Polynomial Rings and Galois Theory

Giacomo Micheli Balázs Szendrői[1]

Introduction

Galois theory studies the symmetries of the roots of a polynomial equation. The existence of the two solutions

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2} \tag{1}$$

of the polynomial equation

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

can be thought of a symmetry of the situation. Assuming that the roots $x_{1,2}$ are (real or complex but) irrational, we have the following.

- Solutions generate a field extension $K = \mathbb{Q}(x_1, x_2)$ of degree two of the rational field $\mathbb{Q}$.
- K has a field automorphism (symmetry) defined by $\phi(x_1) = x_2$, giving rise to a group $G = \{\mathrm{Id}_K, \phi\}$ acting on K.
- $\phi \circ \phi = \mathrm{Id}_K$, so as an abstract group, $\{e, \phi\}$ is of order two, isomorphic to C_2.
- The rational subfield $\mathbb{Q}$ is precisely the subfield of K fixed by both Id_K and ϕ.

The main aim of this course is to study groups of automorphisms of field extensions, their fixed subfields, and the relationship between the structure of field extensions and the structure of the associated groups. We will pay special attention to the question whether a general polynomial has roots expressible by a *formula* consisting of field operations and taking n-th roots, as in formula (1) for the quadratic polynomial. It was known by the 16th century that such a formula exists if $\deg f \leq 4$ (Tartaglia, Cardano, Ferrari). In contrast, it was discovered in the 19th century that there is usually no such formula for $\deg f \geq 5$ (Ruffini, Abel, Galois). We will prove these results as an application of our structure theory of field extensions.

1. Rings, Fields and Polynomial Rings

1.1. **Rings and domains.** Recall that R is a ring if it has addition, additive inverses, an additive identity $0 \in R$, and it also has multiplication that is distributive over addition. All our rings will also have a multiplicative identity $1 \in R$, and will have both operations commutative and associative.

Ring homomorphisms $f : R \to S$ between rings are required to map the multiplicative identity of R to that of S. For example, $\mathbb{Z}$ is a ring while $\mathbb{N}$ is not a ring; the map $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 0$ is not a ring homomorphism.

A ring R is an *integral domain*, if there are no zero-divisors, i.e. $ab = 0$ implies that $a = 0$ or $b = 0$.

A subset I of a ring R is said to be an ideal, denoted $I \trianglelefteq R$, if

(1) for $a \in R, x \in I$, we have $xa \in I$;
(2) $0 \in I$ and for $a, b \in I$, we have $a + b, -a \in I$.

[1]with some small changes by Damian Rössler

Given a ring R and an ideal I, there is a quotient ring R/I consisting of residue classes of elements of R modulo I.

Example. Any ideal in the ring of integers is of the form

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, ...\} \trianglelefteq \mathbb{Z}.$$

The corresponding quotient ring is $\mathbb{Z}/n\mathbb{Z}$, which is a domain if and only if it is a field if and only if n is prime.

Given any ring R we can define a ring homomorphism $\phi : \mathbb{Z} \to R$ such that

$$\phi(n) = \begin{cases} \underbrace{1+1+...+1}_{n \text{ times}} (n \geq 0) \\ \underbrace{-(1+1+...+1)}_{|n| \text{ times}} (n < 0) \end{cases}$$

Its kernel $\ker \phi = \{n \in \mathbb{Z} : \phi(n) = 0\}$ is an ideal in $\mathbb{Z}$. So

$$\ker \phi = \begin{cases} 0 \\ n\mathbb{Z} \end{cases}.$$

In the first case, $\mathbb{Z}$ is a subring of R, and we say R has *characteristic* 0. In the latter case, $\mathbb{Z}/n\mathbb{Z}$ becomes a subring of R, and we say that R has *characteristic* n. In both cases, we call this the *prime subring* of R. The characteristic of a domain is 0 or a prime number.

1.2. **Fields.** A ring K is a field if non-zero elements have multiplicative inverses and $1_K \neq 0_K$. A field is automatically an integral domain, and therefore has characteristic 0 or prime p. In the first case, we have $\mathbb{Q} \subset K$, in the latter case, $\mathbb{F}_p \subset K$, the *prime subfield* of K.

Proposition. *Given an integral domain R, there is a field K, the* field of fractions *of R, with the following properties: there is a homomorphism $\phi : R \to K$ which is injective and for every $x \in K$, there are $a, b \in R$ such that $x = \frac{\phi(a)}{\phi(b)}$.*

Proof. Construct K as the set of pairs (a, b), $a \in R$, $b \in R\backslash\{0\}$ under the equivalence relation $(a, b) \sim (a', b') \iff ab' = ba'$. Then K has addition $(a, b) + (c, d) = (ad + bc, bd)$ and multiplication $(a, b)(c, d) = (ac, bd)$. This has all the required structure including multiplicative inverses: $(a, b)(b, a) = 1$ for $a, b \neq 0$. Hence K is a field. The homomorphism $\phi : R \to K$ is given by $\phi(a) = (a, 1)$ and $(a, b) = \frac{\phi(a)}{\phi(b)}$ if $b \neq 0$. □

Lemma. *(i) Let K be a field, $I \trianglelefteq K$. Then either $I = \{0\}$ or $I = K$.*

(ii) Let K, L be fields. Then if $f : K \to L$ is a ring homomorphism, then f is injective.

Proof. (i) For $a \neq 0 \in I$, $a^{-1} \in K$ and so $1 \in I$. Then for $b \in K$, $1b \in I$ and thus $K \subseteq I$. So $I = K$.

Part (ii) follows from (i). $\ker f = \{a \in K : f(a) = 0\} \trianglelefteq K$. So either $\ker f = K$, and so $f(1) = 0$ which cannot happen as $f(1) = 1$, or $\ker f = \{0\}$ and thus f is injective. □

1.3. **Polynomial Rings.** Given a ring R, we can form another ring by considering

$$R[x] = \left\{ \sum_{i=0}^{d} a_i x^i : a_i \in R \right\},$$

the set of all polynomials with coefficients in R. This becomes a ring by extending the addition and multiplication in the usual way ("opening the bracket"). For a nonzero polynomial $f \in R[x]$, its degree $\deg f$ is the largest n for which $a_n \neq 0$. A polynomial $f \in R[x]$ is said to be monic if its leading coefficient is 1. Given a polynomial $f \in K[x]$, $\alpha \in K$ is a root of f if $f(\alpha) = 0$.

Lemma. *If R is a domain, then $R[x]$ is a domain.*

Proof. Suppose $f, g \neq 0 \in R[x]$ with leading coefficients $a_N x^N$ and $b_M x^M$. Then since these are leading coefficients, they are non-zero. But since R is a domain, $a_N b_M \neq 0$ and so $fg \neq 0$. So $R[x]$ is a domain. □

Now let K be a field. We get a ring $K[x]$, the polynomial ring over K, and its field of fractions

$$K(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in K[x], g \neq 0 \right\}.$$

Definition.
(1) A polynomial $f \in K[x]$ is said to be *irreducible* if $f = gh$ only if $\deg g = 0$ or $\deg h = 0$.
(2) A polynomial $f \in K[x]$ *divides* a polynomial g, written $f \mid g$, if there exists $h \in K[x]$ such that $g = fh$.
(3) A polynomial $f \in K[x]$ is *prime*, if whenever $f \mid gh$, $(f \mid g)$ or $(f \mid h)$.

An ideal I is said to be prime if $ab \in I$ implies $a \in I$ or $b \in I$. Hence f is prime in $K[x]$ if and only if (f) is a prime ideal.

Recall

Proposition. *$K[x]$ is a Euclidean ring; that is, given two monic polynomials f, g with $\deg g \geq 1$ then there exist $q, r \in K[x]$ wth $\deg r < \deg g$, satisfying $f = gq + r$.*

This implies that $K[x]$ is a principal ideal domain (PID). Recall that this means that every ideal in $K[x]$ is generated by a single element. It also implies the following result.

Theorem. *If K is a field, then $K[x]$ is a unique factorization domain. That is,*
(1) *The irreducible polynomials are precisely the prime polynomials.*
(2) *Given $f \neq 0 \in K[x]$, it can be expressed as a product*

$$f = f_1 f_2 f_3 \cdots f_n$$

of irreducible in an essentially unique way (up to rearrangement and multiplication by scalars).

Corollary. *Let K be a field.*
(1) *Given a polynomial $f \in K[x]$, $a \in K$ is a root if $f(a) = 0 \iff f(x) = (x - a)g(x)$.*
(2) *Given $f \in K[x]$, there exists distinct roots $a_i \in K$, multiplicities $m_i \in \mathbb{N}$, and $g \in K[x]$ without roots, such that*

$$f = g(x) \prod_i (x - a_i)^{m_i}.$$

Concerning irreducibility, we have the important and useful

Lemma. (Gauss' Lemma) *Let $f \in \mathbb{Z}[x]$ be monic. Then f is irreducible in $\mathbb{Z}[x]$, if and only if f is irreducible in $\mathbb{Q}[x]$.*

Corollary. *Let f be a monic polynomial with integer coefficients and* $\deg f \leq 3$. *Then if f has no integral root, then f is irreducible in $\mathbb{Q}[x]$.*

Proof. By Gauss' Lemma, $f(x)$ is reducible in $\mathbb{Q}[x]$ if and only if $f(x)$ is reducible in $\mathbb{Z}[x]$ if and only if $f = f_1 f_2$ with $1 \leq \deg f_1,\ 1 \leq \deg f_2$. Since we have made the assumption that $\deg f = 3$, it must be that $\deg f_1 = 1$ (wlog) and so $f = (x - \alpha) f_2(x)$. Then $\alpha \in \mathbb{Z}$ is a root. □

Proposition. (Eisenstein's Criterion) *Let*

$$f(x) = x^d + \sum_{i=0}^{d-1} a_i x^i$$

be a monic polynomial over $\mathbb{Z}$. Suppose that for some prime p, we have that $p | a_i$ for $0 \leq i < d$, but $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Z}$.

We are interested in methods of determining whether monic polynomials are irreducible in $\mathbb{Z}[x]$ (and hence in $\mathbb{Q}[x]$). There are various tools that can be used to do this:

(1) Eisenstein's criterion.
(2) More generally, reduction modulo p, for p a prime. Given a polynomial $f \in \mathbb{Z}[x]$, we have $(f \bmod p) \in \mathbb{F}_p[x] = \sum (a_i \bmod p) x^i$. Clearly, if $f = gh$ then $f \equiv_p gh$. Conversely, if f is monic and if for some p, $(f \bmod p)$ is irreducible, so if f. Checking irreducibility in $\mathbb{F}_p[x]$ is a finite (though perhaps cumbersome) task, since we have only finitely many choices for each coefficient in a splitting.
(3) Substitution: if $f(x) = g(x)h(x)$ then $f(x - a) = g(x - a)h(x - a)$. So $f(x - a)$ irreducible implies $f(x)$ is irreducible. There is an example of this on a problem sheet. This might help (say by the fact that $f(x - a)$ may be an Eisenstein polynomial).
(4) Tricks and ingenuity.

2. Group Actions on Rings and Fields

2.1. **Basic notions.**

Definition. A group G acts on a ring R (on the left) if for every $g \in G$, we are given a ring automorphism (bijective ring homomorphism) $g : R \to R$ mapping $a \mapsto g(a)$, such that for $a \in R$ and $g, h \in G$, we have $h(g(a)) = (hg)(a)$. (For G to act on R on the right, often written $a \mapsto ag$ or $a \mapsto a^g$, we require $(ag)h = a(gh)$).

