THEOFILOS TSANTILAS

Finite and infinite Galois Theory

of fields

Version: December 29, 2025
Athens, Greece

Prologue

These notes were a part of my master thesis and since Galois Theory is one of my favorite subjects, I have decided to undertake the tedious task of correcting the numerous errors and somewhat expanding them, as an opportunity to solidify my knowledge.

It is ***not*** my intention to attempt to write a book or even a set of formal notes on Galois Theory. The intended style is an informal set of notes (despite what the look may suggests; I am just **so** into LaTeX) written by a ***student***, covering some topics I find interesting while most of the time completely missing the big picture!

I would be grateful for any feedback.*

Theofilos Tsantilas
Athens, December 29, 2025**

* Feedback can be sent using any of the ways listed in the "Contact" section of my personal page: `http://users.ntua.gr/tsantilas` or `https://teotsan.github.io`

**This footnote will be here to warn you that this version *still contains many errors*. This is not speculative, I have spotted a great amount of errors and I am sure there will be more.

Contents

Short Historical Introduction

FOR MANY CENTURIES, one of the central problems in Mathematics was finding the solutions of polynomial equations

$$f(x) = a_n x^n + \ldots + a_1 x + a_0 = 0 \quad (n \in \mathbb{N})^*.$$

Formulas that gave the solutions of such equations when the *degree* of the polynomial f, denoted $\deg f$, is 1 or 2 were found as early as the times of ancient Babylonians, while analogous formulas for the cases $\deg f = 3$ and 4 were discovered by the 16th century.

All of these formulas had a common characteristic. They involved the four basic operations $+, -, \times, \div$ along with the extraction of roots applied on the coefficients of the polynomial; for example the roots of the general polynomial equation of degree 2,

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

are given by the well known formulas

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{and} \quad \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

In other words, it was realized that *all* polynomial equations of degree $\leqslant 4$ can be *solved by radicals*.

It was therefore natural to search for similar formulas when $\deg f \geqslant 5$ as well. As Mathematics advanced, mathematicians realized that such formulas most likely did not exist and many attempted proving it. It was Niels Henrik Abel (1802-1829) who eventually gave a satisfactory proof of this fact for the general equation of degree $\deg f = 5$. But are there any special quintic equations that *can* be solved by radicals? What about equations of higher degrees? Immediately, the focus turned to

* Although not historically accurate, for simplicity we may assume at this point that $a_i \in \mathbb{C}\ \forall i = 1, \ldots, n$.

find ways of deciding *when* an equation can be solved by radicals. The final answer was given by Évariste Galois.

Galois' idea was to derive information about the polynomial by studying the *permutations* of its roots. Although many mathematicians before Galois had linked the polynomials' behavior to such permutations, it was Galois who recognized that these permutations form a *group* under composition and used this extra structure to answer questions about the polynomial. He showed how information about a polynomial f could be derived from the group G of permutations of its roots and, as an application, gave an answer to one of the biggest problems of his time: *a polynomial equation can solved by radicals if and only if the group G is solvable* (using modern terminology).

His theory was proven to be most fruitful and over the years evolved. It required the work of many mathematicians, an adequate development of Group Theory and Field Theory (which was done in the 19^{th} century) and a world ready for such an abstract theory in order for Galois Theory to be formulated and established as we know it.

The ideas of modern Galois Theory, whose father is considered to be Emil Artin (1898-1962), trace back to Heinrich Martin Weber (1842-1913) and Julius Wilhelm Richard Dedekind (1831-1916). But it was Artin who managed to formulate the theory in the language of fields and field extensions independently of its main application, i.e. the solvability of polynomial equations by radicals.

Thus modern Galois Theory surpasses the scope of the original theory. Instead of studying polynomials using permutations of their roots, the focus is turned on how to use *automorphisms* to derive information about *field extensions*. In this setting, the original question about the solvability of a polynomial equation is translated into a question about a *specific field extension* (the splitting field of the polynomial over the field where its coefficients lie).

A natural question arises at this early stage: *Why are field extensions so important?* On the one hand, as it turned out, great mathematical problems of the antiquity such as the *solvability of polynomial equations* and the *impossibility of geometric constructions by ruler and compass* can be solved by translating them into questions about field extensions and using the tools of field extensions to solve the latter. On the other, field extensions are important on their own in the Theory of Fields.

Along with fields, we are also interested in field homomorphisms.

Suppose that

$$\phi : k \to E$$

is a field homomorphism. Since $\ker \phi \lhd k$ is an ideal,*

$$\ker \phi = \{0\} \text{ or } k.$$

Therefore either $\phi = 0$ or ϕ is a monomorphism, i.e. $k \leqslant E$ is a field extension. That is, field extensions are the (non zero) *morphisms* in the *category of fields*.

* The only ideals of a field k are 0 and k because any non zero ideal I contains a unit, hence $I = k$.

Chapter **1**

Field Extensions

1.1 Field extensions and their degrees

An extension of a field k is just a bigger field E containing k or, more generally, containing an *isomorphic copy* of k.

> **Definition.** Let k be a field. A **field extension** of k is a field E together with a field monomorphism $i : k \to E$. We refer to the field k as the **base field** and to E as the **extending field**.

Following the customary identification of k with its isomorphic image $i(k)$, we may think of k as a *subfield* of E. This is why we will usually denote a field extension as $k \leqslant E$ or E/k, suppressing the monomorphism i from the notation.

When we are given a mathematical structure to study, e.g. sets, groups, fields, algebras, topological spaces, smooth manifolds etc., we do not confine ourselves to the study of the structure alone. *Substructures* and *structure preserving maps* give us additional information about the mathematical object of interest.

In the theory of field extensions, a **subextension** or **intermediate field** of an extension $k \leqslant E$ is a field L such that $k \leqslant L$ and $L \leqslant E$. We use the notation $k \leqslant L \leqslant E$ to denote a subextension L of $k \leqslant E$.

More often than not, we encounter multiple fields extending one another, i.e. multiple subextensions. For simplicity, we shall use the shorter notation

$$k \leqslant L_1 \leqslant L_2 \leqslant \ldots \leqslant L_n \leqslant E$$

and refer to such extensions as **towers of fields**.

Examples 1.1.1. 1. $\mathbb{Q} \leqslant \mathbb{R}$, $\mathbb{R} \leqslant \mathbb{C}$ and $\mathbb{Q} \leqslant \mathbb{C}$ are all field extensions.
$\mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$ is a tower of fields.

2. All fields can be considered extensions over their prime fields, i.e. over $\mathbb{Q}$ if their characteristic is 0 or over $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ if their characteristic is $q > 0$.
3. Let k be a field, $x_1, \dots, x_n$ be indeterminates and

$$k(x_1, \dots, x_n) = \left\{ \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} : f, g \in k[x_1, \dots, x_n],\ g(x_1, \dots, x_n) \neq 0 \right\}.$$

the field of polynomial functions over k in these indeterminates. Then $k \leqslant k(x_1, \dots, x_n)$ is a field extension since k can be viewed as *the subfield of constant polynomials* through the monomorphism

$$i : k \to k(x_1, \dots, x_n) : a \mapsto f_a(x) = \frac{a + 0x_1 + \dots + 0x_n}{1 + 0x_1 + \dots + 0x_n} \ \forall a \in k.$$ ◀

Given a field extension $k \leqslant E$, the extending field E has the additional (rather trivial) structure of a k-vector space with external multiplication given by the multiplication of E restricted to k, i.e.

$$k \times E \to E.$$

This vector space structure is fundamental to Field Theory; it is one of the main tools we use to study the extension $k \leqslant E$.

Definition. The **degree** $[E : k]$ of the field extension $k \leqslant E$ is the dimension of E as an k-vector space, i.e. $[E : k] := \dim_k E$. The extension is called **finite** if $[E : k] < \infty$ and **infinite** otherwise.

Examples 1.1.2. 1. Consider the tower of fields $\mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$. It is immediate that both $[\mathbb{R} : \mathbb{Q}]$ and $[\mathbb{C} : \mathbb{Q}]$ are infinite because $\mathbb{Q}$ is countable while $\mathbb{R}$ and $\mathbb{C}$ are not.*

2. On the other hand, $[\mathbb{C} : \mathbb{R}] = 2$; every complex number is an $\mathbb{R}$-linear combination of the $\mathbb{R}$-linearly independent set $\{1, i\}$.
3. The extension $k \leqslant k(x)$ has infinite degree. Every polynomial is a finite k-linear combination of the k-linearly independent set $\{1, x, x^2, x^3, \dots\}$. ◀

* Using a famous argument of Georg Ferdinand Ludwig Philipp Cantor (1845-1918), a vector space with a countable basis over a countable field is necessarily countable.

Example 1.1.3. Let's see a simple example of how we can use the vector space structure of an extension to derive information about the extension itself. We will show that $[E : k] = 1$ if and only if $E = k$.

If $E = k$ then $\{1_k\}$ is an k-basis for E and therefore $[E : k] = 1$. On the other hand, if $[E : k] = 1$ and, say, $\{u\}$ is an k-basis for E then $1_E = ru$ for some $r \in k$ and so $u = r^{-1}1_E = r^{-1} \in k$. Now $u \in k$ implies at once that $E = k$. ◂

Proposition 1.1.4. *Let $k \leqslant L \leqslant E$ be a tower of fields. Then*

$$[E : k] = [E : L][L : k]$$

Proof. Let $\mathcal{B} = \{a_i : i \in I\}$ be a k-basis for L and let $\mathcal{B}' = \{b_j : j \in J\}$ be an L-basis for E; the set

$$\mathcal{B}'' = \{a_i b_j : i \in I, j \in J\}$$

is a k-basis for E. We can see that $\mathcal{B}''$ spans E using the distributive law and that any k-linear relation of its elements implies an L-linear relation among the elements of $\mathcal{B}'$, which is absurd. ◇

Using induction on $n \in \mathbb{N}$ we can prove

Corollary 1.1.5. *If $k \leqslant L_1 \leqslant L_2 \leqslant \ldots \leqslant L_n \leqslant E$ is a tower of fields then*

$$[E : k] = [E : L_n] \ldots [L_2 : L_1][L_1 : k].$$

Corollary 1.1.6. *If $k \leqslant L \leqslant E$ is a tower of fields, then $k \leqslant E$ is finite if and only if both $k \leqslant L$ and $L \leqslant E$ are finite.*

1.2 Constructing field extensions I: Polynomials

We turn to more examples of field extensions and, in particular, a way of constructing field extensions using polynomials.

An important class of field extensions arise when trying to solve polynomial equations. For example, $x^2 + 1 = 0$ cannot be solved in the field $\mathbb{R}$ of real numbers but has two solutions in the extension $\mathbb{C}$.

More generally, given a field k and some *irreducible* polynomial $p(x) \in k[x]$ of degree $\deg p \geqslant 2$ (so that not all roots of p are in k), one may wonder whether there is some extension E of k that contains a root of $p(x)$.

We can *construct* such an E. The motivating idea is simple: consider the ring in which $p(x)$ lives and *force* $p(x)$ to be 0 by default. So take the polynomial ring $k[x]$, its prime* ideal $I := \langle p(x) \rangle$ and form the quotient ring

$$E := k[x]/\langle p(x) \rangle = k[x]/I.$$

E is a field that extends k. Since $k[x]$ is a P.I.D., the ideal I is maximal** and therefore E is a field.† To see that E extends k, restrict the natural projection map $\pi : k[x] \to k[x]/I$ to k. The restriction $\pi|_k$ is a ring homomorphism with $\pi|_k(1) = 1$ and $\ker \pi|_k = \{0\}$ hence a field monomorphism.

