X_n)$ by permuting the X_i. If $\operatorname{char} K \neq 2$, then $L^{A_n} = K(s_1, \dots, s_n, \delta)$ where*

$$\delta = \prod_{i<j} (X_i - X_j).$$

Proof: As $(S_n : A_n) = 2$, we have $[L^{A_n} : K(s_1, \dots, s_n)] = 2$. We have $\sigma(\delta) = \operatorname{sgn}(\sigma)\delta$ for $\sigma \in S_n$. In particular, $\delta \in L^{A_n}$ and $\delta \notin L^{S_n}$, so $L^{A_n} = K(s_1, \dots, s_n, \delta)$.

Remark. It can be shown that if $R = K[X_1, \dots, X_n]$, then $R^{A_n} = K[s_1, \dots, s_n, \delta]$.

The idea of the proof is as follows: let $f \in R^{A_n}$. Pick $\sigma \in S_n \setminus A_n$, and write

$$f = \frac{1}{2}((f + \sigma f) + (f - \sigma f)).$$

Then $f + \sigma f$ is fixed by any permutation in S_n, and $f - \sigma f$ is divisible by δ.

14 Fundamental Theorem of Algebra

In this section we will prove the fundamental theorem of algebra, that is:

Theorem 14.1 (Fundamental Theorem of Algebra)**.** $\mathbb{C}$ *is algebraically closed.*

Proof: We will use the following facts:

(i) Every polynomial over $\mathbb{R}$ of odd degree has a root in $\mathbb{R}$.

(ii) Every quadratic over $\mathbb{C}$ has a root in $\mathbb{C}$ (using the quadratic formula).

(iii) Every group of order 2^n (with $n \geq 1$) has an index 2 subgroup.

Suppose $L/\mathbb{C}$ is a finite extension with $L \neq \mathbb{C}$. Replacing L by its Galois closure over $\mathbb{R}$, we may assume that $L/\mathbb{R}$ is Galois. Let $G = \mathrm{Gal}(L/\mathbb{R})$.

Let $H \leq G$ by a Sylow 2-subgroup. Then $[L^H : \mathbb{R}] = (G : H)$ is odd. So if $\alpha \in L^H$, then $[\mathbb{R}(\alpha) : \mathbb{R}]$ is odd, hence $\alpha \in \mathbb{R}$ by (i).

Thus we get $L^H = \mathbb{R}$ and $G = H$ is a 2-group.

Let $G_1 = \mathrm{Gal}(L/\mathbb{C}) \leq \mathrm{Gal}(L/\mathbb{R}) = G$. Since $L \neq \mathbb{C}$, we have G_1 non-trivial, so by (iii) it has an index 2 subgroup, say G_2. Then $[L^{G_2} : \mathbb{C}] = (G_1 : G_2) = 2$, which is impossible by (ii).

Index