Lemma. *Let the group G act on the ring R.*

(1) *Consider*
$$R^G = \{a \in R : g(a) = a \text{ for all } g \in G\}.$$
Then R^G is a subring of R.
(2) *If $R = K$ is a field, then for $g \in G$ and $a \in K \setminus \{0\}$ we have $g(a^{-1}) = (g(a))^{-1}$.*

(3) *If $R = K$ is a field, then K^G is a subfield, containing the prime subfield of K.*

Proof. For (1), just use the subring test. For (2), $1 = g(1) = g(aa^{-1}) = g(a)g(a^{-1})$. For (3), taking an element $a \in K^G$ we have that $g(a^{-1}) = g(a)^{-1} = a^{-1}$ and so $a^{-1} \in K^G$. Moreover, 1 is fixed, and the prime subfield consists of elements which are ratios of sums of 1, so the prime subfield must always be fixed. □

For K a field, denote by $\mathrm{Aut}(K)$ the group of all field automorphisms (bijective field homomorphisms) $g\colon K \to K$, with the group operation being composition. More generally, for a field extension L/K, let

$$\mathrm{Aut}_K(L) = \{g \in \mathrm{Aut}(L) \mid \text{ for all } a \in K, g(a) = a\}$$

denote the group of all field automorphisms of L over K. Using this notation, an action of a group G on a field K is a group homomorphism $G \to \mathrm{Aut}(K)$. In most of our examples, this homomophism will be injective (different elements of G give different automorphisms of K) in which case we will call the action *faithful*.

2.2. **Symmetric Polynomials.** Take K a field and let

$$R = K[x_1, x_2, \ldots, x_n]$$

be the polynomial ring in n variables. This is a domain, since we can define this iteratively adding one variable at a time. The ring R has an action by the symmetric group S_n by permuting variables: if $f(x_1, ..., x_n)$ is a polynomial and $\sigma \in S_n$ then $f^\sigma(x_1, ..., x_n) = f(x_{\sigma 1}, ..., x_{\sigma n})$.

Definition. The *ring of symmetric polynomials* is the fixed ring $K[x_1, ..., x_n]^{S_n}$.

The following *elementary symmetric polynomials* are clearly elements of the ring $K[x_1, ..., x_n]^{S_n}$:

$$s_k = \sum_{i_1 < i_2 < \ldots < i_k} \prod_{j=1}^{k} x_{i_j}.$$

For example.

$$\begin{aligned} s_1 &= \sum_i x_i, \\ s_2 &= \sum_{i<j} x_i x_j, \\ s_3 &= \sum_{i<j<k} x_i x_j x_k, \end{aligned}$$

and so on.

Theorem. (Theorem on Symmetric Functions) *$K[x_1, ..., x_n]^{S_n}$ has the following structure.*

$$K[x_1, ..., x_n]^{S_n} = K[s_1, ..., s_n].$$

In other words, every symmetric polynomial $f \in K[x_1, ..., x_n]^{S_n}$ is uniquely expressible as a polynomial of the elementary symmetric polynomials s_i.

Proof. (sketch) We use a trick. Introduce *lexicographic ordering* on monomials: call the monomial $x_1^{a_1} \dots x_n^{a_n}$ *larger than* the monomial $x_1^{b_1} \dots x_n^{b_n}$, if $a_1 > b_1$, or $a_1 = b_1$ and $a_2 > b_2$ or...

Suppose that $f \in K[x_1, ..., x_n]^{S_n}$. We find the largest monomial term in f in the lexicographic ordering. Let this be $\prod_i x_i^{a_i}$. Since f is symmetric, and $\prod_i x_i^{a_i}$ is the largest, we must have $a_1 \geq a_2 \geq ... \geq a_n$. One can show that $\prod x_i^{a_i}$ is also the largest term in the monomial $\prod s_i^{a_i - a_{i+1}}$ in the elementary symmetric functions. Now for some $c \in K$,

$$g = f - c \prod s_i^{a_i - a_{i+1}} \in K[x_1, ..., x_n]^{S_n}$$

and the largest term in g is smaller than that of f. So we may repeat for g. This shows that f can be written as a polynomial in the s_i. Unicity can be proven in a similar way. □

Remark. The proof is actually constructive: it gives us an algorithm to write a symmetric polynomial as a polynomial in the elementary symmetric polynomials. In practice, we often use this algorithm for the first few steps and then resort to guesswork and substitutions.

Example. The sum of squares $\sum_i x_i^2$ is not an elementary symmetric polynomial, but it is clearly symmetric. We have

$$\sum_i x_i^2 = s_1^2 - 2s_2.$$

Proposition. (1) *The* discriminant *of* $x_1, \dots, x_n$, *defined by*

$$\Delta = \prod_{i<j} (x_i - x_j)^2,$$

is a symmetric polynomial, an element of $K[x_1, ..., x_n]^{S_n}$.

(2) *The expression*

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

is not symmetric, but it is invariant under the alternating group $A_n < S_n$.

Proof. (1) is clear. For (2), note that a transposition $(i\, i+1) \in S_n$ multiplies δ by (-1). So δ is certainly not invariant, but it is invariant for an even product of such transpositions. Such even products generate the alternating group A_n. □

Example. For two variables, we have the well-known expression

$$\Delta = (x_1 - x_2)^2 = s_1^2 - 4s_2,$$

which is just the "$b^2 - 4c$" in the solution formula of the quadratic polynomial.

3. Field Extensions

3.1. **Basic notions.** A field extension M/K (or $M : K$)is just an injection of fields

$$f : K \to M,$$

equivalently a field inclusion

$$K \subseteq M$$

which we will often write in diagram form as

$$\begin{array}{c} M \\ | \\ K. \end{array}$$

In particular, if a group G acts on M, then $M^G \subseteq M$ is a subfield or M/M^G is a field extension. The *degree* of a field extension M/K, denoted $[M : K]$, is the vector space dimension $\dim_K M$, which may be infinite. M/K is called a *finite extension* if $[M : K]$ is finite. Recall

Proposition. (The Tower Law) *If $L/M/K$ are field extensions (finite or infinite) then*

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

Definition/Proposition. *We say that $a \in M$ is algebraic over K, if $f(a) = 0$ for some non-zero polynomial $f \in K[x]$. If a is algebraic over K, its* minimal polynomial *$m_a \in K[x]$ over K is the unique monic polynomial of least degree satisfying $m_a(a) = 0$. This polynomial has the following properties.*

(1) *m_a is irreducible.*
(2) *If $f(a) = 0$ for $f \in K[x]$, then m_a divides f in $K[x]$.*

Definition. A field extension M/K is *algebraic*, if every element $a \in M$ is algebraic over K. Otherwise, M/K is *transcendental*.

Note that every finite extension is algebraic, but not every algebraic extension is finite.

3.2. **Simple Extensions.** Let M/K be a field extension and let $a \in M$. The *simple extension* of K generated by a in M, denoted $K(a)$, is the smallest subfield of M containing K and a. More generally, for a subset S of M, the field $K(S)$ is the smallest subfield of M containing K and S.

Example. (1) Let K be a field and $K(t)$ the field of fractions of the polynomial ring $K[t]$. Then $K(t)$ is a simple transcendental extension of K.
(2) $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ is a simple algebraic extension of $\mathbb{Q}$, generated by $\sqrt{2} + i$.

Theorem. (Existence of simple extensions)

(1) *Given a field K and a monic irreducible polynomial $m \in K[x]$, there exists a field extension M/K with the following properties:*
   (a) *$M = K(\alpha)$ for some element $\alpha \in M$.*
   (b) *The minimum polynomial of $\alpha \in M$ is exactly m.*
   (c) *$[M : K] = \deg m$.*
(2) *Given L/K and $\alpha \in L$ algebraic over K, the simple extension $K(\alpha)$ of K in L is isomorphic to the extension constructed in (1) using the minimal polynomial m_α of α over K.*

Proof. (i) m is monic and irreducible, so (m) is a prime ideal in $K[x]$. So the quotient ring

$$M = K[x]/(m)$$

is a field. Let $\alpha \in M$ be the image of x in M. Clearly every element of M is a polynomial in α with coefficients in K and so $M = K(\alpha)$. Also, $m \in K[x]$ maps to $0 \in M$, so $m(\alpha) = 0$ in M. The minimal polynomial of m_α divides m in $K[x]$. But

m is irreducible and so $m = m_\alpha$. Finally, let $m = x^d +$ lower order terms $\in K[x]$. Then $\{1, x, x^2, ..., x^{d-1}\}$ is a basis of M over K.

(ii) $\alpha \in L$ is algebraic, and so has a minimal polynomial. Then can define a field homomorphism

$$K[x]/(m_\alpha) \to L$$

by mapping $f(x) \mapsto f(\alpha)$, well-defined since $m_\alpha(\alpha) = 0$. So we get $M \hookrightarrow L$, and its image is exactly $K(\alpha)$. So we have $M \cong K(\alpha)$. □

Theorem. (Extending homomorphisms to simple extensions) *Let M/K be a field extension, where $\alpha \in M$ is algebraic over K with minimal polynomial m_α. Let $i : K \to L$ be a field homomorphism and $\beta \in L$. Then there is a homomorphism $j : K(\alpha) \to L$ with the following properties:*

$$\begin{aligned} j|_K &= i \\ j(\alpha) &= \beta \end{aligned}$$

if and only if $i(m_\alpha)(\beta) = 0$, where $i(m_\alpha) \in L[x]$ is the image of $m_\alpha \in K[x]$ under i.

Proof. Suppose that such a j exists. Then

$$i(m_\alpha)(\beta) = j(m_\alpha)(j(\alpha)) = j(m_\alpha(\alpha)) = 0.$$

So $\beta = j(\alpha)$ is a root of the polynomial m_α that had α as a root. So the condition is necessary.

Now suppose that $i(m_\alpha)(\beta) = 0$. Let $\tilde{K} = i(K) \subseteq L$. Then $i(m_\alpha) \in \tilde{K}[x]$ is monic and irreducible, so it is the minimal polynomial of β over $\tilde{K}$. From the previous Theorem,

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

whereas

$$\tilde{K}(\beta) \cong \tilde{K}[x]/i(m_\alpha).$$

Now we can construct the map j as the following composite:

$$K(\alpha) \cong K[x]/(m_\alpha) \xrightarrow{i} \tilde{K}[x]/i(m_\alpha) \cong \tilde{K}(\beta) \subset L.$$

This is a field homomorphism $j : K(\alpha) \to L$ with $j\,|_k = i$ and $j(\alpha) = \beta$. □

Example.
(1) Let $K = \mathbb{Q}$ and let $M = \mathbb{C}$ and let $\alpha = i$. Then $m_\alpha = x^2 + 1$. Take $L = \mathbb{Q}(i)$ and $\beta = -i$. So $i(m_\alpha) = x^2 + 1$ and hence $i(m_\alpha)(\beta) = 0$. So there is a field homomorphism $j : \mathbb{Q}(i) \to \mathbb{Q}(i)$ taking $i \mapsto -i$.
(2) Let $K = \mathbb{Q}$, $L = \mathbb{Q}(i)$, $\alpha = \sqrt{2}$, $m_\alpha = x^2 - 2$ and $\beta = \pm i$. Can we extend i to $K(\sqrt{2})$? No, since $i(m_\alpha)(\pm i) = (\pm i)^2 - 2 \neq 0$.

Corollary. (Uniqueness of simple algebraic extensions) *Suppose we have a field extension M/K with $\alpha, \beta \in M$ algebraic over K with the same minimal polynomial $m \in K[x]$. Then there is an isomorphism $j : K(\alpha) \to K(\beta)$ with $j\,|_k = \mathrm{Id}$.*

Proof. Take $i = \mathrm{Id}_K$, $L = K(\beta)$ in the above theorem. We get

$$\begin{array}{ccc} & \overset{j}{} & \\ K(\alpha) & \longrightarrow & K(\beta) \\ | & & | \\ & \underset{\mathrm{Id}_K}{} & \\ K & \longrightarrow & K \end{array}$$

and j exists, since $m(\beta) = 0$.