To formally verify *there is a root of $p(x)$* (or of $\pi|_k\big(p(x)\big)$ to be more precise) *in E*, take the element $\tilde{x} = x + I \in k[x]/I$ and verify that

$$p(\tilde{x}) = p(x) + I = I = 0 \in E.$$

It would be of benefit to us if we could have an explicit description of the elements of E. Using the extra structure E has as an k-vector space, we obtain a useful characterization of its elements as follows. The set

$$\mathcal{B} = \{1, \tilde{x}, \tilde{x}^2, \ldots, \tilde{x}^{\deg p - 1}\} = \{1, x + I, x^2 + I, \ldots, x^{\deg p - 1} + I\}$$

is a basis of E over k.

$\mathcal{B}$ spans E. Indeed, $k[x]$ is an Euclidean‡ domain with Euclidean function the usual degree function $\deg : k[x] \to \mathbb{N} : \ f \mapsto \deg f$. Using Euclid's algorithm, for every $g \in k[x]$ there are unique $b, r \in k[x]$ such that

$$g = bp + r, \quad \deg r < \deg p.$$

Therefore, $g + I = (bp + r) + I \overset{p=0}{=} r + I \in \langle \mathcal{B} \rangle$ since $\deg r < \deg p$.

Moreover, *$\mathcal{B}$ is k-linearly independent*. Any k-linear relation of the form

$$a_{\deg p - 1}(x^{\deg p - 1} + I) + \ldots + a_1(x + I) + a_0(1 + I) = 0 + I \in E$$

* A principal ideal of $k[x]$ that is generated by an irreducible element is prime.

** Prime ideals are maximal in P.I.D.s.

† If I is an ideal of a commutative ring R, then *R/I is a field iff I is maximal.*

‡ Euclid of Alexandria ($\sim$ 300 B.C.).

among the elements of $\mathcal{B}$ yields a polynomial

$$w(x) = a_{\deg p-1}x^{\deg p-1} + \ldots + a_1 x + a_0 \in k[x]$$

of degree $< \deg p$ which is equal to 0 in $k[x]/I$ or, equivalently, a polynomial of degree $< \deg p$ which is divided by p which is absurd.

Therefore,

$$[E : k] = |\mathcal{B}| = \deg p \tag{1.1}$$

and

$$\begin{aligned} E = k[x]/I &= \{b_0 + b_1\tilde{x} + b_2\tilde{x}^2 + \ldots + b_{\deg p-1}\tilde{x}^{\deg p-1} : \ b_i \in k\} \\ &= \{b_0 + b_1 x + b_2 x^2 + \ldots + b_{\deg p-1}x^{\deg p-1} + I : \ b_i \in k\}. \end{aligned}$$

Example 1.2.1. Take the field $\mathbb{R}$ and the irreducible polynomial $p(x) = x^2 + 1 \in \mathbb{R}[x]$ of degree $\deg p = 2$.*

By the example above, $E = \mathbb{R}[x]/\langle x^2 + 1\rangle$ is a field extension of $\mathbb{R}$ which contains a root of $p(x)$. Moreover, E is spanned by

$$\mathcal{B} = \{1, x + \langle x^2 + 1\rangle\}$$

and, as a result, $[E : \mathbb{R}] = 2$ and

$$E = \{a + b(x + I) : a, b \in \mathbb{R}\}.$$

If we decide to just change the notation and set $i := x + I \in E$ (observe that $x + I$ is the root of $p(x)$ in E) then

$$E = \{a + b(x + I) : a, b \in \mathbb{R}\} \cong \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}.$$

The formal way to do this is by constructing the field isomorphism

$$\sigma : E \to \mathbb{C} : a + bx + I \mapsto a + bi.$$

Thus we have constructed $\mathbb{C}$ in a very elegant, algebraic way. ◂

* The polynomial $x^2 + 1$ is irreducible since it has degree 2 and no real roots.

1.3 Isomorphic extensions

We now make a short pause from our examples to define a crucial notion.

Even in our first examples we came across two very different yet isomorphic fields that both extend $\mathbb{R}$, i.e. $\mathbb{C}$ and $E = \mathbb{R}[x]/\langle x^2+1\rangle$. Therefore it is only natural to consider both extensions $\mathbb{R} \leqslant E$ and $\mathbb{R} \leqslant \mathbb{C}$ to be the same from a field-theoretic point of view. This notion of isomorphic field extensions is the one we want to define.

Definition. A **morphism** between two abstract field extensions $i_1 : k_1 \to E_1$ and $i_2 : k_2 \to E_2$ is a pair of maps $\sigma : E_1 \to E_2$ and $\tau : k_1 \to k_2$ such that the following diagram commutes, i.e. $\sigma \circ i_1 = i_1 \circ \tau$.

$$\begin{array}{ccc} E_1 & \xrightarrow{\sigma} & E_2 \\ {\scriptstyle i_1}\uparrow & & \uparrow{\scriptstyle i_2} \\ k_1 & \xrightarrow{\tau} & k_2 \end{array}$$

The field extensions are called **isomorphic** if the maps σ and τ are *field isomorphisms*.

What this definition says is that an isomorphism of field extensions must *preserve the structure of the extensions* in question, i.e. *the base fields*, *the extending fields* and *the way they are related* (the monomorphisms).

With the identification of k_j with its isomorphic image $i_j(k_j) \leqslant E_j$ (in which case $i_j = \mathrm{id}_{E_j}|_{k_j}$), $j = 1, 2$, the commutativity of the above diagram gives

$$\sigma(i_1(x)) = i_2\big(\tau(x)\big) \Leftrightarrow \sigma(x) = \tau(x)\ \forall x \in k_1.$$

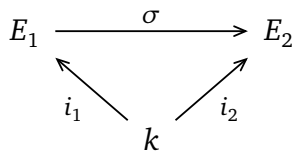
Hence we get the following *equivalent* definition.

Definition. Two field extensions $k_1 \leqslant E_1$ and $k_2 \leqslant E_2$ are **isomorphic** if there is a field isomorphism $\tau : k_1 \to k_2$ that can be *extended* to an isomorphism $\sigma : E_1 \to E_2$.

In many instances, such as Ex. 1.2.1, we will encounter the simpler case when the extensions are over the same base field.

Definition. Two abstract field extensions $i_1 : k \to E_1$ and $i_2 : k \to E_2$ *over the same field* are called **isomorphic** if there is a *field isomorphism*

$\sigma : E_1 \to E_2$ so that the following diagram commutes, i.e. $\sigma \circ i_1 = i_2$.



Although we could simply use the first definition and take $\tau = \mathrm{id}_k$ when two extensions are over the same field, the importance of this special case dictates to formulate it separately.

In the case where we regard k as a subfield of both E_1 and E_2, the commutativity of the above diagram gives

$$\sigma(i_1(x)) = i_2(x) \iff \sigma(x) = x \ \forall x \in k.$$

That is, σ is a field isomorphism $E_1 \to E_2$ that *fixes k pointwise*. In this case we say that σ is a k-**isomorphism** from E_1 to E_2 (or in the case where $E_1 = E_2 = E$, a k-**automorphism** of E) and we can restate the previous definition as

Definition. Two field extensions $k \leqslant E_1$ and $k \leqslant E_2$ *over the same field* are called **isomorphic** if there is an *k-isomorphism* $\sigma : E_1 \to E_2$.

Lemma 1.3.1. *Field extension isomorphism is an equivalence relation.*

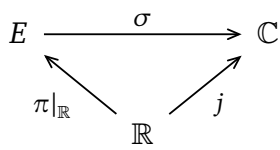
Example 1.3.2. The extensions $\mathbb{R} \leqslant \mathbb{C}$ and $\mathbb{R} \leqslant E = \mathbb{R}[x]/\langle x^2 + 1\rangle$ are isomorphic. If we define

$$\sigma : E \to \mathbb{C} : a + bx + I \mapsto a + bi$$

as before, and

$$j : \mathbb{R} \to \mathbb{C} : r \mapsto r + 0i,$$

to be the usual inclusion $\mathbb{R} \hookrightarrow \mathbb{C}$ then it is easily seen that the diagram



commutes. Indeed,

$$\sigma(\pi|_{\mathbb{R}}(r)) = \sigma(r + I) = \sigma(r + 0(x + I)) = r + 0i = j(r) \ \forall r \in \mathbb{R}.$$

Therefore, the extensions are isomorphic. ◂

Field extension isomorphisms *over the same field* preserve all the information of a field extension including the structure of the extending fields as vector spaces over the base field.

Proposition 1.3.3. *If E_1, E_2 are fields extending a field k and $\sigma : E_1 \to E_2$ is an k-isomorphism then σ is a bijective k-linear transformation.*

Proof. The bijection is immediate; the linearity is clear from the corresponding commutative diagram. ◇

Corollary 1.3.4. *If $k \leqslant E_1$ and $k \leqslant E_2$ are isomorphic field extensions over the same field then $[E_1 : k] = [E_2 : k]$.*

Lastly, before we continue with our examples we introduce the concept of an automorphism of a field extension which will be needed later.

Definition. Let $k \leqslant E$ be a field extension. An **automorphism** of $k \leqslant E$ is an isomorphism from $k \leqslant E$ to itself, i.e. a k-automorphism of E. The set of all k-automorphisms of E is denoted by $\mathrm{Aut}(E/k)$.

Using elementary Group Theory, it is immediate that

Lemma 1.3.5. *If $k \leqslant E$ be a field extension then $\mathrm{Aut}(E/k)$ is a subgroup of $\mathrm{Aut}(E)$.*

1.4 Constructing field extensions II: Finitely generated extensions

We continue with more examples and ways of constructing field extensions.

Given a fixed field extension $k \leqslant E$ and a subset X of E, the intersection of all subfields L of E that contain $X \cup k$ is non empty (E is such a field), and is a subfield of E.* It is the smallest extension of k with these properties and is denoted by $k(X)$;

$$k(X) := \bigcap_{X \cup k \subseteq L \leqslant E} L. \tag{1.2}$$

* The intersection of any family of subfields of E is again a subfield of E.

The elements of X are called the **generators** of the extension. A field extension $k \leqslant E$ is called **finitely generated** over k if there is some *finite* subset $X \subseteq E$ such that $E = k(X)$. If there exists a single element $a \in E$ such that $E = k(a)$, then the extension is called **simple**. Using (1.2) we can see that

$$k(a,b) = \bigcap_{\{a,b\}\cup k \subseteq L \leqslant E} L = \bigcap_{\{b\}\cup k(a) \subseteq L \leqslant E} L = \big[k(a)\big](b) \tag{1.3}$$

and by induction that $k(a_1,\dots,a_n) = k(a_1,\dots,a_{n-1})(a_n)$; this suggests that simple extensions act as building blocks for finitely generated extensions. Therefore, if we want to understand the structure of finitely generated extensions, we should first understand the structure of simple extensions.

Finitely generated extensions are the core of *finite* Galois Theory. As we shall see, every finite extension is finitely generated.