Then $j : K(\alpha) \to K(\beta)$ is injective. Also by the Tower Law,

$$[K(\beta) : j(K(\alpha))] \cdot [K(\alpha) : K] = [K(\beta) : K],$$

hence $K(\alpha) \cong K(\beta)$. □

Corollary. (Homomorphisms from simple extensions) *Let $K(\alpha)/K$ be a simple algebraic extension with α having minimal polynomial m_α over K. Let $i : K \to L$ be a homomorphism. Suppose that $i(m_\alpha) \in L[x]$ has exactly k distinct roots $\{\beta_i\}_{i \leq k}$ in L. Then there are exactly k distinct homomorphisms $j_m : K(\alpha) \to L$ with the property that $j_m|_K = i$ and these are distinguished by $j_m(\alpha) = \beta_m$ for $m \leq k$.*

4. Splitting Fields

4.1. **Basics.**

Definition. Let K be a field, and $f \in K[x]$ a monic polynomial. Then we say that f splits (completely) over K, if

$$f(x) = \prod_{i=1}^{n} (x - a_i) \in K[x].$$

Example. $x^2 + 1$ does not split over $\mathbb{Q}$, but it does split over $\mathbb{Q}(i)$ as $x^2 + 1 = (x - i)(x + i)$.

Trivially, an irreducible polynomial over K of degree at least 2 does not split over K.

Definition. Let K be a field and $f \in K[x]$. A field extension M/K is a *splitting field* of f over K, if

(1) $f \in M[x]$ splits over M;
(2) if $K \subset L \subsetneq M$, then $f \in L[x]$ does not split over L.

Example. The splitting field of $x^2 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$. $x^2 + 1$ splits over $\mathbb{Q}(i)$ and for degree reasons there is no intermediary field.

Theorem. (Existence and Uniqueness of Splitting Fields)

(1) *Given $f \in K[x]$, f has a splitting field M/K over K.*
(2) *Consider $f \in K[x]$ and a field isomorphism $i : K \to K'$ taking*

$$f \mapsto i(f) = f' \in K'[x].$$

Given splitting fields M/K for f, and M'/K' for f', there is an isomorphism $j : M \to M'$ extending $i : K \to K'$.

Proof. We do an induction on the degree of f, noting that all statements are trivial for $\deg f = 1$.

For (1), the induction hypothesis is as follows: for any field K, $f \in K[x]$ with $\deg f < n$, there is a splitting field M/K of f over K.

Take $f \in K[x]$ of degree n, and let f_1 be an irreducible factor of f. Let $K_1 := K[x]/(f_1)$. Then this is a finite extension of K. So in $K_1[x]$ we can write $f = (x - \alpha_1)^{m_1} g(x)$. Now $\deg g < \deg f$ and so has by induction a splitting field N/K_1 over K_1. Now in N, g splits and so f splits completely. Take a smallest subfield M of N in which f splits completely; this is a splitting field of f.

There were choices in the proof of (1), so the statement of (2) is not obvious. We must prove that the resulting fields are isomorphic.

For (2), the induction hypothesis is as follows: for any fields $i : K \cong K'$, $f \in K[x]$ with $\deg f < n$, we have that the splitting fields of f and $i(f)$ over K, K' are isomorphic.

Take any $f \in K[x]$ of degree n. Take a splitting field M/K for f over K. Let $\alpha_1 \in M$ be a root of f and let m be the minimal polynomial of α_1 over K. Now $f(\alpha_1) = 0$, so m divides f in $K[x]$. For $m' = i(m) \in K'[x]$, m' is irreducible in $K'[x]$, and we similarly have that m' divides f' in $K'[x]$. So m' splits in the splitting field M' of f' over K'. Let β_1 be a root of m' in M'. By uniqueness of simple extensions, the extensions $K(\alpha_1)$ and $K(\beta_1)$ are isomorphic, since they correspond to the minimial polynomials m and $m' = i(m)$.

Now M is a splitting field of $f/(x - \alpha_1)$ over $K(\alpha_1)$ and M' is a splitting field of $f'/(x - \beta_1)$ over the isomorphic field $K'(\beta_1)$. So by induction, there is an isomorphism $M \cong M'$ extending $K(\alpha_1) \cong K'(\beta_1)$, which itself extends $K \cong K'$. □

4.2. **Normal Extensions.**

Definition. A field extension L/K is *normal* if, wherever an irreducible polynomial $f \in K[x]$ has a root in L, then f splits in L.

Example. Consider $K = \mathbb{Q}$ and the polynomial $x^3 - 2$, with the field extension $L = \mathbb{Q}\left(\sqrt[3]{2}\right) \cong \mathbb{Q}[x]/(x^3 - 2)$.

Claim. L/K is not normal.

Proof. f has one root $\alpha = \sqrt[3]{2} \in L$, but no other roots in L, since all other roots of f over $\mathbb{Q}$ are non-real. The splitting field M of f is not contained in the real numbers:

$$M = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right),$$

with

$$\omega = e^{\frac{2\pi i}{3}}$$

a third root of unity. □

Example. The field extensions $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are normal, since if a quadratic splits into factors then it splits completely into linear factors.

Theorem. (Characterisation of Normal Extensions) *A finite extension L/K is normal if and only if it is the splitting field of some $f \in K[x]$.*

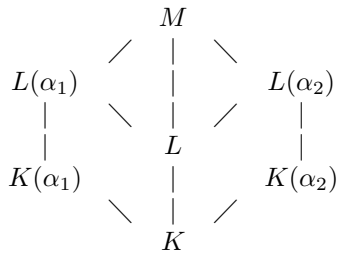
Proof. Assume first that L/K is normal and finite. If $L = K$ then there is nothing to prove. Otherwise, take $\alpha_1 \in L \setminus K$, $\alpha_2 \in L \setminus K(\alpha_1)$, and so on; since the degree increases in each step, this process must terminate, with a generating set

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

with each α_i algebraic over K. Let $m_i \in K[x]$ the minimal polynomial of α_i over K. Set $f = \prod m_i \in K[x]$. Thus each m_i has one root α_i in L, and as L/K is normal, it splits in L. Hence f splits in L. Furthermore, any splitting field of f over K must contain all roots of m_i and so no subfield of L splits f.

Conversely, suppose that L is the splitting field of $f \in K[x]$. Take $g \in K[x]$ irreducible, with a root $\alpha_1 \in L$. Consider a splitting field $M \supseteq L$ of fg over K.

Let $\alpha_2 \in M$ be another root of g in M. We want that $\alpha_2 \in L$. We argue using the following diagram.



We have $K(\alpha_1) \cong K(\alpha_2)$ and $[K(\alpha_1) : K] = [K(\alpha_2) : K] = d = \deg g$, since both are simple extensions using the irreducible $g \in K[x]$.

Next, $L(\alpha_i)$ is the splitting field of f over $K(\alpha_i)$. Thus, by Uniqueness of Splitting Fields, we get an isomorphism $L(\alpha_1) \cong L(\alpha_2)$ extending $K(\alpha_1) \cong K(\alpha_2)$. In particular, $[L(\alpha_1) : K(\alpha_1)] = [L(\alpha_2) : K(\alpha_2)] = e$ for some integer e.

Recalling $\alpha_1 \in L$, we have $[L(\alpha_1) : L] = 1$. Hence by the tower law,

$$\begin{aligned} [L : K] &= \frac{[L(\alpha_1) : K(\alpha_1)] \cdot [K(\alpha_1) : K]}{[L(\alpha_1) : L]} \\ &= d \cdot e. \end{aligned}$$

Hence

$$\begin{aligned} [L(\alpha_2 : L)] &= \frac{[L(\alpha_2) : K(\alpha_2)] \cdot [K(\alpha_2) : K]}{[L : K]} \\ &= \frac{d \cdot e}{d \cdot e} \\ &= 1. \end{aligned}$$

Thus $\alpha_2 \in L$. This completes the proof. □

4.3. **Separable extensions.**

Definition. An irreducible polynomial $f \in K[x]$ is *separable*, if it has $\deg f$ distinct roots in a splitting field. An arbitrary polynomial $f \in K[x]$ is *separable* if all its irreducible factors are.

Definition. Given a field extension L/K, $\alpha \in L$ is *separable over* K, if its minimal polynomial $m_\alpha \in K[x]$ over K is a separable polynomial. A field extension L/K is *separable*, if every $\alpha \in L$ is separable over K.

Theorem. (Separability in characteristic 0) *Assume that* $\operatorname{char} K = 0$. *Then any finite extension* L/K *is separable.*

Proof. Let $m \in K[x]$ be the minimal polynomial of $\alpha \in L$ over K. Suppose that m has a double root β in some splitting field $M \supset K$. Then $m(\beta) = Dm(\beta) = 0$, where D is the formal derivative (see Problem Sheet 1).

On the other hand, Dm is a polynomial with co-efficient of x^{d-1} nonzero since $\operatorname{char} K = 0$, hence Dm is nonzero. $m \in K[x]$ is irreducible, and Dm has smaller degree, so $(m, Dm) = 1$ and thus there are $a, b \in K[x]$ such that $am + b(Dm) = 1$. But substituting β we get a contradiction. □

Example. Take $K = \mathbb{F}_p(t)$. Then this is an infinite field of characteristic p. Consider the polynomial $f(x) = x^p - t \in K[x]$.

Let L/K be a splitting field of f and let $\alpha \in L$ be one root of f. Then in $L[x]$, we have that $(x^p - t) = (x - \alpha)^p$ (since $\beta \to \beta^p$ is a field homomorphism in characteristic p). So f is a non-separable polynomial in K.

The proof of the Theorem breaks down, since $Df = px^{p-1} = 0$ since $\operatorname{char} K = p$.

Proposition. (Separability of intermediate extensions) *If M/K is separable, then for any intermediate field L, the extensions M/L and L/K are separable.*

Proof. L/K is clearly separable, since the minimal polynomial of $\alpha \in L$ over K is the minimal polynomial of $\alpha \in M$ over K. On the other hand, the minimal polynomial $m \in L[x]$ of $\beta \in M$ over L divides the minimal polynomial $m' \in K[x]$ of the same element $\beta \in M$ over K, by properties of the minimal polynomial. If m' has no roots in a splitting field, neither has m. □

Theorem. (Extending homomorphisms to separable extensions) *Let M/K be a field extension of degree d. Let $i : K \to L$ be a field homomorphism to some other field L. Then*

$$\left\{\begin{array}{c}\text{there exist exactly}\\ d \text{ homomorphisms}\\ j_k \colon M \to L\\ \text{extending } i\end{array}\right\} \iff \left\{\begin{array}{c}M/K \text{ is separable, and}\\ \text{the minimal polynomial}\\ \text{of every } \alpha \in M\\ \text{splits in } L[x]\end{array}\right\}.$$

Otherwise, there are fewer than d extensions of i.

Proof. We work by induction on d, the case $d = 1$ being obvious. Let $d > 1$, and assume that the stated equivalence is true for all extensions M/K of smaller degree. Suppose first that

(1) either M/K is not separable,
(2) or there is $\alpha \in M/K$ whose minimal polynomial over K does not split in L.

In both cases, for some $\alpha \in M/K$ its minimal polynomial has fewer than $\deg(m)$ distinct roots in L. So there are fewer than $\deg(m)$ extensions of $i : K \to L$ to $K(\alpha) \to L$. Also, by induction, there are at most $[M : K(\alpha)]$ extensions of each such j to $\tilde{j} : M \to L$. Hence, there are fewer than $\deg(m) \cdot [M : K(\alpha)]$ extensions of $i : K \to L$. However, this number is

$$\begin{aligned}\deg(m) \cdot [M : K(\alpha)] &= [K(\alpha) : K][M : K(\alpha)]\\ &= [M : K]\\ &= d.\end{aligned}$$

Now assume that M/K is separable and that all m_α split in $L[x]$, $\alpha \in M$. Take $\alpha \in M \backslash K$, and let m be its minimal polynomial over K. Then $m \in L[x]$ splits into distinct linear factors

$$m(x) = \prod_{k=1}^{\deg m} (x - \beta_k) \quad \text{for } \beta_k \in L \text{ different.}$$

Now by the Theorem on extending homomorphisms to simple extensions, we have $\deg(m)$ *distinct* extensions of i to $K(\alpha)$. By induction, each of these in turn leads $[M : K(\alpha)]$ extensions of i, giving a total of $[M : K(\alpha)] \cdot \deg(m) = d$ extensions. □

Corollary. *The splitting field L over K of a separable polynomial $f \in K[x]$ is a separable extension of K.*

Remark. The statement is not obvious: for L/K to be separable, we need all minimal polynomials to be separable, not just (components of) f.

Proof. We will give a sketch proof here; see the lectures for more details. Let K be a subfield of a field M and let $i : K \to L$ be a homomorphism of fields. By the proof of the last theorem, using induction on $d = [M : K]$, we have

(i) if $M : K$ is not separable, or if there is some $\alpha \in M$ such that $i(m_\alpha)$ does not split in L, then there are strictly fewer than d field homomorphisms $\tilde{j} : M \to L$ such that $\tilde{j}|_K = i$; and
(ii) if $M = K(\alpha_1, \ldots, \alpha_n)$ where for $1 \leq k \leq n$ the minimal polynomial m_{α_k} of α_k over K is separable and its image under i splits in L, then there are exactly d field homomorphisms $\tilde{j} : M \to L$ such that $\tilde{j}|_K = i$.

Now let $M = L$ be the splitting field of a separable polynomial f over K. Then $M = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of f in L, and for $1 \leq k \leq n$ the minimal polynomial m_{α_k} of α_k over K divides f, so m_{α_k} is separable over K and its image under the inclusion $i : K \to L$ splits in L. Thus (ii) above is satisfied and therefore by (i) the extension is separable.

□

5. Galois Extensions and their Galois Groups

Example. Consider the field extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$. Our aim is to find and understand field automorphisms of the field $\mathbb{Q}(\sqrt{2}, i)$ that fix the subfield $\mathbb{Q}$, in the hope that this will help us to understand the structure of the extension. The field $\mathbb{Q}(\sqrt{2}, i)$ is the splitting field of the irreducible polynomial $x^2 + 1$ over $\mathbb{Q}(\sqrt{2})$; the elements $\pm i$ both have minimal polynomial $x^2 + 1$ over this field. Therefore, by the Theorem on extending field homomorphisms to simple extensions, there is a field automorphism

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}, i) & \xrightarrow{\sigma} & \mathbb{Q}(\sqrt{2}, i) \\ | & & | \\ \mathbb{Q}(\sqrt{2}) & = & \mathbb{Q}(\sqrt{2}), \end{array}$$

with $\sigma\colon i \mapsto -i$.

We can also regard $\mathbb{Q}(\sqrt{2}, i)$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}(i)$. So using the same argument, there is a field automorphism τ defined by

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}, i) & \xrightarrow{\tau} & \mathbb{Q}(\sqrt{2}, i) \\ | & & | \\ \mathbb{Q}(i) & = & \mathbb{Q}(i), \end{array}$$

with $\tau\colon \sqrt{2} \mapsto -\sqrt{2}$.

Consider the group $G =< \sigma, \tau >$, which acts on the field $\mathbb{Q}(\sqrt{2}, i)$ fixing $\mathbb{Q}$. The actions of elements of G on a basis of $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$ can be tabulated as follows.

Notice that

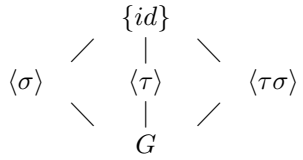
$$\begin{aligned} \sigma^2 &= \mathrm{Id} \\ \tau^2 &= \mathrm{Id} \\ (\sigma\tau)^2 &= \mathrm{Id} \end{aligned}$$

	1	$\sqrt{2}$	i	$\sqrt{2}i$
Id	1	$\sqrt{2}$	i	$\sqrt{2}i$
σ	1	$\sqrt{2}$	$-i$	$-\sqrt{2}i$
τ	1	$-\sqrt{2}$	i	-$\sqrt{2}i$
$\sigma\tau$	1	$-\sqrt{2}$	$-i$	$\sqrt{2}i$

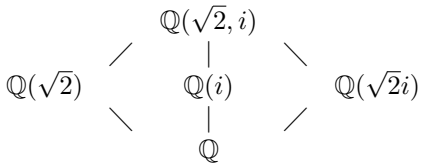
and therefore as an abstract group,

$$G \cong C_2 \times C_2.$$

Finally, let us consider the subgroups of the group G. We get the following structure, where lines denote inclusions of subgroups.



Correspondingly, there is a diagram of subfields of $\mathbb{Q}(\sqrt{2}, i)$:



The diagrams contain all subgroups, respectively subfields, and each subfield is the fixed field of the subgroup in the same position in the table.

Example. Consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Are there any field automorphisms of $\mathbb{Q}(\sqrt[3]{2})$ fixing $\mathbb{Q}$? Note that a field automorphism takes a root of an irreducible polynomial $f \in \mathbb{Q}[x]$ to another root of the same irreducible polynomial f since coefficients of the minimal polynomial are fixed by σ. Applying this to the minimal polynomial $f(x) = x^3 - 2$, we get that for any $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}))$, $\sigma(\sqrt[3]{2})$ is a root of $x^3 - 2$. However, there is only one root of $x^3 - 2$ in this field. So $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ and so $\sigma = \mathrm{Id}$.

The problem here is that the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is *not normal*.

Example. Let L be the splitting field of $x^p - t$ over $\mathbb{F}_p(t)$, which is given by $\mathbb{F}_p(\sqrt[p]{t}) : \mathbb{F}_p(t)$. Are there any automorphisms of L fixing $K = \mathbb{F}_p(t)$? This polynomial has only one root with multiplicity, so again any automorphism is the identity.

The problem here is that the field extension $L/\mathbb{F}_p(t)$ is *not separable*.

5.1. **Definitions.** Recall that for a field extension L/K, we defined

$$\mathrm{Aut}_K(L) = \{\alpha \in \mathrm{Aut}(L) : \alpha|_K = \mathrm{Id}_K\}.$$

From now on, we call this *the Galois group* of L over K, and denote it by $\Gamma(L/K)$, or sometimes $G(L/K)$.

Remark.
(1) $\Gamma(L/K)$ is a subgroup of $\mathrm{Aut}(L)$.
(2) $\Gamma(L/K)$ acts on L fixing K.
(3) By definition, the fixed field $L^{\Gamma(L/K)}$ contains K, but *there is no a priori reason why these two fields should be equal.*

Definition. The field extension L/K is a *Galois extension*, if

$$L^{\Gamma(L:K)} = K.$$

Example. Let $K = \mathbb{Q}(\sqrt{2}, i)$ and $G = \Gamma(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong C_2 \times C_2$. As we saw above, the fixed field $K^G = \mathbb{Q}$ and so $K/\mathbb{Q}$ is a Galois extension. Colloquially we say that the extension ''is Galois".

$\Gamma(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{Id}\}$ and $\mathbb{Q}(\sqrt[3]{2})^{\{\mathrm{Id}\}} \neq \mathbb{Q}$, so $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois. Similarly, the splitting field L of $x^p - t$ over $\mathbb{F}_p(t)$ is not Galois.

The following Theorem summarizes our discussion through examples above. We will prove it in stages in the following sections.

Theorem. (1) *A finite extension L/K is Galois if and only if L/K is normal and separable.*

(2) *Suppose that L/K is Galois. Then there is an inclusion reversing bijection between $\{$Intermediate fields $L \supseteq M \supseteq K\}$ and $\{$Subgroups of $\Gamma(L : K)\}$ given by*

$$\begin{array}{rcl} M & \mapsto & \{\sigma \in \mathrm{Aut}(L) : \sigma|_M = \mathrm{Id}_M\} \\ L^H & \leftarrow & H. \end{array}$$

5.2. **Field degrees and Group Orders.** This section is the techinical core of our proof of the Fundamental Theorem.

Lemma. (Linear Independence of Field Homomorphisms) *Let L, K be fields and let $\sigma_k : K \to L$ be distinct field homomorphisms $k = 1, \ldots, n$. Then $\{\sigma_1, \ldots, \sigma_k\}$ are linearly independent over L.*

Proof. Suppose the converse. Then $\sum_{i=1}^m \lambda_i \sigma_i \equiv 0$ be the shortest relation ($m \leq n$) with $\lambda_i \in L \setminus \{0\}$. So for $x \in K$, $\sum_{i=1}^m \lambda_i \sigma_i(x) = 0$. Pick $\alpha \in K$ such that $\sigma_1(\alpha) \neq \sigma_2(\alpha)$. Then for $x \in K$,

$$\begin{aligned} \sum_{i=1}^m \lambda_i \sigma_i(\alpha x) &= 0 \\ \sum_{i=1}^m \lambda_i \sigma_i(\alpha)\sigma_i(x) &= 0 \\ \sum_{i=1}^m \lambda_i \sigma_1(\alpha)\sigma_i(x) &= 0 \\ \sum_{i=2}^m \lambda_i (\sigma_i(\alpha) - \sigma_1(\alpha))\sigma_i(\alpha) &= 0. \end{aligned}$$

So with $\mu_i = \lambda_i(\sigma_i(\alpha) - \sigma_1(\alpha))$,

$$\sum_{i=2}^m \mu_i \sigma_i \equiv 0$$

is a shorter relation. □

Recall that a group G acts on a field L faithfully if different group elements give different field automorphisms; in other words, the map $G \to \mathrm{Aut}(L)$ is injective.

Theorem. (Degree of fixed subfield) *Suppose a finite group G acts faithfully on a field L. Then $[L : L^G] = |G|$, the number of elements of G.*

Proof. Let $G = \{g_1 = \mathrm{Id}_L, g_2, \ldots, g_n\}$, with $g_i : L \to L$ field automorphisms. Let $m = [L, L^G]$ (perhaps $m = \infty$).

Suppose first that $m < n$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be a basis of L over L^G. For n unknowns $\beta_k \in L$, consider the system of m equations

$$\sum_{k=1}^{n} g_k(\alpha_i)\beta_k = 0 \text{ for } i = 1, \ldots, m.$$

Since $n > m$, there are more unknowns than equations. Hence by the Rank-Nullity Theorem, there is a nonzero solution $\{\beta_k\}$. Hence, for $\alpha \in L$,

$$\sum_{i=1}^{n} \beta_i g_i(\alpha) = 0,$$

and so

$$\sum_{i=1}^{n} \beta_i g_i \equiv 0,$$

as a map $L \to L$. This contradicts Linear Independence of Field Homomorphisms.

Now assume $n < m$ so that there is a linearly independent subset $\{\alpha_1, \ldots, \alpha_{n+1}\}$ of L over L^G with $n + 1$ elements. This time consider the set of n equations

$$\sum_{i=1}^{n+1} g_j(\alpha_i)\beta_i = 0 \text{ for } j = 1, \ldots, n,$$

for $n + 1$ unknowns $\beta_i \in L$. Once again, there are more unknowns than there are equations, so there is a nonzero solution. Reorder this solution $\{\beta_1, \ldots, \beta_{n+1}\}$ such that $\beta_i, \ldots, \beta_r \neq 0$ and $\beta_{r+1}, \ldots, \beta_{n+1} = 0$, and choose a solution with minimal $r \geq 1$. So

$$\sum_{i=1}^{r} g_j(\alpha_i)\beta_i = 0. \tag{2}$$

Operate on this by an element $g \in G$:

$$\sum_{i=1}^{r} g g_j(\alpha_i) g(\beta_i) = 0$$

which implies (through renaming group elements)

$$\sum_{i=1}^{r} g_j(\alpha_i) g(\beta_i) = 0. \tag{3}$$

Now take $(2) \cdot g(\beta_1) - (3) \cdot \beta_1$ to get

$$\sum_{i=2}^{r} g_j(\alpha_i)(\beta_i g(\beta_1) - \beta_1 g(\beta_i)) = 0.$$

The minimality of r implies that all coefficients here are zero. So for all $g \in G$,

$$\beta_i g(\beta_1) - \beta_1 g(\beta_i) = 0,$$

that is,

$$\beta_i/\beta_1 = g(\beta_i/\beta_1)$$

and therefore

$$\beta_i/\beta_1 \in L^G.$$

But from (3), we deduce that

$$\sum_{i=1}^{r} \alpha_i \frac{\beta_i}{\beta_1} = 0$$

which gives a contradiction, since $\{\alpha_1, \alpha_2, \ldots, \alpha_{n+1}\}$ was chosen to be linearly independent over L^G. □

Corollary. *If a finite extension L/K is Galois, then the number of elements in the Galois group $\Gamma(L/K)$ is the same as the degree $[L : K]$.*

Proof. This follows from the previous Theorem, together with the Galois property. □

5.3. **Characterisation of Galois Extensions.**

Theorem. (Characterisation of Galois Extensions) *A finite extension L/K is Galois if and only if L/K is separable and normal.*

Proof. Suppose that L/K is separable and normal of degree n. Then by the Theorem on extending homormophisms to separable extensions, there are exactly $n = [L : K]$ homomorphisms $L \to L$ extending the inclusion $K \to L$. Thus $|\Gamma(L/K)| = n$. Hence $[L : L^{\Gamma(L:K)}] = n$. But $L^{\Gamma(L/K)} \supset K$, $[L : L^{\Gamma(L/K)}] = n = [L : K]$ which implies $K = L^{\Gamma(L/K)}$. Hence L/K is Galois.