Example 1.4.1. We can take the extension $\mathbb{R} \leqslant \mathbb{C}$ and the element $i \in \mathbb{C}$. Then $\mathbb{R}(i)$ is a simple extension. It is the smallest field in $\mathbb{C}$ containing both $\mathbb{R}$ and i. ◂

Example 1.4.2. To the same direction we can also take the extension $\mathbb{Q} \leqslant \mathbb{R}$ and the elements $\pi, \sqrt{2} \in \mathbb{R}$. Then $\mathbb{Q}(\sqrt{2},\pi)$ is the smallest field $\subseteq \mathbb{R}$ that contains $\mathbb{Q}$ as well as π and $\sqrt{2}$. ◂

Example 1.4.3. We will later see (Prop. 1.6.9) that every extension of the form $k \leqslant k[x]/\langle p(x)\rangle$ constructed as in Ex. 1.2 is isomorphic to a simple extension, generated by an element that satisfies some extra properties. So finitely generated extensions generalize the construction of Ex. 1.2. ◂

So far we have no information about the structure of finitely generated extensions.

Proposition 1.4.4. *Let $k \leqslant E$ be a field extension and $a \in E$. Then*

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

Proof. Let L_0 be the right hand side of the above equality. L_0 is a subextension of $k \leqslant E$ such that $a \in L_0$. Therefore

$$k(a) = \bigcap_{\{a\} \cup k \subseteq L \leqslant E} L \subseteq L_0.$$

On the other hand, L_0 is obviously contained in every field L that contains both k and a. Hence

$$L_0 \subseteq \bigcap_{\{a\} \cup k \subseteq L \leqslant E} L = k(a)$$

The two inclusions imply the required equality. ◇

Corollary 1.4.5. *Let $k \leqslant E$ be a field extension and $a_1, \dots, a_n \in E$. Then*

$$k(a_1, \dots, a_n) = \left\{ \frac{f(a_1, \dots, a_n)}{g(a_1, \dots, a_n)} : f, g \in k[x_1, \dots, x_n],\ g(a_1, \dots, a_n) \neq 0 \right\}.$$

Example 1.4.6. Now we know that

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

and

$$\mathbb{Q}(\sqrt{2}, \pi) = \left\{ \frac{f(\sqrt{2}, \pi)}{g(\sqrt{2}, \pi)} : f, g \in \mathbb{Q}[x_1, x_2],\ g(\sqrt{2}, \pi) \neq 0 \right\}.$$

But these descriptions do not depict accurately the structure of the extensions. In particular, the form of the elements might not be as complex as described in the previous propositions as the generator may satisfy some polynomial equation. For example, the element

$$\frac{i^{15} + 3i^6 - 2i + 1}{i - 1} \in \mathbb{R}(i)$$

can be simplified to

$$\begin{aligned} \frac{i^{15} + 3i^6 - 2i + 1}{i - 1} &= (i^{15} + 3i^6 - 2i + 1)(i - 1)^{-1} \\ &= (-3i - 2)\left(-\frac{1}{2}i - \frac{1}{2}\right) = \frac{5}{2}i - \frac{1}{2} \in \mathbb{R}(i). \end{aligned}$$

After studying simple extensions in more depth, we will be able to get better descriptions of finitely generated extensions such as the above. ◂

1.5 Algebraic extensions I

As we said, the understanding of finitely generated extensions requires a very good grasp of their building blocks, i.e. the simple extensions. In the general case, we can classify all simple extensions $k \leqslant k(a)$ up to isomorphism; their structure depends on whether the generator a is algebraic or not.

Definition. Let $k \leqslant E$ be a field extension and $a \in E$. The element $a \in E$ is said to be **algebraic over** k if there exists some $f(x) \in k[x]$ such that $f(a) = 0$. An extension whose elements are all algebraic is called an **algebraic extension**.

Example 1.5.1. The element $i \in \mathbb{C}$ is the root of $x^2 + 1 \in \mathbb{R}[x]$ hence algebraic over $\mathbb{R}$. In fact there is no point to commit ourselves to i. Any complex number $z = a + bi$ is the root of $x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$ hence algebraic over $\mathbb{R}$. So $\mathbb{R} \leqslant \mathbb{C}$ is an algebraic extension. ◂

Definition. If the element $a \in E$ is not algebraic over k then it is said to be **transcendental over** k. An extension with transcendental elements is called **transcendental extension**.

Example 1.5.2. The extension $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt{2}, \pi)$ is transcendental since π is transcendental over $\mathbb{Q}$.* ◂

Example 1.5.3. An important example of a transcendental extension is $k \leqslant k(x)$, where x is an indeterminate. As we shall see, this is the only simple transcendental extension of k up to isomorphism. ◂

1.6 Classifying simple extensions

Let $k \leqslant E = k(a)$ be a simple field extension ($a \in E$) and

$$e_a : k[x] \to k[a] : f(x) \mapsto f(a)$$

be the evaluation homomorphism. Note that e_a is clearly *onto*.

* For a proof of the transcendence of π see [**25**].

If $a \in E$ is transcendental, then there is no $g(x) \in k[x]$ such that $g(a) = 0$; in other words, $\ker e_a = \{0\}$. By the 1st Isomorphism Theorem we have a ring isomorphism

$$k[x]/\ker e_a = k[x] \cong \operatorname{Im} e_a = k[a].$$

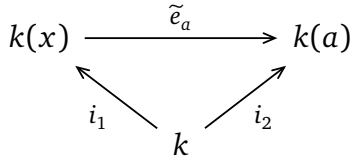
Since $k(x)$ and $k(a)$ are the fields of quotients (which are unique up to isomorphism) of $k[x]$ and $k[a]$ respectively, we get a *field isomorphism*

$$\widetilde{e}_a : k(x) \xrightarrow{\cong} k(a) : \frac{f(x)}{g(x)} \mapsto \frac{f(a)}{g(a)}.$$

This field isomorphism together with the two inclusions

$$i_1 : k \to k(x) : z \mapsto \frac{f(x)}{g(x)} = \frac{z + 0x + 0x^2 + \ldots}{1 + 0x + 0x^2 + \ldots} = \frac{z}{1} \in k(x)$$
$$i_2 : k \to k(a) : z \mapsto \frac{f(a)}{g(a)} = \frac{z + 0a + 0a^2 + \ldots}{1 + 0a + 0a^2 + \ldots} = \frac{z}{1} \in k(a)$$

make the corresponding diagram commute.



Thus we have proven the following.

Proposition 1.6.1. *Let k be a field. $k \leqslant k(x)$, where x is an indeterminate, is the only simple transcendental extension of k up to isomorphism.*

If, on the other hand, $a \in E$ is algebraic over k then

$$\{0\} \neq \ker e_a \lhd k[x].$$

Hence $\ker e_a$ is generated by some non-zero element.*

Among all polynomials f that have a as a zero (i.e. $f \in \ker e_a$), there exist some with minimum degrees (by the well-ordering principle). Of all

* $k[x]$ is a P.I.D.

these we can choose a *monic* one.* This monic polynomial, denoted by $m(a,k)(x)$, such that $m(a,k)(a)=0$ and whose degree $\deg m(a,k)$ is the smallest among all the polynomials that have a as root, is *unique*; if not, any other such polynomial $w(x)$ would result in a non-zero polynomial $m(a,k)-w$ with a as a root and degree less that $\deg m$ (because both m and w are monic) - a contradiction.

Definition. This polynomial $m(a,k)$ is called the **minimal polynomial** of a over k and it obviously depends not only on a but on k as well.

Proposition 1.6.2. *With the above notation, the minimal polynomial $m=m(a,k)\in k[x]$*

1. *is irreducible*
2. *divides every polynomial $g(x)\in k[x]$ such that $g(a)=0$.*

Proof. 1. If not, then $m(x)=f_1(x)f_2(x)$ with $\deg f_1, \deg f_2 < \deg m$. But then $m(a)=f_1(a)f_2(a)=0$ hence either $f_1(a)=0$ or $f_2(a)=0$ which contradicts the minimality of $\deg m$.

2. By Euclid's Algorithm (and the minimality of $\deg m$), there exist unique $q,r\in k[x]$ such that

$$g(x)=q(x)m(x)+r(x),\ \deg r<\deg m.$$

If $r\neq 0$ then $g(a)=q(a)m(a)+r(a)\Rightarrow r(a)=0$ which again contradicts the minimality of $\deg m$. Therefore $r=0$ and $m|g$. ◇

Corollary 1.6.3. *With the above notation,* $\ker e_a=\langle m(a,k)\rangle$.

Corollary 1.6.4. *Let $k\leqslant E$ be a field extension, $a\in E$ and $m(x)\in k[x]$ a monic polynomial such that $m(a)=0$. Then $m=m(a,k)$ if and only if m is irreducible.*

Corollary 1.6.5. *Let $k\leqslant L\leqslant E$ be a tower of fields and $a\in E$. Then $m(a,L)$ divides $m(a,k)$. In particular* $\deg m(a,L)\leqslant \deg m(a,k)$.

Example 1.6.6. $m(i,\mathbb{R})=m(i,\mathbb{Q})=x^2+1$. ◂

* Take one with minimum degree and divide it by its leading coefficient.

Example 1.6.7. $m(\sqrt{2},\mathbb{Q}) = x^2 - 2 = m\big(\sqrt{2},\mathbb{Q}(\pi)\big)$. ◂

Returning to the extension $k \leqslant k(a)$. The evaluation homomorphism e_a is a well defined ring epimorphism with kernel

$$\ker e'_a = \langle m(a,k)\rangle \equiv \langle m\rangle.$$

The 1st Isomorphism Theorem for Rings now gives a ring isomorphism

$$\widetilde{e}'_a : k[x]/\langle m\rangle \cong k[a] : f(x) + \langle m\rangle \mapsto f(a). \tag{1.4}$$

However m is irreducible, so $\langle m\rangle$ is a maximal ideal of $k[x]$, hence $k[x]/\langle m\rangle$ is actually a field. That means that $k[a]$ is also a field, i.e. $k[a] = k(a)$, and therefore $k(a) \cong k[x]/\langle m(a,k)\rangle$.

By the previous discussion, if $k \leqslant k(a)$ is a simple extension with a algebraic over k then $k(a)$ is isomorphic to an extension of the form $k[x]/\langle p(x)\rangle$ where $p(x)$ is a monic irreducible polynomial in $k[x]$, namely $p = m(a,k)$.

We can show that the converse also holds. Given a field k and an irreducible, monic polynomial $p(x) \in k[x]$, the quotient $E = k[x]/\langle p(x)\rangle$ is a field extension of k that contains a root of p, namely the element $\widetilde{x} = x + I \in E$ (Ex. 1.2). Since p is monic and irreducible, $m(\widetilde{x},k) = p$ by Cor. 1.6.4. Therefore

$$k[x]/\langle p(x)\rangle = k[x]/\langle m(\widetilde{x},k)\rangle \cong k(\widetilde{x}).$$

The restriction that p be monic is actually superfluous. For if p is an irreducible polynomial in $k[x]$ with leading coefficient a then $q(x) = a^{-1}p(x) \in k[x]$ is *irreducible* and *monic* and

$$\langle q(x)\rangle = \langle p(x)\rangle.$$

Therefore

$$k[x]/\langle q(x)\rangle = k[x]/\langle p(x)\rangle.$$

Thus we have proven

Proposition 1.6.8. *Let k be a field. The simple field extensions of k which are generated by algebraic elements are exactly the fields $k[x]/\langle p(x)\rangle$ for $p(x) \in k[x]$ irreducible polynomials.*

Using now the data we have from Ex. 1.2 for the structure of extensions of the form $k[x]/\langle p(x)\rangle$, we can get a better description of the elements of simple extensions with algebraic generators than those provided by Prop. 1.4.4 and Cor. 1.4.5.