Conversely, suppose that L/K is Galois of degree m. Then there exist exactly m homomorphisms $L \to L$ extending the inclusion $K \to L$, the elements of $\Gamma(L : K)$. So by the converse direction of the Theorem on extending homormophisms to separable extensions, L/K is separable and the minimal polynomial of every $\alpha \in L$ over K splits in L. So L/K is normal. □

5.4. **The main theorem.**

Theorem. (Fundamental Theorem of Galois Theory) *Suppose that L/K is finite and Galois, with Galois group G.*

(1) *There is an inclusion reversing correspondence between intermediate field extensions $L/M/K$ and subgroups of G, given as follows:*

$$\begin{Bmatrix} \textit{intermediate fields} \\ L \supset M \supset K \end{Bmatrix} \leftrightarrow \{\textit{subgroups } H < G\}$$

$$\begin{aligned} M &\mapsto G_M = \{\alpha \in \mathrm{Aut}(L) : \alpha \mid_M = \mathrm{Id}_M\} \\ L^H &\leftarrow H. \end{aligned}$$

The degrees are given by

$$[L : M] = |G_M|, \quad [M : K] = \frac{|G|}{|G_M|}.$$

(2) *The intermediate field extension M/K is Galois if and only if $G_M \trianglelefteq G$ is a normal subgroup. In this case, its Galois group is given by*

$$\Gamma(M/K) \cong G/G_M.$$

Proof. For (1), let M be an intermediate field. Then L/M is normal (it is a splitting field over K and so a splitting field over M). Also, L/K separable implies L/M is separable by the Proposition on Separability of intermediate extensions. It follows that L/M is Galois with Galois group $\Gamma(L/M) = G_M$, acting on L as a subgroup of G, with fixed field $L^{G_M} = M$.

Conversely, consider a subgroup $H < G$. It is clear that $H \subseteq G_{L^H}$: H is contained in the group that fixes all elements fixed by H. Now by what we proved in the previous step, we have that

$$L^{G_{L^H}} = L^H.$$

On the other hand, by the theorem on fixed fields and group orders,

$$|H| = [L : L^H] = [L : L^{G_{L^H}}] = |G_{L^H}|.$$

So H and G_{L^H} are both subgroups of G, $H \subseteq G_{L^H}$ and they have the same size. So $H = G_{L^H}$.

Hence the maps $M \mapsto G_M$ and $H \mapsto L^H$ are mutual inverses, so indeed we have a one-to-one correspondence. Clearly, as M gets larger, G_M gets smaller and vice versa. So the correspondence is inclusion reversing.

To do (2), we need a lemma.

Lemma. *Let L/K be a field extension, $L \supset M \supset K$, $\tau \in \Gamma(L/K) = G$. Then $G_{\tau(M)} = \tau G_M \tau^{-1}$, as subgroups of G. Slogan: "Stabilizer of a translate is the conjugate of the stabilizer."*

Proof. If $\alpha \in M$, $g \in G_M$ with $g\alpha = \alpha$ then

$$(\tau g \tau^{-1})(\tau\alpha) = \tau g \alpha = \tau\alpha$$

implies

$$\tau g \tau^{-1} \in G_{\tau(M)}.$$

The converse works likewise. □

Recall we have $L \supset M \supset K$. Suppose that M/K is Galois, in particular normal. Given $g \in G$ and $\alpha \in M$ let m be the minimal polynomial of α over K. Then

$$m(g(\alpha)) = g(m(\alpha)) = 0,$$

so $g(\alpha)$ is another root of the irreducible polynomial $m \in K[x]$. m has one root $\alpha \in M$, and so by normality it splits in M. So $g(\alpha) \in M$. Therefore, $g(M) = M$ for all $g \in G$. By the Lemma therefore, for all $g \in G$,

$$gG_M g^{-1} = G_M.$$

So $G_m \trianglelefteq G$ is a normal subgroup.

Conversely, suppose G_M is a normal subgroup of G. We want to show that the corresponding extension M/K is Galois. Let $\alpha \in M$, $\beta \in L$ a different root of the minimal polynomial m of α over K. Then $K(\alpha)$ is a subfield of L and $K(\beta)$ is a subfield of L, so there are isomorphisms of fields

$$K(\alpha) \cong K(\beta)$$

with $\alpha \mapsto \beta$. By the theorem on uniqueness of splitting fields, this extends to an isomorphism

$$\begin{array}{ccc} L & \cong & L \\ | & & | \\ K(\alpha) & \cong & K(\beta), \end{array}$$

in other words an element $g \in \Gamma(L/K)$, such that $g(\alpha) = \beta$. But $G_{g(M)} = G_M$ by the lemma and the normal subgroup property, so $g(M) = M$, by the one-to-one correspondence of (1). So $\beta \in M$. Hence M/K is normal. Separability follows from that of L/K. M/K is thus Galois.

Finally, if M/K is Galois, define a map

$$\sigma : G \to \Gamma(M/K)$$

by $\sigma(g) = g|_M$. This is surjective by the extension theorem, with $\ker \sigma = G_M$. The isomorphism theorem for groups now gives

$$\Gamma(M/K) \cong G/G_M$$

as claimed. □

6. Galois groups of polynomials

6.1. **Basics.** Take $f \in K[x]$, and for simplicity assume $\operatorname{char} K = 0$ in this section. Let L/K be a splitting field of f over K, and let

$$G_f := \Gamma(L/K).$$

Note that, since we assumed $\operatorname{char} K = 0$, L/K is automatically separable and hence Galois.

Recall that if

$$\begin{aligned} f &= x^n + \sum_{i=0}^{n-1} b_i x^i \in K[x] \\ &= \prod_{i=1}^{n} (x - \alpha_i) \in L[x] \end{aligned}$$

then the coefficients $b_i \in K$ are symmetric polynomials in the roots $\alpha_i \in L$. In particular, the discriminant

$$\Delta_f = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

of f is a polynomial in the b_i's. Finally recall that

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

is not symmetric, but it is invariant under $A_n < S_n$.

Proposition. (1) *If $f \in K[x]$ has n distinct roots then G_f is naturally a subgroup of the symmetric group S_n.*

(2) *If f is irreducible, then G_f is a transitive subgroup of S_n.*

(3) *If $f \in K[x]$ has degree n and has n distinct roots then G_f is contained in the alternating group A_n if and only if*

$$\Delta_f \in K^2 = \{a^2 : a \in K\}.$$

Proof. (1) If $\alpha \in L$ is a root of $f \in K[x]$, then for all $g \in G_f$, $g(f(\alpha)) = f(g(\alpha)) = 0$ and so $g(\alpha) \in L$ is another root of f. If $\alpha_1, \ldots, \alpha_n$ are all the roots of f, then

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

So we obtain a homomorphism $G \to S_n$ with $g \mapsto (\alpha_i \mapsto \alpha_j)$. This homomorphism is injective, since g fixes K and $g : \alpha_i \mapsto \alpha_j$ determines the action of g on L.

(2) Using the argument often used before, if f irreducible, then for α_i, α_j different roots, there is an isomorphism $K(\alpha_i) \cong K(\alpha_j)$ extending to an automorphism $g : L \to L$ such that $g(\alpha_i) = \alpha_j$. So G_f is transitive.

(3) We have $\Delta_f \in K^2$ if and only if $\delta_f \in K$ if and only if $\delta_f \in L^{G_f} = K$ if and only if $G_f \leq A_n$, by the last observation before the statement of the proposition. □

Lemma. *Let L be a finite field, then $L^* = L \setminus \{0\}$ is cyclic.*

Proof. Recall that a finite group is cyclic if and only if there is exactly one subgroup for each divisor of the group order. Suppose L^* is not cyclic and then fix two subgroups G_1, G_2 having the same order d. Consider the polynomial $f = x^d - 1$. The set of roots of this polynomial contains $S = G_1 \cup G_2$. Since S has size greater or equal than $d + 1$, we get the contradiction, as L is a field f has degree d. □

Theorem. (Theorem of the Primitive Element) *If L/K is finite and separable, then there is some $\theta \in L$ such that $L = K(\theta)$.*

Example. $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$.

Proof. If K is finite, than L is finite and we can set θ to be the generator of $L^* = L \setminus \{0\}$.

Therefore, we can assume that K is infinite. Since L is finite dimensional over K, it can be written as $K(\alpha_1, \ldots, \alpha_n)$ for some $n \in \mathbb{N}$ and $\alpha_1, \ldots, \alpha_n \in M$. If we can find θ_1 such that $K(\alpha_1, \alpha_2) = K(\theta_1)$, the claim will follow by induction. Let m_1 and m_2 be the minimal polynomials of α_1 and α_2 respectively. Consider the splitting field of $m_1 m_2$, which is a Galois extension of K. Using the fundamental theorem of Galois Theory we observe that the number extensions of K contained is M is finite (why?). Therefore, the set of extensions of the form $\{K(\alpha_1 + b\alpha_2)\}_{b \in K}$ is finite. Which directly implies $K(\alpha_1 + c\alpha_2) = K(\alpha_1 + d\alpha_2)$, which forces $\alpha_1 + c\alpha_2 \in K(\alpha_1 + d\alpha_2)$, from which it follows $\alpha_2 \in K(\alpha_1 + d\alpha_2)$ and so $\alpha_1 \in K(\alpha_1 + d\alpha_2)$. Therefore, set $\theta_1 = \alpha_1 + d\alpha_2$.

□

6.2. **Polynomials of Low Degree.**

Quadric Polynomials Let $f(x) = x^2 + ax + b$, which we reduce to $g(y) = y^2 + c$ using the change of variables $x \mapsto y + \frac{a}{2}$. We have $\Delta_f = \Delta_g = -4c$. Then f is irreducible if and only if $-c \notin K^2$, if and only if $[L : K] = 2$, and in this case, the Galois group has one nontrivial element

$$\begin{array}{rcl} \sigma : \sqrt{-c} & \mapsto & -\sqrt{-c} \\ \alpha_1 & \leftrightarrow & \alpha_2 \end{array}$$

leading to

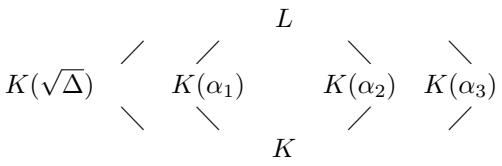
$$G_f = \langle \sigma \rangle / \langle \sigma^2 = \mathrm{id} \rangle \cong S_2.$$

Cubic Polynomials

Proposition. *Let $f \in K[x]$ be an irreducible cubic with discriminant Δ, splitting field L/K and Galois group $\Gamma(L/K) = G_f$. Then*

(1) *if $\Delta \in K^2$, then $G_f \cong A_3$ and L/K is a cubic extension, generated by any of the roots of f.*

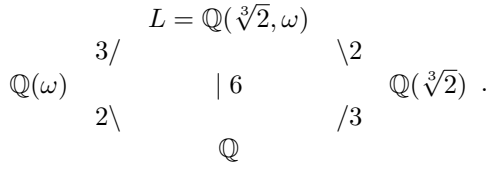
(2) *If $\Delta \in K \setminus K^2$, then $G_f \cong S_3$, and the structure of intermediate fields is as follows:*



with α_i the roots of f.

Proof. Since f is irreducible, the simple extension it generates is of degree 3. By general theory, $G_f < S_3$ and has order divisible by 3, so it can only be S_3 or A_3, depending on the discriminant. The rest of the statement follows immediately. □

Example. (1) Consider $f(x) = x^3 - 2$ over $\mathbb{Q}$. f is irreducible by Eisenstein, and we have



So $|G_f| = [L : \mathbb{Q}] = 6$ and $G_f \cong S_3$.

In this case, we can in fact construct the elements of G_f explicitely. We have roots $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ and there is a Galois automorphism σ, fixing $\mathbb{Q}(\omega)$, and mapping

$$\begin{aligned} \sqrt[3]{2} &\mapsto \sqrt[3]{2}\omega \\ \sqrt[3]{2}\omega &\mapsto \sqrt[3]{2}\omega^2 \\ \sqrt[3]{2}\omega^2 &\mapsto \sqrt[3]{2}. \end{aligned}$$

There is also an automorphism τ fixing $\mathbb{Q}\left(\sqrt[3]{2}\right)$, and mapping

$$\omega \mapsto \omega^2.$$

The elements σ and τ generate a group isomorphic to S_3, with σ acting as a three-cycle on the roots and τ as a two-cycle.

(2) $f(x) = x^3 - x - \frac{1}{3} \in \mathbb{Q}[x]$. Then by Sheet 1,

$$\Delta \quad = \quad -4(-1)^3 - 27\left(-\frac{1}{3}\right)^2 = 4 - 3 = 1 \in \mathbb{Q}^2.$$

f is irreducible over $\mathbb{Q}$, since f has no root over $\mathbb{Q}$. Thus $G_f \cong A_3$.

Quartic Polyomials We have done one example in the introduction to Chapter 5, $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$ over $\mathbb{Q}$. Here we obtained

$$\Gamma(\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}) \cong C_2 \times C_2 \hookrightarrow S_4.$$

For another example, let $f(x) = x^4 - 2$. Set $\alpha = \sqrt[4]{2}$, then the splitting field is $L = \mathbb{Q}(\alpha, i)$. We have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, and $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$ since the two fields cannot be the same (one real, the other not) but the degree is clearly at most two.

On the other hand, much as before, there is a Galois automorphism σ, fixing $\mathbb{Q}(i)$, and mapping α to $i\alpha$, as well as an automorphism τ fixing $\mathbb{Q}(\alpha)$, and mapping i to $-i$. These elements σ and τ generate a group of order eight, isomorphic to the dihedral group D_8. For further details, read Chapter 12 of Stewart's book.

7. Some special classes of extensions

7.1. **Cyclotomic Extensions.** Let L be the splitting field of $f(x) = x^n - 1$ over a field K, assuming that $\operatorname{char} K \nmid n$.

Proposition. *L/K is Galois.*

Proof. L is a splitting field, so L/K is normal. The polynomial $x^n - 1$ is separable over K, since $Df = nx^{n-1} \neq 0$ since $\operatorname{char} L \nmid n$. So L/K is Galois. □

Definition. Let

$$\mu_n(L) = \{\alpha \in L : \alpha^n = 1\}.$$

Note that $\mu_n(L)$ is a group.

Fact. The group $\mu_n(L)$ cyclic of order n. You know this fact over $\mathbb{Q}$ from the Argand plane description of $\mathbb{C}$; we will take this for granted over arbitrary fields of characteristic prime to n.

Definition. An element $\omega \in \mu_n(L)$ is *primitive* or a *primitive root of* 1, if it generates the cyclic group $\mu_n(L)$.

Note that if ω is primitive, then $L = K(\omega)$. Note also that if ω is a primitive root, then the other primitive roots are ω^i for $i \in U(\mathbb{Z}_n)$, the units in $\mathbb{Z}_n$.

Theorem. *Fix a primitive root $\omega \in L$ of 1.*

(1) *Define*

$$\Phi_n(x) = \prod_{i \in U(\mathbb{Z}_n)} (x - \omega^i).$$

(Note that the product is over all primitive roots of 1.) Then $\Phi_n(x) \in K[x]$.

(2) *There is an injective homomorphism $\theta : \Gamma(L : K) \to U(\mathbb{Z}_n)$.*

(3) *θ is an isomorphism if and only if Φ_n is irreducible.*

Proof. Let $G = \Gamma(L : K)$ be the Galois group, then $\sigma \in G$ must map a generator of $\mu_n(L)$ to another generator, and a root of $x^m - 1$ to another root. So $\sigma(\omega) = \omega^{\theta(\sigma)}$, where $\theta(\sigma) \in U(\mathbb{Z}_n)$. Then this defines $\theta : G \to U(\mathbb{Z}_n)$ which is easily seen to be a group homomorphism. It is injective, since the effect of σ on L is determined by the effect of σ on ω, since as we saw, $L = K(\omega)$.

Now G permutes $\{\omega^j : j \in U(\mathbb{Z}_n)\}$ so the coefficients of $\Phi_n(x)$ are fixed by G, and so $\Phi_n(x) \in L^G[x] = K[x]$. Φ_n is irreducible if and only if ω can be mapped to all other primitive roots, if and only if θ is an isomorphism. □

Corollary. *G is abelian.*

Proof. □

Remark. In fact, the cyclotomic polynomial Φ_n is irreducible in $\mathbb{Q}[x]$ for all n. This is very easy to see for $n = p$ prime. We will not need the general case. Φ_n is often reducible over finite fields; see Worksheets for examples.

7.2. **Kummer Extensions.** Continuing our study in the last section, let L be a field in which $x^n - 1$ splits. Let us study the polynomial $x^n - \theta \in L[x]$, for $\theta \in L$. In other words, we are studying extensions

$$M = L(\sqrt[n]{\theta}),$$

under the assumption that $\mathrm{char} L \nmid n$.

Theorem. *Suppose that L is a field with $\mathrm{char} L \nmid n$ and assume that $x^n - 1$ splits in L.*

(1) *Let M be the splitting field of $x^n - \theta$ over L. Then M/L is Galois, with Galois group cyclic of order dividing n.*
(2) *Suppose that M/L is a Galois extension of L with Galois group cyclic of order n. Then there exists $\theta \in L$ and a root $\beta \in M$ of $x^n - \theta \in L[x]$, an irreducible polynomial such that $M = L(\beta)$.*

Proof. (i) Let $L(\beta)$ be a primitive extension of L with a root of $x^n - \theta$. Let $\omega \in L$ be a primitive n^{th} root of unity. Then in $L(\beta)$,

$$x^n - \theta = (x - \beta)(x - \omega\beta)(x - \omega^2\beta) \dots (x - \omega^{n-1}\beta) \in L(\beta)[x]$$

so $M = L(\beta)$ is the splitting field. $\beta \in M$ is separable over L and so M/L is separable (see Worksheet 3). So M/L is Galois.

Now let $G = \Gamma(M : L)$, then for $\sigma \in G$, $\sigma(\beta) = \omega^{j(\sigma)}\beta$, since it has to be another root of $x^n - \theta$. We get an injective map

$$j : G \quad \to \quad \mathbb{Z}_n.$$

It is a group homomorphism, since

$$\begin{aligned} \tau(\sigma(\beta)) &= \tau(\omega^{j(\sigma)}\beta) = \omega^{j(\sigma)}\tau(\beta) = \omega^{j(\sigma)}\omega^{j(\sigma)}\beta \\ &= \omega^{j(\sigma)+j(\sigma)}\beta. \end{aligned}$$

Hence $G < \mathbb{Z}_n$, so is cyclic of order dividing n.

(ii) Let $G =< \sigma >$ be the cyclic Galois group of M/L. Then

$$\mathrm{id}, \sigma, \sigma^2, \dots, \sigma^{n-1} : M \to M$$

are distinct field homomorphisms, so they are linearly independent, hence $\exists \alpha \in M$ such that

$$\beta = \alpha + \omega\sigma(\alpha) + \omega^2\sigma^2(\alpha) + \dots + \omega^{n-1}\sigma^{n-1}(\alpha) \neq 0. \tag{4}$$

So

$$\sigma(\beta) = \sigma(\alpha) + \omega\sigma^2(\alpha) + \omega^2\sigma^3(\alpha) + \dots + \omega^{n-1}\alpha = \omega^{-1}\beta.$$

Hence $\beta \notin L$ (not fixed by σ), $\sigma(\beta^n) = \beta^n$, so $\beta^n = \theta \in M^G = L$. So $L(\beta)/L$ splits $x^n - \theta$ over L, and $< \sigma >$ consists of distinct field automorphisms of $L(\beta)$ fixing L. That is,

$$n = [M : L] \geq [L(\beta) : L] \geq n$$

and so

$$M = L(\beta).$$

□

7.3. **Solving cubics by radicals.** Let $f \in K[x]$ be an irreducible cubic, and assume $\mathrm{char}K \neq 2, 3$. Recall the discriminant Δ_f of f, and that if L is a splitting field of f over K, then

$$\Gamma(L:K) = \begin{cases} A_3, & \text{if } \Delta \in K^2 \\ S_3, & \text{if } \Delta \notin K^2 \end{cases}.$$

Let ω be a primitive cube root of unity over K. Then $L(\omega)$ is Galois over $K(\omega, \sqrt{\Delta})$, with $\Gamma(L(\omega) : K(\omega, \sqrt{\Delta}))$ having order 3. Since the only group of order 3 is C_3, the Galois group is cyclic. So by the Theorem above, $L(\omega)$ is a Kummer extension, the splitting field of some polynomial $x^3 - \theta$ over $K(\omega, \sqrt{\Delta})$. So all the roots of f are contained in the extension $K(\omega, \sqrt{\Delta}, \sqrt[3]{\theta})$ of K.

Explicitely, take

$$f(x) = x^3 + px + q \in K[x].$$

Suppose that the roots are $\alpha_1, \alpha_2, \alpha_3$. Imitating (4) above, set

$$\beta = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$$

and

$$\gamma = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3.$$

Explicit calculations show that

$$\begin{aligned} \beta\gamma &= -3p \\ \beta^3 + \gamma^3 &= -27q. \end{aligned}$$

So β^3, γ^3 are roots of $X^3 + 27qX - 27p^3 = 0$ and we can solve for the roots explicitly from this, recalling that $\alpha_1 + \alpha_2 + \alpha_3 = 0$.

8. Solvable Groups and Solubility by Radicals

8.1. **Solvable Groups.**

Definition. A finite group G is *soluble* or *solvable*, if it has a series of subgroups $\{e\} = G_0 < G_1 < \cdots < G_n = G$, such that $G_{i-1} \trianglelefteq G_i$ is normal, and G_i/G_{i-1} is abelian.

Examples. (1) Any abelian group is solvable; take $\{e\} \trianglelefteq G$.

(2) S_3 is not abelian, but it is solvable: take the chain

$$\{e\} < A_3 < S_3.$$

The quotients are $A_3/\{e\} \cong C_3$ and $S_3/A_3 \cong C_2$.

(3) S_4 is not abelian, but still solvable. This time take the chain

$$\{e\} < V_4 < A_4 < S_4,$$

where V_4 is the Klein Four group generated by all permutations of cycle type $2-2$. The quotients are $V_4/\{e\} \cong C_2 \times C_2$, $A_4/V_4 \cong C_3$ and of course $S_4/A_4 \cong C_2$.

(4) The group A_5 is not soluble. See below.

Proposition. (1) *Suppose that G is solvable, $H \leq G$. Then G is solvable.*

(2) *Suppose G is solvable, $N \trianglelefteq G$. Then G/N is solvable.*

(3) *Suppose $N \trianglelefteq G$ and N, G/N are both solvable. Then G is solvable.*

Remark. Motto: "The set of solvable finite groups is closed under taking subgroups, quotient groups and extensions." This would not be true for abelian groups!