Corollary 1.6.9. *Let $k \leqslant E$ be a field extension and $a \in E$ an algebraic element over k. Then $[k(a) : k] = \deg m(a,k) = \deg m$ and*

$$k(a) = \{c_0 + c_1 a + c_2 a^2 + \ldots + c_{\deg m - 1} a^{\deg m - 1} : c_i \in k\}.$$

Proof. We already saw that $k(a) = k[a]$. Since $m(a) = 0$, we can replace every power of a in some $f(a) \in k[a]$ which is greater than $\deg m$ by powers $\leqslant \deg m$.

Moreover, the set $\mathscr{B} = \{1, a, \ldots, a^{\deg m - 1}\}$ is k-linearly independent. Otherwise, any k-linear relation among the elements of $\mathscr{B}$ yields a polynomial $g \in k[x]$ such that $g(a) = 0$ and $\deg g < \deg m$ which is absurd. ◇

Example 1.6.10. Consider the extension $\mathbb{R} \leqslant \mathbb{R}(i)$. The element $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$ with minimal polynomial $m(i, \mathbb{R}) = x^2 + 1$ of degree $\deg = 2$. Therefore $[\mathbb{R}(i) : \mathbb{R}] = 2$ and

$$\mathbb{R}(i) \cong \{a + bi : \ a, b \in \mathbb{R}\} = \mathbb{C}.$$ ◂

Example 1.6.11. Now to the extension $\mathbb{Q} \leqslant \mathbb{Q}(\pi, \sqrt{2})$. Although

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

using the structure of simple extensions

$$\mathbb{Q}(\pi, \sqrt{2}) = \big[\mathbb{Q}(\pi)\big](\sqrt{2}) \ \text{ and } \ \mathbb{Q}(\pi) = \{f(\pi) : f \in \mathbb{Q}(x)\}$$

(x being an indeterminate), we can again have a better description of the elements of the extension. Indeed, the element $\sqrt{2}$ is algebraic over $\mathbb{Q}(\pi)$ with minimal polynomial $m\big(\sqrt{2}, \mathbb{Q}(\pi)\big) = x^2 - 2$. Hence $[\mathbb{Q}(\pi, \sqrt{2}) : \mathbb{Q}(\pi)] = 2$ and

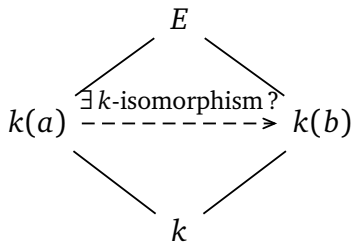
$$\mathbb{Q}(\pi, \sqrt{2}) = \big[\mathbb{Q}(\pi)\big](\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}(\pi)\}.$$ ◂

1.7 Introducing an extension theorem

Before continuing with the study of algebraic extensions, we take the opportunity the classification of simple extensions gives us to start

discussing *extension theorems*. Our aim is to classify simple extensions *up to isomorphism*.

Suppose we begin with a field extension $k \leqslant E$ and two elements $a, b \in E$. We can then form the simple extensions $k(a)$ and $k(b)$. By definition, these are isomorphic if there is an k-isomorphism between them.



If one element is algebraic and the other is transcendental then the extensions cannot be isomorphic (the one is an infinite dimensional vector space over k while the other has finite dimension; see Cor. 1.3.4).

If both elements are transcendental then the extensions are isomorphic by Prop. 1.6.1.

So the interesting case is when both a and b are algebraic over k.

Example 1.7.1. The extensions $\mathbb{R} \leqslant \mathbb{R}(i)$ and $\mathbb{R} \leqslant \mathbb{R}(-i)$ are isomorphic through complex conjugation map $z \mapsto \overline{z}$ (which is an $\mathbb{R}$-isomorphism).◀

Counterexample 1.7.2. The extensions $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2})$ are *not* isomorphic; they have different degrees. ◀

By Prop. 1.6.8,

$$k(a) \cong k[x]/\langle m(a,k)\rangle \quad \text{and} \quad k(b) \cong k[x]/\langle m(b,k)\rangle.$$

Therefore a sufficient condition would be $\langle m(a,k)\rangle = \langle m(b,k)\rangle$. Since both $m(a,k)$ and $m(b,k)$ are irreducible and monic, this condition is equivalent to $m(a,k) = m(b,k)$. Therefore if a, b are roots of the same irreducible polynomial then the extensions are isomorphic.

Proposition 1.7.3. *If $k \leqslant E$ is a field extension and $a, b \in E$ algebraic elements over k such that $m(a,k) = m(b,k)$ then the extensions $k \leqslant k(a)$ and $k \leqslant k(b)$ are isomorphic.*

Proof. The required k-isomorphism is the composition

$$k(a) \xrightarrow{\cong} k[x]/\langle m(a,k)\rangle = k[x]/\langle m(b,k)\rangle \xrightarrow{\cong} k(b).$$

The details are easy to fill. ◇

Let us examine the general case where we have two different extensions $k_1 \leqslant E_1$ and $k_2 \leqslant E_2$ over *isomorphic* base fields with, say, $\tau : k_1 \to k_2$ being the base field isomorphism.

Given $\alpha \in E_1$ and $\beta \in E_2$ we can form the extensions $k_1 \leqslant k_1(\alpha)$ and $k_2 \leqslant k_2(\beta)$. We would like to know if these extensions are isomorphic. Again the non-trivial case is when α and β are algebraic over their respective base fields. In this case, the extensions are isomorphic if we can *extend* the given isomorphism τ to an isomorphism σ between $k_1(\alpha)$ and $k_2(\beta)$.

$$\begin{array}{ccc} k_1(\alpha) & \overset{\exists\,\sigma\,?}{\dashrightarrow} & k_2(\beta) \\ | & & | \\ k_1 & \xrightarrow{\quad\tau\quad} & k_2 \end{array}$$

Before proceeding, recall that if $\tau : k_1 \to k_2$ is a field homomorphism then τ induces a ring homomorphism

$$\widetilde{\tau} : k_1[x] \to k_2[x] : \sum_{i=0}^{m} a_i x^i \mapsto \sum_{i=0}^{m} \tau(a_i) x^i$$

and if τ is bijective then so is $\widetilde{\tau}$. Since

$$k_1(\alpha) \cong k_1[x]/\langle m(\alpha,k_1)\rangle, \quad k_2(\beta) = k_2[x]/\langle m(\beta,k_2)\rangle$$

and $\widetilde{\tau} : k_1[x] \to k_2[x]$ is an isomorphism, a sufficient condition for the extensions to be isomorphic would be $\widetilde{\tau}\big(m(\alpha,k_1)\big) = m(\beta,k_2)$.

Indeed, if this is the case, then we can define

$$\sigma : k_1(\alpha) \to k_2(\beta) : f(\alpha) = \sum_{i=0}^{m} a_i \alpha^i \mapsto \big(\widetilde{\tau}(f)\big)(\beta) = \sum_{i=1}^{m} \tau(a_i)\beta^i.$$

This is a field isomorphism that makes the diagram

$$\begin{array}{ccc} k_1(\alpha) & \xrightarrow{\sigma} & k_2(\beta) \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j} \\ k_1 & \xrightarrow{\tau} & k_2 \end{array}$$

commute (here i and j are the canonical inclusions). Moreover $\sigma(\alpha) = \beta$ and $\sigma|_{k_1} = \tau$, that is, σ *extends* τ. Thus we have proven

Proposition 1.7.4 (Extension Theorem for simple extensions). *Suppose $k_1 \leqslant k_1(\alpha)$ and $k_2 \leqslant k_2(\beta)$ are algebraic simple extensions and $\tau : k_1 \to k_2$ is a field isomorphism such that $\widetilde{\tau}\big(m(\alpha, k_1)\big) = m(\beta, k_2)$. Then there exists an isomorphism $\sigma : k_1(\alpha) \to k_2(\beta)$ that extends τ. In other words, $k_1 \leqslant k_1(\alpha)$ and $k_2 \leqslant k_2(\beta)$ are isomorphic.*

1.8 Algebraic extensions II

Algebraic extensions are the core of classical Galois Theory and from now on we focus solely on them; no matter how interesting it is, the study of Galois Theory for arbitrary extensions is far beyond the scopes of this dissertation.

Convention. Henceforth all extensions are assumed to be algebraic unless explicitly stated otherwise.

So we need to put some extra effort into understanding algebraic extensions better.

Proposition 1.8.1. *A field extension is finite if and only if it is algebraic and finitely generated over the base field.*

Proof. ($\Rightarrow$) For a given finite extension $k \leqslant E$ with $[E : k] = n < \infty$, and any $z \in E$, the set

$$\{1, z, z, z^2, \ldots, z^n\} \subseteq E$$

is k-linearly dependent since it contains $n + 1 > [E : k]$ elements. That means we can find $a_0, \ldots, a_n \in k$, not all zero, such that

$$a_0 1 + a_1 z + a_2 z^2 + \ldots + a_n z^n = 0.$$

Therefore z is the root of $a_0 + a_1 x + \ldots + a_n x^n \in k[x]$ hence algebraic over k.

Moreover, since $[E : k] = n < \infty$, there exists an k-basis $\mathcal{B} = \{b_1, \ldots, b_n\} \subseteq E$ of E and thus

$$E = \{f_1 b_1 + \ldots + f_n b_n : f_i \in k\}.$$

Now on the one hand $k \leqslant k(\mathcal{B}) \leqslant E$ by definition of $k(\mathcal{B})$; so $k(\mathcal{B}) \subseteq E$. On the other hand,

$$\{f_1 b_1 + \ldots + f_n b_n : f_i \in k\} \subseteq L$$

for every extension L of k that contains $\mathcal{B}$ because

$$\underbrace{\underbrace{f_1}_{\in k \subseteq L}\ \underbrace{b_1}_{\in L}}_{\in L} + \ldots + \underbrace{\underbrace{f_n}_{\in k \subseteq L}\ \underbrace{b_n}_{\in L}}_{\in L} \in L \ \forall f_1, \ldots, f_n \in k.$$

But E *is* an extension of k that contains $\mathcal{B}$. Therefore $E \subseteq k(\mathcal{B})$ and as a result $E = k(\mathcal{B})$, i.e. E is finitely generated.