Proof. For (i), let $\{G_i\}_{i\leq n}$ be a series for G, and $H \leq G$. Then let $H_i := G_i \cap H$. Clearly $H_{i-1} \trianglelefteq H_i$, and the inclusion

$$H_i \quad = \quad H \cap G_i \hookrightarrow G_i$$

defines, after taking quotients, an injective map

$$H_i/H_{i-1} \quad = \quad H \cap G_i/H \cap G_{i-1} \hookrightarrow G_i/G_{i-1}.$$

The latter is abelian by assumption. So H_i/H_{i-1} is a subgroup of an abelian group and thus abelian.

For (ii), let $\{G_i\}_{i\leq n}$ be a series for G, and let $N_i := G_i \cdot N/N < G/N$. It's clear that $N_{i-1} \trianglelefteq N_i$ and for the quotient,

$$\begin{aligned} G_i/G_{i-1} \quad &\to \quad N_i/N_{i-1} = \frac{(G_i \cdot N)/N}{(G_{i-1} \cdot N)/N} \\ g \quad &\mapsto \quad g.e + (G_{i-1} \cdot N)/N \end{aligned}$$

is a surjective map. By assumption, G_i/G_{i-1} is abelian, hence N_i/N_{i-1} is a quotient of an abelian group and thus abelian.

For (iii), suppose we have a series $\{N_i\}_{i\leq m}$ for N. A result from elementary group theory says that any subgroup of G/N can he written as G_i/N for some $G_i \leq G$. So we take the series $\{G_i/N\}_{i\leq n}$. We then stick the two chains together:

$$N_0 < N_1 < \cdots < N_m = G_0 < G_1 < \cdots < G_n.$$

By assumption, each group here is normal in the next one, and successive quotients are N_i/N_{i-1}, which is abelian, or

$$G_i/G_{i-1} \quad \cong \quad \frac{G_i/N}{G_{i-1}/N}$$

by the 3rd Isomorphism Theorem, which is also abelian, by assumption. □

Proposition. *The groups A_n and S_n, for $n \geq 5$, are not soluble.*

Proof. As proved in Part A, the group A_5 is simple: it has no normal subgroups at all. Since A_5 is certainly not abelian, it cannot be soluble. The groups A_n and S_n, for $n \geq 5$, have A_5 as a subgroup, so they cannot be soluble either. □

8.2. **Solubility by Radicals.** In order to avoid assumptions on the characteristic, assume in this section that all fields have characteristic 0.

Definition. A field extension L/K is *radical*, if there is a sequence of elements $\alpha_1, \ldots, \alpha_n \in L$ and positive integers $m_1, \ldots, m_n$, so that

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

and for all i,

$$\alpha_i^{m_i} \in K(\alpha_1, \ldots, \alpha_{i-1}).$$

Given a polynomial $f \in K[x]$, we say that f can be *solved by radicals*, if there is a radical extension M/K in which f splits. Note that M can be larger than the splitting field.

Theorem. *Suppose L/K is a finite Galois extension. Then there exists a finite extension M of L such that M/K is radical if and only if $\Gamma(L : K)$ is solvable.*

Proof. "⇒":
Step 1. Suppose that there is a radical extension M/K containing L/K; let $M = K(\alpha_i)$ with

$$\alpha_i^{m_i} \in K(\alpha_1, \ldots, \alpha_{i-1}).$$

Let m_i be the minimal polynomial of α_i over K. Let N be the splitting field over K of $\prod_{i=1}^n m_i$. Then N is a splitting field and each α_i is separable over K, so N is separable over K. So N/K is Galois.
Step 2. We show that N/K is still radical. Let β be any root of m_i. Then since m_i is irreducible over K, there is an element $\sigma \in \Gamma(N/K)$, such that $\sigma(\alpha_i) = \beta$. Hence

$$\beta^{n_i} = \sigma(\alpha_i)^{n_i} \in K(\sigma(\alpha_j) : \sigma \in \Gamma(N/K), j < i).$$

Doing this inductively, we see that N/K is radical.
Step 3. We have an iterated extension $N/L/K$. Here N/K is Galois by Step 1, L/K is Galois by assumption. By the Fundamental Theorem of Galois Theory, we have a surjective map $\Gamma(N : K) \to \Gamma(L : K)$. Hence it would be enough to prove that $\Gamma(N/K)$ is solvable.
Step 4. Now N/K is Galois and radical. We prove that $\Gamma(N/K)$ is solvable by induction on the degree $[N : K]$. Let $N = K(\beta_1, \ldots, \beta_s)$, with

$$\beta_i^{n_i} \in K(\beta_1, \ldots, \beta_{i-1}).$$

Without loss of generality, we can assume that $n_i = p_i$ prime. Then $\beta = \beta_1 \notin K$, but for $p = p_1$, $\gamma = \beta^p \in K$ for p prime. So the minimal poly of β over K divides $x^p - \gamma \in K[x]$. Let $\beta' \in N$ be another root of this minimal polynomial over K. So $(\beta'/\beta)^p = 1$, so N contains a non-trivial, therefore primitive, p^{th} root of unity ϵ.
Step 5. Finally consider

$$K \hookrightarrow K(\epsilon) \hookrightarrow K(\epsilon, \beta_1) \hookrightarrow N.$$

$K(\epsilon)/K$ is the splitting extension of $x^p - 1$, a cyclotomic extension, so has abelian Galois group. $K(\epsilon, \beta)/K(\epsilon)$ is the splitting extension of $x^p - \gamma$ over $K(\epsilon)$, a Kummer extension, and so has cyclic Galois group. $N/K(\epsilon, \beta_1)$ is a radical Galois extension of degree strictly smaller than $[N : K]$.

The corresponding chain of subgroups of $\Gamma(N : K)$ is

$$\Gamma(N : K) \triangleright \Gamma(N : K(\epsilon)) \triangleright \Gamma(N : K(\epsilon, \beta_1)).$$

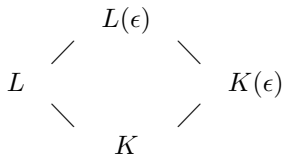
The quotients in these steps are abelian since they are the Galois groups of the cyclotomic and Kummer extensions discussed above; $\Gamma(N : K(\epsilon, \beta_1))$ is solvable by induction. Hence $\Gamma(N : K)$ is solvable.

"⇐":

We prove this by induction on the size of the Galois group $\Gamma(L : K)$.

Let $G = \Gamma(L : K) \triangleright H$, for H a maximal normal subgroup of G. Then G/H is solvable and has no nontrivial normal subgroups by maximality of H. So G/H is abelian (since it must have chain $\{e\} \trianglelefteq G/H$) without subgroups, and so it must be the case that $G/H \cong C_p$ for some prime p.

Let L_1 be the splitting field of $x^p - 1$ over L. We have $L_1 = L(\epsilon)$ where ϵ is a primitive p^{th} root of unity. Then L_1/K is Galois. We have the tower of fields



If $\sigma \in \Gamma(L(\epsilon) : K(\epsilon))$, then σ maps L to L, since L/K is normal. Consider the homomorphism

$$\begin{array}{rcl} \theta : \Gamma(L(\epsilon) : K(\epsilon)) & \to & \Gamma(L : K) \\ \sigma & \mapsto & \sigma|_L. \end{array}$$

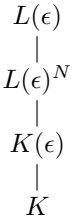
If $\theta(\sigma) = \mathrm{Id}_L$, i.e. $\sigma|_L = \mathrm{Id}_L$, then σ fixes L and also ϵ, so $\sigma = \mathrm{Id}_{L(\epsilon)}$. Hence θ is an injection. There are two cases.

Case 1: θ is strictly injective.

We have that $\#\Gamma(L(\epsilon) : K(\epsilon)) < \#\Gamma(L : K)$. $\Gamma(L(\epsilon) : K(\epsilon))$ is then solvable (being a subgroup of a solvable group $\Gamma(L : K)$) and of smaller order. By induction, $L(\epsilon)$ is contained in a radical extension M of $K(\epsilon)$, so L is contained in a radical extension M of K.

Case 2: θ is an isomorphism.

$H \trianglelefteq G$ corresponds under θ to $N \trianglelefteq \Gamma(L(\epsilon) : K(\epsilon))$. Then consider the following chain of fields:



Then $L(\epsilon) : L(\epsilon)^N$ is a Galois extension with Galois group N, soluble of order less than G. So by induction, $L(\epsilon)$ is contained in a radical extension of $L(\epsilon)^N$.

$L(\epsilon)^N : K(\epsilon)$ is a Galois extension with Galois group $\Gamma(L(\epsilon) : K(\epsilon)) \cong G/H \cong C_p$ and $K(\epsilon)$ has all the p^{th} roots of unity, so this is a radical extension by Kummer theory.

$K(\epsilon) : K$ is a radical extension.

So L is contained in M, a radical extension of H. □

Corollary. *Over a field K of characteristic zero, polynomials $f \in K[x]$ of degree at most four can be solved by radicals.*

Proof. The Galois group $G_f < S_4$, S_4 is solvable and so G_f is solvable. □

8.3. **The general polynomial equation.** Fix a field k of characteristic 0, and let $\alpha_1, \ldots, \alpha_n$ be independent variables. Consider

$$\prod_{i=1}^{n}(x - \alpha_i) = \sum_{i=0}^{n}(-1)^i s_{n-i} x^i.$$

The *field of coefficients* is $K = k(s_1, \ldots, s_n)$, the field of rational functions in the n variables $s_i = s_i(\alpha_j)$, the elementary symmetric polynomials of the α_j. The *field of roots* is $L = k(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n)$, the splitting field of f over K.

Theorem. *The extension L/K is finite and Galois with $\Gamma(L : K) \cong S_n$.*

Proof. Recall that S_n acts on $L = k(\alpha_1, \ldots, \alpha_n)$ by permuting the α_i. By the theorem on symmetric functions,

$$L^{S_n} = k(\alpha_1, \ldots, \alpha_n)^{S_n} \cong k(s_1, \ldots, s_n) = K.$$

So L/K is Galois, with Galois group S_n. □

Corollary. *If $n \geq 5$, L/K is not contained in a radical extension of K. In other words, for $n \geq 5$, there is no formula involving field operations and radical expressions that expresses the roots α_j in terms of the coefficients s_i.*

8.4. **Insoluble quintics.** The Corollary in the previous section leaves open the possibility that, for special fields (e.g. $\mathbb{Q}$), any quintic (say) could be solved by some radical formula. To see that this is not the case, we will exhibit some explicit polynomials over $\mathbb{Q}$ with maximal Galois group. We recall the following group-theoreric

Facts.
(1) (Cauchy's Theorem) For G a finite group, if a prime p divides the order of G, then G has an element of order p.
(2) For a prime p, if $\sigma, \tau \in S_p$ are an arbitrary 2-cycle and p-cycle respectively, then the symmetric group S_p is generated by σ, τ.

Proposition. *Let p be prime, f an irreducible degree p polynomial over $\mathbb{Q}$, and suppose f has precisely two non-real roots. Then $G_f \cong S_p$.*

Proof. Let L be the splitting field of f. Then $\mathbb{Q} \subseteq \mathbb{Q}[x]/(f) \subseteq L$, so by the Tower Lemma, $[L : \mathbb{Q}]$ is divisible by $[\mathbb{Q}[x]/(f) : \mathbb{Q}] = \deg f = p$. So p divides $[L : \mathbb{Q}]$ and hence $\#G_f$. So by Cauchy's Theorem, G_f has an element τ of order p, which is necessarily a p-cycle.

On the other hand, $L \not\subseteq \mathbb{R}$, since f has some complex roots, so

$$\begin{array}{rcl} \sigma : L & \to & L \\ z & \mapsto & \bar{z} \end{array}$$

is a non-trivial element of G_f, interchanging two roots and fixing all others. Thus σ is a 2-cycle.