($\Leftarrow$) If $k \leqslant k(a_1, \ldots, a_n)$ is algebraic then in particular all a_i are algebraic over k. Applying 1.1.5 to the tower of fields

$$k \leqslant k(a_1) \leqslant k(a_1, a_2) \leqslant \ldots \leqslant k(a_1, \ldots, a_n),$$

we get

$$\begin{aligned}
[k(a_1, \ldots, a_n) : k] &= [k(a_1, \ldots, a_n) : k(a_1, \ldots, a_{n-1})] \ldots [k(a_1) : k] \\
&\overset{1.3}{=} [k(a_1, \ldots, a_{n-1})(a_n) : k(a_1, \ldots, a_{n-1})] \ldots [k(a_1) : k] \\
&\overset{1.6.9}{=} \deg m\big(a_n, k(a_1, \ldots, a_{n-1})\big) \ldots \deg m(a_1, k) \\
&\overset{1.6.5}{\leqslant} \deg m(a_n, k) \ldots \deg m(a_1, k) < \infty,
\end{aligned}$$

i.e. the extension is finite. ◇

Corollary 1.8.2. *Every finite field extension is algebraic.*

Corollary 1.8.3. *Suppose $k \leqslant E$ is a field extension and X a finite subset of E. Every $x \in X$ is algebraic if and only if the extension $k \leqslant k(X)$ is algebraic.*

Both hypotheses of 1.8.1 are essential for the converse. Example 1.5.2 gives a finitely generated but not finite, transcendental extension. Infinite algebraic extensions also exist.

Counterexample 1.8.4. The extension

$$\mathbb{Q} \leqslant \mathbb{A} = \{z \in \mathbb{C} : \ z \text{ is algebraic over } \mathbb{Q}\}$$

is a field extension which is by construction algebraic but not finite.*

Consider the n^{th} root of some number, say 2, and adjoin it to $\mathbb{Q}$. We get the tower of fields $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[n]{2}) \leqslant \mathbb{A}$. Since $\sqrt[n]{2}$ is algebraic over $\mathbb{Q}$ with minimal polynomial $m = x^n - 2$ (it is irreducible by Eisenstein's** criterion), the degree of the simple extension will be $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Therefore, from 1.1.4, we get

$$[\mathbb{A} : \mathbb{Q}] = [\mathbb{A} : \mathbb{Q}(\sqrt[n]{2})][\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] \geqslant n.$$

Since $n \in \mathbb{N}$ was arbitrary, the degree of the extension is infinite. ◂

Before closing this paragraph on algebraic extensions, we will see how they behave under subextensions.

Proposition 1.8.5 (Transitivity of algebraic extensions). *Given a tower of fields $k \leqslant L \leqslant E$, the extension $k \leqslant E$ is algebraic if and only if both the extensions $k \leqslant L$ and $L \leqslant E$ are algebraic.*

Proof. ($\Rightarrow$) Immediate.

($\Leftarrow$) Let $a \in E$. Since $L \leqslant E$ is algebraic, we can find the minimal polynomial

$$m(a, L) = x^n + \ldots + a_1 x + a_0 \in L[x].$$

Consider the extension generated by the coefficients of $m(a, L)$ over k,

$$k \leqslant k(a_0, \ldots, a_{n-1}) \leqslant L.$$

Since $k \leqslant L$ is algebraic, so is $k \leqslant k(a_0, \ldots, a_{n-1})$ which is by construction finitely generated over k, hence, by 1.8.1, finite

$$[k(a_0, \ldots, a_{n-1}) : k] < \infty.$$

Moreover $m(a, k) \in k(a_0, \ldots, a_{n-1})[x]$, which means that a is algebraic over $k(a_0, \ldots, a_{n-1})$ and, again by 1.8.1,

$$[k(a_0, \ldots, a_{n-1}, a) : k(a_0, \ldots, a_{n-1})] < \infty.$$

* An accessible proof that $\mathbb{A}$ is indeed a field can be found in [**6**].

**Ferdinand Gotthold Max Eisenstein (1823–1852).

Therefore, by 1.1.4,

$$[k(a_0,\dots,a_{n-1},a):k] = [k(a_0,\dots,a_{n-1},a):k(a_0,\dots,a_{n-1})] \cdot [k(a_0,\dots,a_{n-1}):k] < \infty.$$

Thus the extension is finite and by 1.8.2, algebraic. In particular a is algebraic over k. ◇

1.9 Constructing field extensions III: Splitting fields

For a given polynomial $f(x) \in k[x]$, we constructed in 1.2 a field extension that contains a zero of f. We can take one step further and construct a field that contains all roots of a given polynomial.

Definition. A polynomial $f(x) \in k[x]$ **splits over** k if all roots of f lie inside k. A **splitting field** for f is a minimal field over which f splits.

Example 1.9.1. The polynomial $x^2+1 \in \mathbb{Q}(x)$ does not split over $\mathbb{Q}$ or $\mathbb{R}$. It splits over $\mathbb{C}$ as well as over the smaller field $\mathbb{Q}(i)$; the latter is by definition a splitting field of $x^2+1 \in \mathbb{Q}[x]$. ◂

Example 1.9.2. Suppose $k \leqslant E$ is a field extension and let $f(x) \in k[x]$ such that $\deg f = n$. If f splits over E and $a_1,\dots,a_n \in E$ are its roots, then $k(a_1,\dots,a_n)$ is by construction a splitting field of f. ◂

A famous theorem of Leopold Kronecker (1823-1891) states that any polynomial has a splitting field.

Proposition 1.9.3 (Kronecker). *If $f(x) \in k[x]$ is a non-zero polynomial, then there exists a splitting field of f.*

Proof. Using induction on $\deg f$. The base case $\deg f = 1$ holds trivially. Assume that the theorem holds for all polynomials of degrees $\leqslant n$. Given a polynomial f with $\deg f = n+1$, the construction in 1.2 gives an extension E containing a root a of f. In E we can write $f(x) = (x-a)g(x)$, $\deg g \leqslant n$ and apply the induction hypothesis on $g(x)$. ◇

Example 1.9.4. Both $\mathbb{C} = \mathbb{R}(i)$ and $E = \mathbb{R}[x]/\langle x^2+1\rangle$ are splitting fields of $x^2+1 \in \mathbb{R}[x]$. To begin with, x^2+1 splits over both fields.

On the one hand, any splitting field $\mathbb{R} \leqslant L \leqslant \mathbb{R}(i)$ must contain both $\mathbb{R}$ and i. By the minimality of $\mathbb{R}(i)$, we deduce that $L = \mathbb{R}(i)$. On the other hand, for any splitting field $\mathbb{R} \leqslant L \leqslant E$, Prop. 1.1.4 gives

$$2 = [E:\mathbb{R}] = [E:L][L:\mathbb{R}].$$

But x^2+1 does not split over $\mathbb{R}$. Therefore, $[L:\mathbb{R}] > 1$ (so $[L:\mathbb{R}] = 2$) and $[E:L] = 1$ which means that $E = L$.

As we have already seen, the two fields are isomorphic. So in this case, these two splitting fields of $x^2+1 \in \mathbb{R}[x]$ are isomorphic. ◂

Actually, any two splitting fields of a polynomial $f(x) \in k[x]$ are isomorphic. Inspired by the extension theorem 1.7.4, we will prove the result directly for the general case of two isomorphic base fields.

Proposition 1.9.5 (Extension Theorem for Splitting Fields). *Let $\tau : k_1 \to k_2$ be a field isomorphism. If E_1 is the splitting field of some $f(x) \in k_1[x]$ and E_2 is the splitting field of $\widetilde{f} = \widetilde{\tau}(f) \in k_2[x]$ then there is a field isomorphism $\sigma : E_1 \to E_2$ that extends τ.*

Proof. With induction on $\deg f$.

If $\deg f = 1$ then k_1 is itself a splitting field of f and therefore, by the minimality of splitting fields, $k_1 = E_1$. Since $\widetilde{\tau}$ is an isomorphism, $\widetilde{f}$ also splits in k_2 and again $k_2 = E_2$. So the required extension of τ is itself.

Assume the theorem holds for all polynomials $f(x) \in k[x]$ of degree $\deg f < m$ for some $m \in \mathbb{N}$.

Let $f(x) \in k_1[x]$ be a polynomial of degree $\deg f = m$ and take $p(x)$ some *monic*, irreducible factor of f (it may be that $p = f$) of degree $\deg p \geqslant 2$; $p(x)$ has a root α in E_1 and $\widetilde{p} = \widetilde{\tau}(p)$ has a root β in E_2. By 1.7.4 there is an isomorphism σ_1 that extends τ to $k_1(\alpha)$.

$$\begin{array}{ccc} k_1(\alpha) & \xrightarrow{\sigma_1} & k_2(\beta) \\ \uparrow & & \uparrow \\ k_1 & \xrightarrow{\tau} & k_2 \end{array}$$

We now have that $f(x) = (x-\alpha)f_1(x) \in k(\alpha)[x]$ and $\widetilde{f}(x) = (x-\beta)\widetilde{f}_1(x) \in k(\beta)[x]$ where $\widetilde{f}_1 = \widetilde{\tau}(f_1)$ and $\deg f_1 = \deg \widetilde{f}_1 < m$. By the inductive hypothesis, E_1 is *the* splitting field of f_1 and E_2 is *the* splitting field of $\widetilde{f}_1$ (any other splitting field L of f_1 contains both α and the roots of f_1; this means that it is a splitting field of f inside E_1 and by minimality $L = E_1$; same for $\widetilde{f}_1$) and there is an isomorphism $\sigma : E_1 \to E_2$ extending σ_1.

$$\begin{array}{ccc} E_1 & \xrightarrow{\sigma} & E_2 \\ \uparrow & & \uparrow \\ k_1(\alpha) & \xrightarrow{\sigma_1} & k_2(\beta) \end{array}$$

Combining the two diagrams, we conclude that σ is an extension of τ. Therefore the extensions are isomorphic. ◇

Corollary 1.9.6. *Let k be a field, $f(x) \in k[x]$ some polynomial and E_1, E_2 two splitting fields of f. The extensions $k \leqslant E_1$ and $k \leqslant E_2$ are isomorphic. In particular, the splitting field of a polynomial $f(x)$ is unique up to isomorphism.*

1.10 Algebraic closures

The results in the preceding paragraph can be generalized in the sense that we can construct the splitting field of any *finite* set of polynomials $\{f_i(x) \in F[x] : i = 1, 2, \ldots, n\}$ by carrying out the construction of Example 1.2 at most $\prod_{i=1}^{n} \deg f_i$ times.

Using *Zorn's Lemma** we can take things one (huge) step further and consider an extension E of a field k that not only contains the roots of *every* polynomial $f(x) \in k[x]$, but also of *every polynomial* $g(x) \in E[x]$.

Lemma 1.10.1. *The following conditions are equivalent for a field k:*

1. *There are no algebraic extensions $k \subsetneq E$.*
2. *There are no finite extensions $k \subsetneq E$.*
3. *Every $f(x) \in k[x]$ splits over k.*
4. *Every $f(x) \in k[x]$ has a root in k.*

* Named after Max August Zorn (1906–1993).

5. *Every irreducible polynomial* $p(x) \in k[x]$ *has degree* 1.

Proof. (i)⇒(ii): Immediate since every finite extension is algebraic.

(ii)⇒(iii): If some $f \in k[x]$ did not split, then we could construct an extension E of k that contains a root of f. By construction this would be a finite extension (of degree at most $\deg f$).

(iii)⇒(iv): Immediate.

(iv)⇒(v): If $p(x) \in k[x]$, then p has a root in k hence a linear factor $l(x) \in k[x]$. If p is irreducible then $p = l$ so $\deg p = 1$.

(v)⇒(i): Suppose we have an algebraic extension $k \leqslant E$ and let $a \in E$. By the hypothesis, $m(a,k)$ has degree 1 so $[k(a) : k] = \deg m(a,k) = 1$. Therefore $k(a) = k$ which means that $a \in k$ and thus $E = k$. ◇

Definition. A field that satisfies any of the above equivalent conditions is called **algebraically closed**.

Example 1.10.2. By the *Fundamental Theorem of Algebra*, $\mathbb{C}$ is algebraically closed. ◂

Example 1.10.3. The field $\mathbb{A} = \{z \in \mathbb{C} : z \text{ algebraic over } \mathbb{Q}\}$ is algebraically closed. Indeed, suppose we have a finite (hence *finitely generated* and *algebraic*) extension $\mathbb{A} \leqslant \mathbb{A}(a_1, \ldots, a_n)$. The extension $\mathbb{Q} \leqslant \mathbb{A}$ is algebraic and, by Proposition 1.8.5, so is $\mathbb{Q} \leqslant \mathbb{A}(a_1, \ldots, a_n)$. Therefore $a_1, \ldots, a_n \in \mathbb{A}$ by the definition of $\mathbb{A}$ which implies that $\mathbb{A} = \mathbb{A}(a_1, \ldots, a_n)$. ◂

Counterexample 1.10.4. Neither $\mathbb{Q}$ nor $\mathbb{R}$ are algebraically closed. In both cases, the irreducible polynomial $x^2 + 1$ has degree 2. ◂

Definition. Let k be a field. An **algebraic closure** $\overline{k}$ of k is an *algebraic extension* of k that is *algebraically closed*.

Example 1.10.5. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. It is a finite, hence algebraic, extension of $\mathbb{R}$ that is algebraically closed. ◂

Counterexample 1.10.6. $\mathbb{C}$ is *not* an algebraic closure of $\mathbb{Q}$ because it is not an algebraic extension. ◂

Example 1.10.7. $\mathbb{A}$ is an algebraic closure of $\mathbb{Q}$. It is by construction algebraic and, as we saw, algebraically closed. ◂

Algebraic closures of arbitrary fields exist. As we mentioned, we are going to need Zorn's Lemma.

Lemma 1.10.8 (Kuratowski*, Zorn). *If $(P, \leqslant)$ is a partially ordered set so that every chain of P has an upper bound, then P has a maximal element.*

* Kazimierz Kuratowski (1896–1980) had indepedently proven this lemma a few years before Zorn.

We take Zorn's Lemma as an axiom since it is equivalent to the Axiom of Choice. The interested reader can consult [**26**].

Proposition 1.10.9. *Suppose k is a field. Then an algebraic closure of k exists.*

Proof. For every non constant polynomial $f(x) \in k[x]$, we take an independent variable x_f and consider the polynomial ring R generated by all these variables over k. The ideal $I = \langle f(x_f) : f \in k[x] \rangle$ of R is proper. Otherwise we would find some $g_1, \ldots, g_k \in R$ and some $f_1, \ldots, f_m \in I$ such that

$$g_1 f_1(x_{f_1}) + \ldots + g_m f_m(x_{f_m}) = 1.$$

But each f_i has a root, say a_i. Evaluating at $(x_{f_1}, \ldots, x_{f_m}) = (a_1, \ldots, a_m)$, we get $0 = 1$ which is absurd.

Since the ideal I is proper, it is contained in a maximal ideal J, i.e. $I \subseteq J \subset R$. This is a standard result from Algebra that *requires Zorn's Lemma*. Take the set S of all proper ideals of R and show that every chain has an upper bound, the union of its elements. Zorn's Lemma ensures the existent of a maximal element of S. It is easy to see that this is the required ideal. The missing details are easy to fill.

Now J is maximal so R/J is a field. Using the restriction of the natural projection to F, i.e.

$$\pi|_k : k \to R/J$$

we can see that R/J is an extension of k. This extension contains a root of every $f(x) \in k[x]$, namely $x_f + I$, since

$$f(x_f) + I = I.$$

We have constructed a field $k_1 = R/J$ that extends k and contains a root for every irreducible polynomial of $k[x]$. With the same arguments

we can construct a tower of fields

$$k \leqslant k_1 \leqslant k_2 \leqslant k_3 \leqslant \ldots \leqslant k_s \leqslant \ldots$$

such that k_{j+1} contains a root for every irreducible polynomial in $k_j[x]$. Their union

$$E = \bigcup_{j=1}^{\infty} k_j$$

is clearly an extension of k. By construction, it contains the root of every polynomial $g \in E[x]$. In other words, it is algebraically closed.

We can now take

$$\overline{k} = \{z \in E : z \text{ algebraic over } k\}.$$

$\overline{k}$ is an algebraic extension of k that is algebraically closed. Thus we have constructed an algebraic closure of k. ◇

Using Zorn's Lemma again, it can be shown that

Proposition 1.10.10 (Extension Thm for Algebraic Closures). *Suppose $\tau : k_1 \to k_2$ is a field isomorphism, S_1 is a set of polynomials over k_1 and $S_2 = \widetilde{\tau}(S_1)$ where $\widetilde{\tau} : k_1[x] \to k_2[x]$ is the map induced by τ. If E_1 is a splitting field of S_1 and E_2 is a splitting field of S_2, then there is an isomorphism $\sigma : E_1 \to E_2$ extending τ. In particular, algebraic closures are unique up to isomorphism.*

Furthermore, if $a_1 \in E_1$ has minimal polynomial $m = m(a, k_1)$ and $a_2 \in E_2$ is any root of $\widetilde{\tau}(m)$, then σ can be chosen so that $\sigma(a_1) = a_2$.

Proof. Consider the set

$$S = \{(L, \vartheta) : L \leqslant E_1,\ \vartheta : L \to E_2 : \vartheta|_{k_1} = \tau\}.$$

Then $S \neq \emptyset$ since $(k_1, \tau) \in S$ and is partially ordered by defining

$$(L_1, \vartheta_1) \leqslant (L_2, \vartheta_2) \Leftrightarrow L_1 \leqslant L_2 \text{ and } \vartheta_2|_{L_1} = \vartheta_1.$$

If $c \equiv (L_i, \vartheta_i)$ is a chain in S and we define $L = \bigcup L_i$ and

$$\vartheta : L \to E_2 : \vartheta(x) = \vartheta_i(x) \text{ if } x \in L_i$$

then (L, ϑ) is an upper bound of c. By Zorn's Lemma, there is a maximal element (L_0, ϑ_0) in S. By definition, $L_0 \leqslant E_1$. If $L_0 \neq E_1$, then there is

some $f_1 \in S_1$ that does not split over L_0. Take a root $a_1 \in E_1 \setminus L_0$ of f_1, its minimal polynomial $m_1 = m(a_1, k_1)$ and its image $m_2 = \widetilde{\tau}(m_1)$ and a root $a_2 \in E_2$ of m_2. From the Extension Theorem for simple extensions, τ can be extended to an isomorphism $\rho : L_0(a_1) \to \vartheta_0(L_0)(a_2)$. Then $(L_0(a_1), \rho)$ is an element of S which is bigger that (L_0, ϑ_0), a contradiction. Therefore, $L_0 = E_1$. From the Extension Theorem for splitting fields, $\vartheta_0(E_1) = E_2$. ◇

Corollary 1.10.11. *Every algebraic field extension E of a field k can be embedded in $\overline{k}$.*

Proof. The algebraic closure $\overline{E}$ of E is an algebraic closure of k as well since $k \leqslant E$ is algebraic. So there is an isomorphism $f : \overline{E} \to \overline{k}$ and E is then embedded in $\overline{k}$ as $E \cong f(E)$. ◇

1.11 Constructing field extensions IV: Compositums

Having defined algebraic closures, we obtain another way of constructing field extensions that will be proved useful.

Definition. Given any field k and any two *algebraic* field extensions L, M of k, we define their **compositum** LM to be the *smallest subfield of $\overline{k}$ that contains both L and M*, i.e.

$$LM = L(M) = M(L) \leqslant \overline{k}.$$

Similarly, we can define the compositum of any family $\{L_i\}_{i \in I}$ of algebraic extensions of k.

Obviously,

Lemma 1.11.1. *The compositum of any family of algebraic extensions of k is an algebraic extension of k.*

and

Lemma 1.11.2. *The compositum of any finite family of finite extensions of k is a finite extension of k.*

Proof. Suppose L and M are two finite extensions of k. From the previous lemma and Proposition 1.8.1, we need only show that their compositum is finitely generated. Since both L and M are finite, they are finitely generated; write $L = k(a_1, \ldots, a_s)$ and $M = k(b_1, \ldots, b_r)$. It is now immediate that $LM = k(a_1, \ldots, a_s, b_1, \ldots, b_r)$. We proceed with induction. ◇

Chapter 2
The Galois-Artin Correspondence

The distinction, although artificial, between Field Theory and Galois Theory is in the tools we use to study field extensions. Until now, we have only used the theory of vector spaces. When Galois' ideas are introduced into the theory of fields, richer and deeper results are obtained.

In this section we define the Galois correspondence. We will see how we can associate each field extension to a suitably chosen group and what information can the latter give us about the extension. This group will be the group of automorphisms of the extension in question. So before we see how we can use it, lets state some important results.

2.1 More on k-automorphisms

Let us recall some definitions. Suppose $k \leqslant E$ be a field extension. An k-**automorphism** of E is a map $\sigma \in \mathrm{Aut}(E)$ such that $\sigma|_k = \mathrm{id}_k$. The k-automorphisms of E are exactly the field extension isomorphisms from $k \leqslant E$ to itself.

The set of all k-automorphisms of E, denoted by $\mathrm{Aut}(E/k)$, forms a group under the usual composition of maps; it is a *subgroup* of $\mathrm{Aut}(E)$ (Lemma 1.3.5).

For *finite* extensions, there is a rather straightforward way of computing $\mathrm{Aut}(E/k)$.

Example 2.1.1. Consider the *finite* (hence *finitely generated* and *algebraic*) extension $k \leqslant E$ where $E = k(X)$ for some finite subset $X = \{\alpha_1, \ldots, \alpha_n\}$ of E. Let $\sigma \in \mathrm{Aut}(E/k)$.