Thus G contains both a p-cycle and a 2-cycle. By the second fact above, $G_f \cong S_p$. □

Corollary. *The polynomial $x^5 - 6x + 3 \in \mathbb{Q}[x]$ has Galois group S_5 and thus cannot be solved by radicals over $\mathbb{Q}$.*

9. Other topics

9.1. **Finite Fields.**

Theorem. *Let F be a finite field. Then for some prime p,*
(1) $\operatorname{char} F = p > 0$, *the prime subfield of F is $\mathbb{F}_p$, and $|F| = p^n$ for $n = [F : \mathbb{F}_p]$.*
(2) *F is the splitting field over $\mathbb{F}_p$ of $x^{p^n} - x \in \mathbb{F}_p[x]$. In particular, any two finite fields of the same size are isomorphic.*

(3) *$F/\mathbb{F}_p$ is Galois with $\Gamma(F:\mathbb{F}_p) \cong C_n$.*
(4) *If F_1, F_2 are finite extensions of $\mathbb{F}_p$ of degrees m, n, then $F_1 \subseteq F_2$ if and only if m divides n.*

Proof. The statements in (1) follow from the definition of the prime subfield and the fact that F is finite. For (2), the multiplicative group $F^\star$ has order $p^n - 1$, so each $\alpha \in F^\star$ has a multiplicative order dividing $p^n - 1$, and so $\alpha^{p^n-1} = 1 \in F$. Hence for all $\alpha \in F$, $\alpha^{p^n} - \alpha = 0$. The polynomial $x^{p^n} - x$ has p^n different roots in F, so F is the splitting field over $\mathbb{F}_p$ of $x^{p^n} - x \in \mathbb{F}_p[x]$. By the uniquness of the splitting field, any two finite fields of the same size are isomorphic.

For (3), $F/\mathbb{F}_p$ is a splitting field of the polynomial $x^{p^n} - x$ which is a separable polynomial, since $D[x^{p^n} - x] = -1 \neq 0$ at any root. Hence $F/\mathbb{F}_p$ is separable and thus Galois.

Consider the Frobenius homomorphism

$$\begin{array}{rcl} \varphi : F & \to & F \\ \alpha & \mapsto & \alpha^p. \end{array}$$

As a map of fields, φ is injective, and since F is finite, it must be an isomorphism. For $\alpha \in \mathbb{F}_p$, $\varphi(\alpha) = \alpha$ and so $\varphi \in \Gamma(F:\mathbb{F}_p)$. On the other hand, for $\alpha \in F$, we have

$$\varphi^n(\alpha) = \alpha^{p^n} = \alpha$$

in F, hence

$$\varphi^n = e \in \Gamma(F:\mathbb{F}_p).$$

Also, for $1 < i < n$, φ^i cannot be trivial since $\alpha^{p^i} = \alpha$ cannot hold for all $\alpha \in F$ for degree reasons. Thus $(\varphi) \cong C_n < \Gamma(F:\mathbb{F}_p)$. But $[F:\mathbb{F}_p] = n$ and so $\Gamma(F:\mathbb{F}_p) \cong C_n$, generated by the Frobenius automorphism.

Finally for (4), $F_1 \subseteq F_2$ gives a tower of fields and groups

$$\begin{array}{cc} F_2 & \{e\} \\ | & | \\ F_1 & G \\ | & | \\ \mathbb{F}_p & C_n. \end{array}$$

$G < C_n$, so it is cyclic of order k with $k \mid m$ by Lagrange. Then $[F_2 : F_1] = k$, $[F_1 : \mathbb{F}_p] = \frac{m}{k} = n$ and so m divides n. Conversely, if m divides n, we have a tower of groups with $G \cong C_{m/n}$ and then F_1 arises as the fixed subfield $F_2^G \subseteq F_2$. □

Note in particular that any finite extension of finite fields is separable.

9.2. **Constructibility.** We would like to make geometric constructions in the Euclidean plane using ruler and compass. Formally, we are working in $\mathbb{R}^2$ with basic operations:

- Given two points in $\mathbb{R}^2$, connect them by a line.
- Given a point in $\mathbb{R}^2$ and a line segment, draw a circle with the point as centre and that segment as radius.
- Given any pair of lines and/or circles, take the points of intersection.

The aim is to perform certain classical constructions, such as dividing a given angle into n equal parts, and constructing regular polygons.

Definition. Given finite sets $S \supset S_0$ of points in $\mathbb{R}^2$, we say that S can be constructed from S_0 if there is a chain of subsets

$$S_0 \subset S_1 \subset \cdots \subset S_n = S$$

such that points in $S_i \backslash S_{i-1}$ have been constructed from points in S_{i-1} using the basic operations.

We start with $S = \{p_0, p_1\}$ and say that $d(p_0, p_1) = 1$.

Example. Some basic constructions.

(1) We can construct midpoints of line sections: take $S = (p_0, p_1)$ as above. Then we can put a line through them and take the intersections of two circles through p_0 and p_1 using the line segment $\overrightarrow{p_0 p_1}$ as its radius. This will yield two more points, and the intersection of this new line with the original line segment is the midpoint of p_0, p_1.

(2) Given P, Q, R we can construct T_1, T_2, T_3 so that for the lengths of segments, we have

$$\begin{aligned} \overline{PQ} \cdot \overline{PR} &= \overline{PT_1} \text{ (multiply lengths);} \\ \overline{PQ} \cdot \overline{PT_2} &= \overline{PR} \text{ (divide lengths);} \\ \overline{PT_3} \cdot \overline{PT_3} &= \overline{PQ} \text{ (take square root).} \end{aligned}$$

We can also add and subtract segments easily.

Given a set $S = \{(x_i, y_i) : i \in I\}$, let $K_S := \mathbb{Q}(\bigcup_i \{x_i, y_i\})$. We start with $K_{s_0} = \mathbb{Q}$.

Theorem. (1) *If S is constructible from S_0, then $[K_S : \mathbb{Q}] = 2^m$.*

(2) *Given any subfield of the real numbers wiith a series of subfields*

$$\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L_n = L$$

with $[L_i : L_{i+1}] = 2$, then a point P with coordinates in L can be constructed from S_0.

(3) *Given any normal extension L of $\mathbb{Q}$ with $L \subseteq \mathbb{R}$ and $[L : G] = 2^n$, any point p with co-ordinates in L is constructible from S_0.*

Proof. To prove (1), by the Tower Lemma, it is enough to prove that given a construction chain $S_0 \subset S_1 \subset \cdots \subset S_n$, all points $p \in S_i \backslash S_{i-1}$ have coordinates (x, y) which are solutions of quadratic equations with coefficients in K_S. This is true since

- computing the intersection point of two lines is a linear problem;
- computing the intersection points of a line and a circle is a quadratic problem;
- computing the intersection points of two circles is a quadratic problem.

For (2), argue by induction on n. If $n = 0$, points with $\mathbb{Q}$-coordinates are constructible. Since $[L_n : L_{n-1}] = 2$, any $\alpha \in L_n$ solves a quadratic polynomial over L_{n-1}, Using the constructions above, we can solve a quadratic geometrically.

Finally (3) follows from (2), together with the following group theoretic

Claim. Given a finite group G with 2^n elements, there is a chain of subgroups $G_0 = \{e\} < G_1 < \cdots < G_n = G$ such that $[G_i : G_{i-1}] = 2$.

Assuming the Claim, note that $L/\mathbb{Q}$ is normal and $\operatorname{char}\mathbb{Q} = 0$, so the extension $L/\mathbb{Q}$ is Galois. Let $G = \Gamma(L:\mathbb{Q})$ be the Galois group, with $\#(G) = 2^n$. Given the claim, take $L_i = L^{G_{n-i}}$ and apply (2). □

Corollary. (1) *It is not possible to divide a general angle into three equal parts using a lines and circles construction.*

(2) *(Gauss) It is possible to construct a regular 17-gon.*

Proof.

(1) It is sufficient to show a single angle which we cannot divide. Let $\alpha = \frac{\pi}{3}$, and suppose that $\frac{\alpha}{3} = \frac{\pi}{9}$ is constructible. Using the multiple angle formula

$$\cos\theta = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3},$$

for $\alpha = 2\cos\frac{\pi}{9}$ we get

$$\alpha^3 - 3\alpha - 1 = 0.$$

A geometric construction of $\frac{\pi}{9}$ would be equivalent to a geometric construction of $\cos\frac{\pi}{9}$, which is itself equivalent to a geometric construction of α. On the other hand, the polynomial $p(x) = x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\alpha):\mathbb{Q})] = 3$. Hence by the Tower law, α cannot be an element of any extension of $\mathbb{Q}$ of degree 2^n.

(2) Clearly constructing a 17-gon is equivalent to constructing $\cos\frac{2\pi}{17}$. Let $\xi = \exp(\frac{2\pi i}{17})$, then as $17 = 4^2 + 1$, we get the tower

$$\begin{array}{ccc} \{e\} & & \mathbb{Q}(\xi) \\ | & & | \\ C_2 & \mathbb{Q}(\xi+\xi^{-1}) = \mathbb{Q}\left(\cos\frac{2\pi}{17}\right) & \\ | & & | \\ C_{16} & & \mathbb{Q}. \end{array}$$

$\mathbb{Q}(\cos\frac{2\pi}{17})$ is Galois over $\mathbb{Q}$ with Galois group $C_{16}/C_2 \cong C_8$. So by our theorem, $\cos\frac{2\pi}{17}$ is constructible.

□

9.3. **Algebraic Closure.**

Definition. Given a field K, an *algebraic closure* $\bar{K}$ of K is a field extension such that

(1) the extension $\bar{K}/K$ is algebraic;
(2) the field $\bar{K}$ has no nontrivial finite extensions.

In particular, (2) implies that any polynomial $f(x) \in \bar{K}[x]$ has a root in $\bar{K}$. Such extensions are 'rather big'.

Examples. (1) Consider the field of all algebraic numbers

$$\mathbb{A} = \{z \in \mathbb{C} : z \text{ satisfies some polynomial equation over } \mathbb{Q}\}$$

from Problem Sheet 1. Clearly this is algebraic over $\mathbb{Q}$. Let $K/\mathbb{A}$ be a finite extension, and let $\alpha \in K$ have minimal polynomial $m \in \mathbb{A}[x]$ with coefficients $a_1, \ldots, a_n \in \mathbb{A}$. Then $\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}$ is finite, and α is an element of a finite extension of $\mathbb{Q}(a_1, \ldots, a_n)$. Thus $\mathbb{Q}(\alpha)/\mathbb{Q}$ is finite, so $\alpha \in \mathbb{A}$. So $K = \mathbb{A}$. Hence

$$\bar{\mathbb{Q}} = \mathbb{A}.$$

(2) By the Fundamental Theorem of Algebra,
$$\bar{\mathbb{R}} = \mathbb{C}.$$
(3) We sketch the construction of $\bar{\mathbb{F}_p}$. This is the union $\bigcup_n \mathbb{F}_{p^n}$, remembering that we had inclusions $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ if $n \mid m$. So there will always be a place where we can compare elements in these separate fields. The union is really a limit construction.

Finally, given a field K, a sensible question is to ask for a description of the Galois group $\Gamma(\bar{K} : K)$. Since $\bar{K}$ is usually built as a union or limit, so is the group $\Gamma(\bar{K} : K)$. In increasing order of difficulty and interest, we have:

(1) $\Gamma(\mathbb{C} : \mathbb{R}) = C_2$, generated by complex conjugation $z \mapsto \bar{z}$.
(2) Corresponding to the construction of $\bar{\mathbb{F}_p}$ as a union (limit), the Galois group $\Gamma(\bar{\mathbb{F}_p} : \mathbb{F}_p)$ is a kind of limit of the finite groups $\mathbb{Z}_n$ generated by Frobenius, acting at each level on $\mathbb{F}_{p^n}/\mathbb{F}_p$.
(3) The group $\Gamma(\bar{\mathbb{Q}} : \mathbb{Q})$ is one of the least understood and mysterious objects in mathematics!

THE END