Since $\sigma|_k = \mathrm{id}_k$, the map σ is determined solely by its action on the elements of X. Indeed, using Cor. 1.4.5, for any $x \in E = k(\alpha_1, \ldots, \alpha_n)$,

we have

$$\sigma(x) = \sigma\left(\frac{f(\alpha_1,\ldots,\alpha_n)}{g(\alpha_1,\ldots,\alpha_n)}\right) = \frac{f\big(\sigma(\alpha_1),\ldots,\sigma(\alpha_n)\big)}{g\big(\sigma(\alpha_1),\ldots,\sigma(\alpha_n)\big)}.$$

Since $k \leqslant E$ is *algebraic*, every $\alpha \in X$ is algebraic over k. If the minimal polynomial of an element $\alpha \in X$ over k is

$$m(x) \equiv m(\alpha,k)(x) = x^n + \ldots + a_1 x + a_0 \in k[x],$$

then $\sigma(\alpha)$ is just another root of m. Indeed,

$$\begin{aligned} m(\alpha) = 0 &\Rightarrow \sigma\big(m(\alpha)\big) = \sigma(0) \\ &\Rightarrow \sigma(\alpha^n + \ldots + a_1\alpha + a_0) = 0 \\ &\Rightarrow \sigma(\alpha^n) + \ldots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) = 0 \\ &\Rightarrow \sigma(\alpha)^n + \ldots + a_1\sigma(\alpha) + a_0 = 0 \\ &\Rightarrow m\big(\sigma(\alpha)\big) = 0. \end{aligned}$$

The roots of an irreducible polynomial are said to be **conjugate**. So the image $\sigma(\alpha)$ of some $\alpha \in X$ under $\sigma \in \mathrm{Aut}(E/k)$ *is a conjugate of* α. ◂

Example 2.1.2. The only $\mathbb{R}$-automorphisms of $\mathbb{C} = \mathbb{R}(i)$ are the identical map $\mathrm{id}_{\mathbb{C}}$ and complex conjugation $z \mapsto \overline{z}$. ◂

It is now apparent that

Proposition 2.1.3. *If $k \leqslant E$ is a finite extension, then* $\mathrm{Aut}(E/k)$ *is also finite.*

Proof. Immediate since (i) every $\sigma \in \mathrm{Aut}(E/k)$ is determined by its action on X, (ii) X is finite, (iii) $\sigma(\alpha)$ is a conjugate of α for every $\alpha \in X$ and (iv) $\partial m(\alpha,k) < \infty$ and therefore $\sigma(\alpha)$ can only take a finite number of values. ◇

2.2 The correspondence

It is time to describe the Galois correspondence. Let $k \leqslant E$ be a field extension. As we said, the group we are going to use to study the

extension is the group $\mathrm{Aut}(E/k)$ of k-automorphisms of E. The way we will pass from the extension to the group and vice versa is the following.

We associate every intermediate field $k \leqslant L \leqslant E$ with the group $\mathrm{Aut}(E/L)$ of L-automorphisms of E. Using elementary Group Theory it is easy to deduce that $\mathrm{Aut}(E/L)$ *is a subgroup of* $\mathrm{Aut}(E/F)$.

Lemma 2.2.1. *If L is a subextension of $k \leqslant E$ then $\mathrm{Aut}(E/L)$ is a subgroup of $\mathrm{Aut}(E/k)$.*

In the opposite direction, we associate with each subgroup $H \leqslant \mathrm{Aut}(E/k)$, the set

$$\mathrm{Fix}_E(H) = \{x \in E : \sigma(x) = x \ \forall \sigma \in H\}.$$

Using elementary properties of homomorphisms, it is easy to see that the above set is a *subextension* of $k \leqslant E$.

Lemma 2.2.2. *If $k \leqslant E$ is a field extension and H is a subgroup of $\mathrm{Aut}(E/k)$ then $\mathrm{Fix}_E(H)$ is a subextension of $k \leqslant E$.*

This establishes a correspondence between intermediate fields of a field extension and subgroups of its k-automorphism group.

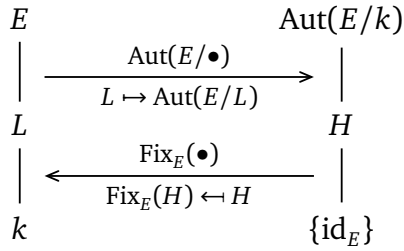


Figure 2.1: The Galois-Artin Correspondence

Example 2.2.3. Let $k \leqslant E$ be a field extension and $G = \mathrm{Aut}(E/k)$ its k-automorphism group. To the field k we assign the subgroup of G that fixes k which is, by definition, the whole group G. To the field E we assign the subgroup of G that fixes E, which is the trivial subgroup $\{\mathrm{id}_E\}$ since id_E is the only isomorphism $E \to E$ that fixes E. Observe how the *whole group* is associated to the *base field* while the *trivial subgroup* is associated to the *extending field*. ◀

The above example reveals a crucial property of the correspondence.

Proposition 2.2.4. *The Galois correspondence of a field extension*

$$\{\textit{subextensions } L:\ k \leqslant L \leqslant E\} \rightleftarrows \{\textit{subgroups } H:\ H \leqslant \mathrm{Aut}(E/k)\}$$

as described above, is order reversing.

Proof. If $L_1 \leqslant L_2$ then given some automorphism $\sigma \in \mathrm{Aut}(E/L_2)$ that fixes L_2 pointwise, σ also fixes $L_1 \subseteq L_2$ pointwise.

On the other hand, if $H_1 \leqslant H_2$ and some element $a \in E$ is fixed by every automorphism $\tau \in H_2$, then it is also fixed by every automorphism $\tau' \in H_1 \subseteq H_2$. ◇

Another important property which is an immediate consequence of the definitions is

Proposition 2.2.5. *If $k \leqslant E$ is a field extension, then*

$$H \subseteq \mathrm{Aut}\left(E/\mathrm{Fix}_E(H)\right)\ \forall H \leqslant \mathrm{Aut}(E/k) \textit{ and}$$
$$L \subseteq \mathrm{Fix}_E\left(\mathrm{Aut}(E/L)\right)\ \ \forall L : k \leqslant L \leqslant E.$$

2.3 Bijective Galois correspondences

By its definition, the Galois correspondence is a correspondence between *the set of subextensions L of $k \leqslant E$ that arise as fixed fields*, i.e. $L = \mathrm{Fix}_E(H)$ for some $H \leqslant \mathrm{Aut}(E/k)$, and *the set of subgroups H of* $\mathrm{Aut}(E/k)$ *that arise as automorphism groups*, i.e. $H = \mathrm{Aut}(E/L)$ for some $k \leqslant L \leqslant E$.

$$\left\{\begin{array}{c}\text{subextensions } k \leqslant L \leqslant E:\\ \exists H \leqslant \mathrm{Aut}(E/k) : L = \mathrm{Fix}_E(H)\end{array}\right\} \rightleftarrows \left\{\begin{array}{c}\text{subgroups } H \leqslant \mathrm{Aut}(E/k):\\ \exists k \leqslant L \leqslant E : H = \mathrm{Aut}(E/L)\end{array}\right\}$$

The next result suggests that this is a bijective correspondence, i.e. the maps $\mathrm{Aut}(E/\bullet)$ and $\mathrm{Fix}_E(\bullet)$ are mutually inverse.

Proposition 2.3.1. *Let $k \leqslant E$ be a field extension. With the above notation,*

1. *If $H = \mathrm{Aut}(E/L)$ for some $k \leqslant L \leqslant E$ then*

$$H = \mathrm{Aut}\left(E/\mathrm{Fix}_E(H)\right).$$

2. *If* $L = \mathrm{Fix}_E(H)$ *for some* $H \leqslant \mathrm{Aut}(E/k)$ *then*

$$L = \mathrm{Fix}\big(\mathrm{Aut}(E/L)\big).$$

Proof. 1. If $H = \mathrm{Aut}(E/L)$ for some subextension L of $k \leqslant E$ then

$$\begin{aligned} H = \mathrm{Aut}(E/L) &\Rightarrow L \subseteq \mathrm{Fix}_E(H) \\ &\Rightarrow \mathrm{Aut}(E/L) \supseteq \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big) \\ &\Rightarrow H \supseteq \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big) \end{aligned}$$

and we already know that $H \subseteq \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)$. The two inclusions give $H = \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)$.

2. Similarly, if $L = \mathrm{Fix}_E(H)$ for some subgroup $H \leqslant \mathrm{Aut}(E/k)$ then

$$\begin{aligned} L = \mathrm{Fix}_E(H) &\Rightarrow H \subseteq \mathrm{Aut}(E/L) \\ &\Rightarrow \mathrm{Fix}_E(H) \supseteq \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big) \\ &\Rightarrow L \supseteq \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big) \end{aligned}$$

and we already know that $L \subseteq \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)$. The two inclusions give $L = \mathrm{Fix}\big(\mathrm{Gal}(E/L)\big)$. ◇

Our main objective now is to examine to which extend the Galois correspondence for an arbitrary field extension $k \leqslant E$ is a bijective correspondence between the set of *all* subextensions of $k \leqslant E$ and the set of *all* subgroups of $\mathrm{Aut}(E/k)$. In other words, to what extend the maps $\mathrm{Aut}(E/\bullet)$ and $\mathrm{Fix}_E(\bullet)$ are onto or, equivalently by Prop. 2.3.1, mutually inverse, i.e.

$$H = \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big) \ \forall H \leqslant \mathrm{Aut}(E/k) \tag{2.1}$$

and

$$L = \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big) \ \forall L : k \leqslant L \leqslant E. \tag{2.2}$$

In general these maps are *not* mutualy inverse. As we saw (Prop. 2.2.5), they satisfy the weaker conditions

$$H \subseteq \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big) \ \forall H \leqslant \mathrm{Aut}(E/k) \tag{2.3}$$

and

$$L \subseteq \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big) \ \forall L : k \leqslant L \leqslant E. \tag{2.4}$$

There are examples where these inclusions can be equalities as shown below.

Example 2.3.2. Consider the extension $\mathbb{R} \leqslant \mathbb{R}(i)$ inside $\mathbb{C}$. On the one hand, $G = \mathrm{Aut}(\mathbb{R}(i)/\mathbb{R})$ is a group of order 2 (Ex. 2.1.2). On the other, by Ex. 1.1.3 and Prop. 1.1.4, the only intermediate fields $\mathbb{R} \leqslant L \leqslant \mathbb{R}(i)$ are $L = \mathbb{R}$ and $L = \mathbb{R}(i)$. Thus the Galois correspondence associates

$$\mathbb{R} \rightleftarrows G \quad \text{and} \quad \mathbb{R}(i) \rightleftarrows \{\mathrm{id}_{\mathbb{R}(i)}\}$$

and the two inclusions are (rather trivially) equalities. ◂

But there are also examples where the inclusions are strict.

Counterexample 2.3.3. A case where (2.3) might be strict is when a given extension $k \leqslant E$ has infinite degree. In this case we will see in due time that the corresponding group $\mathrm{Aut}(E/k)$ is also infinite, hence too big to be handled properly. In particular, $\mathrm{Aut}(E/k)$ has too many subgroups! Indeed, as we shall see in Ex. 5.2.3, in this case not every subgroup H of $\mathrm{Aut}(E/k)$ arises as an automorphism group, i.e. there might not exist L such that $k \leqslant L \leqslant E$ and $H = \mathrm{Aut}(E/L)$.

So if H is a subgroup that cannot arise as an automorphism group of some intermediate field, then $H \subsetneq \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)$. ◂

Counterexample 2.3.4. Consider the extension $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2})$. If $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ then σ is determined by its image $\sigma(\sqrt[3]{2})$ which is a conjugate of $\sqrt[3]{2}$. But the conjugates of $\sqrt[3]{2}$ are all complex numbers that are not in $\mathbb{Q}(\sqrt[3]{2})$. Therefore, the group of automorphisms $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is trivial, hence its fixed field is

$$\mathrm{Fix}_{\mathbb{Q}(\sqrt[3]{2})}\big(\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})\big) = \mathbb{Q}(\sqrt[3]{2}) \supsetneq \mathbb{Q}$$

and that shows that the inclusion (2.4) may also be strict. ◂

Counterexample 2.3.5. There is another instance where (2.4) may be strict, but for completely different reasons this time. Consider the

finite field $\mathbb{F}_2$ and an indeterminate t. We can then form the extension $\mathbb{F}_2 \leqslant \mathbb{F}_2(t)$. If we take the element $t^2 \in \mathbb{F}_2(t)$, we can further form the tower

$$\mathbb{F}_2 \leqslant \mathbb{F}_2(t^2) \leqslant \mathbb{F}_2(t).$$

We will focus on the extension $\mathbb{F}_2(t^2) \leqslant \mathbb{F}_2(t)$.

First of all, it is intuitively clear (but requires a long, technical proof which we will avoid) that $\mathbb{F}_2(t) = [\mathbb{F}_2(t^2)](t)$ and therefore the extension is simple (every polynomial in t with coefficients in $\mathbb{F}_2$ can be viwed as a polynomial in t with coefficients from $\mathbb{F}_2(t^2)$ since $\mathbb{F}_2 \leqslant \mathbb{F}_2(t^2)$; on the other hand, a polynomial in t with coefficients in $\mathbb{F}_2(t^2)$ can be considered as a polynomial in t using the distributive law and grouping together all the t's in every monomial).

The element t does not belong in $\mathbb{F}_2(t^2)$ but is algebraic over $\mathbb{F}_2(t^2)$: the polynomial

$$m(x) = x^2 - t^2 \in [\mathbb{F}_2(t^2)][x]$$

is monic, of minimal degree such that $m(t) = 0 \in \mathbb{F}_2(t^2)$ hence by definition is the minimal polynomial of t over $\mathbb{F}_2(t^2)$, i.e.

$$m(x) = m\big(t, \mathbb{F}_2(t^2)\big)(x).$$

Observe at this point that since we are inside $\mathbb{F}_2$, we have

$$m(x) = x^2 - t^2 = (x - t)^2$$

so the only root of m is t. We can now imagine where this leads us.

If $\sigma \in \mathrm{Aut}\big(\mathbb{F}_2(t)/\mathbb{F}_2(t^2)\big)$ then σ is determined by its action on t and $\sigma(t)$ is a conjugate of t. But the only conjugate of t is t itself. Therefore $\sigma(t) = t$ and the automorphism group is again the trivial, which means

$$\mathrm{Fix}_{\mathbb{F}_2(t)}\big[\,\mathrm{Aut}\big(\mathbb{F}_2(t)/\mathbb{F}_2(t^2)\big)\big] = \mathbb{F}_2(t) \supsetneq \mathbb{F}_2(t^2). \qquad \blacktriangleleft$$

By the above examples it is apparent that the Galois correspondence is *not* bijective in general. Our next plan is to understand why it failed to be bijective in the above counterexamples and define for which extensions the correspondence is actually bijective.

2.4 The correspondence for finite extensions

If we try to understand why

$$H = \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)\ \forall H \leqslant \mathrm{Aut}(E/k) \tag{2.1}$$

fails to hold for infinite extensions (2.3.3), we end up thinking if it is due to the automorphism group being too big. So it is natural to wonder whether finite extensions suffice for such an equality. We will see that the answer is *yes*.

If $k \leqslant E$ is a *finite* field extension then, by Prop. 2.1.3, $\mathrm{Aut}(E/k)$ is finite and so are its subgroups H and $\mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)$.

So we have two *finite* subgroups of $\mathrm{Aut}(E/k)$ for which we already know that

$$H \subseteq \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big).$$

So it suffices to show that

$$|H| \geqslant |\mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)|.$$

We will proceed by finding an upper bound b for the cardinality $|\mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)|$ and we will then show that $|H| = b$.

Lemma 2.4.1 (Dedekind). *Let $\vartheta_1, \ldots, \vartheta_n : k \to E$ be distinct field monomorphisms. Then the ϑ_i's are linearly independent over E.*

Proof. Suppose, for the contrary, that there are $c_1, \ldots, c_n \in E$ not all zero such that

$$c_1\vartheta_1(x) + \ldots + c_n\vartheta_n(x) = 0 \ \forall x \in k.$$

Omitting the terms whose $c_i = 0$ and rearranging the rest if necessary, we get a minimal $m \leqslant n$ such that

$$c_1\vartheta_1(x) + \ldots + c_k\vartheta_m(x) = 0 \ \forall x \in k \tag{2.5}$$

and $c_i \neq 0$ for all $i = 1, \ldots, m$. Since the monomorphisms are distinct, there is some $x_0 \in k$ such that $\vartheta_1(x_0) \neq \vartheta_2(x_0)$. If we multiply both sides of (2.5) by $\vartheta_1(x_0)$ we get

$$c_1\vartheta_1(x)\vartheta_1(x_0) + \ldots + c_m\vartheta_m(x)\vartheta_1(x_0) = 0 \ \forall x \in k. \tag{2.6}$$

Taking $x = x_0x$ in (2.5) we have

$$c_1\vartheta_1(x_0x) + \ldots + c_m\vartheta_m(x_0x) = 0 \ \forall x \in k$$

or, equivalently,

$$c_1\vartheta_1(x_0)\vartheta_1(x) + \ldots + c_m\vartheta_m(x_0)\vartheta_m(x) = 0 \ \forall x \in k. \tag{2.7}$$

Substracting (2.7) from (2.6) gives us

$$c_1\vartheta_1(x)\big(\vartheta_1(x_0)-\vartheta_1(x_0)\big)+\ldots+c_m\vartheta_m(x)\big(\vartheta_1(x_0)-\vartheta_m(x_0)\big)=0$$

or, equivalently,

$$c_2\vartheta_2(x)\big(\vartheta_1(x_0)-\vartheta_2(x_0)\big)+\ldots+c_m\vartheta_m(x)\big(\vartheta_1(x_0)-\vartheta_m(x_0)\big)=0$$

which contradicts the minimality of m. ◇

Proposition 2.4.2. *If $k \leqslant E$ is a finite field extension then $|\mathrm{Aut}(E/k)|$ is at most $[E:k]$.*

Proof. Since $k \leqslant E$ is finite, so is $\mathrm{Aut}(E/k)$. Suppose that $\mathrm{Aut}(E/k) = \{\vartheta_1,\ldots,\vartheta_n\}$ and that $[E:k]=m<n$. If $\mathscr{B}=\{a_1,\ldots,a_m\}$ is an k-basis of E, the matrix

$$A=\begin{pmatrix}\vartheta_1(a_1) & \vartheta_1(a_2) & \ldots & \vartheta_1(a_m)\\ \vartheta_2(a_1) & \vartheta_2(a_2) & \ldots & \vartheta_2(a_m)\\ \vdots & \vdots & \ddots & \vdots\\ \vartheta_n(a_1) & \vartheta_n(a_2) & \ldots & \vartheta_n(a_m)\end{pmatrix}$$

has rank $\mathrm{rank}(A) \leqslant m < n$. Therefore, its rows are linearly dependent over k; so there are $c_{ji}\in E$, $i=1,\ldots,n$, not all zero, such that $\sum_{i=1}^n c_{ji}\vartheta_i(a_j)=0$ for all $j=1,\ldots,m$. As a result, for every $x=\sum_{j=1}^m x_j a_j \in E$ $(x_j\in F)$ we have

$$\begin{aligned}\sum_{i=1}^n c_{ji}\vartheta_i(x)&=\sum_{i=1}^n c_{ji}\vartheta_i\left(\sum_{j=1}^m x_j a_j\right)=\sum_{i=1}^n c_{ji}\left(x_j\sum_{j=1}^m \vartheta_i(a_j)\right)\\ &=\sum_{j=1}^m x_j\left(\sum_{i=1}^n c_{ji}\vartheta_i(a_j)\right)=0\end{aligned}$$

so the ϑ_i's are E-lineraly dependent which contradicts Dedekind's Lemma since the ϑ_i's are distinct monomorphisms $E\to E$. Therefore, $|\mathrm{Aut}(E/k)| \leqslant [E:k]$ ◇

The above, together with Cor 1.1.6, give us an upper bound for $|\mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)|$.

Corollary 2.4.3. *Suppose $k \leqslant E$ is a finite field extension and H is a subgroup of* $\mathrm{Aut}(E/k)$. *Then* $|\mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)| \leqslant [E : \mathrm{Fix}_E(H)]$.

Proposition 2.4.4. *If E is a field and H is a finite subgroup of* $\mathrm{Aut}(E)$ *then*

$$|H| = [E : \mathrm{Fix}_E(H)].$$

Proof. Let

$$H = \{\vartheta_1 = 1, \vartheta_2, \ldots, \vartheta_n\}$$

and $[E : \mathrm{Fix}_E(H)] = m$. We will show that $m < n$ and $m > n$ cannot happen.

Suppose $m < n$ and $\{a_1, \ldots, a_m\}$ is a $\mathrm{Fix}_E(H)$-basis of E. The homogenous system

$$\begin{cases} \vartheta_1(a_1)x_1 + \ldots + \vartheta_n(a_1)x_n = 0 \\ \quad \vdots \\ \vartheta_1(a_m)x_1 + \ldots + \vartheta_n(a_m)x_n = 0 \end{cases}$$

has m linear equations and $n < m$ unknowns. Hence it has a non-zero solution $(y_1, \ldots, y_n) \in E^n$, i.e.

$$\vartheta_1(a_i)y_1 + \ldots + \vartheta_n(a_i)y_n = 0 \quad \forall i = 1, \ldots, m.$$

For an arbitrary $x = \sum_{j=1}^m c_j a_j \in E$, $c_j \in \mathrm{Fix}_E(H)$, we get

$$\begin{aligned} \vartheta_1(x)y_1 + \ldots + \vartheta_n(x)y_n &= \vartheta_1\left(\sum_{j=1}^m c_j a_j\right) y_1 + \ldots + \vartheta_n\left(\sum_{j=1}^m c_j a_j\right) y_n \\ &= \sum_{j=1}^m c_j[\vartheta_1(a_j)y_1 + \ldots + \vartheta_n(a_j)y_n] = 0. \end{aligned}$$

That is, the monomorphisms $\vartheta_1, \ldots, \vartheta_n$ are linearly dependent. But this contradicts Dedekind's Lemma. Therefore, $m \geqslant n$.

Suppose now that $m > n$ and take again some $\mathrm{Fix}_E(H)$-lineraly independent set of $n+1$ elements, say $\{a_1, \ldots, a_{n+1}\}$. Once more, we have a homogenous linear system

$$\begin{cases} \vartheta_1(a_1)x_1 + \ldots + \vartheta_1(a_{n+1})x_{n+1} = 0 \\ \quad \vdots \\ \vartheta_n(a_1)x_1 + \ldots + \vartheta_n(a_{n+1})x_{n+1} = 0 \end{cases}$$

with n equations and $n+1 > n$ unknowns. Hence it has a non-zero solution. We can choose a solution $(y_1, \dots, y_{n+1}) \in E^n$ that has the fewest possible non-zero coordinates. Without loss of generality we may assume that

$$y_1, \dots, y_r \neq 0, \quad y_{r+1}, \dots, y_{n+1} = 0$$

for some $1 \leqslant r \leqslant n+1$ so that we have

$$(*) \qquad \vartheta_i(a_1)y_1 + \dots + \vartheta_i(a_r)y_r = 0 \quad \forall i = 1, \dots, n.$$

For all $\vartheta \in H$ we have

$$\vartheta\vartheta_i(a_1)\vartheta(y_1) + \dots + \vartheta\vartheta_i(a_r)\vartheta(y_r) = 0 \quad \forall i = 1, \dots, n.$$

or equivalently, since the map $H \to H : \vartheta_i \mapsto \vartheta\vartheta_i$ is a bijection,

$$(**) \qquad \vartheta_i(a_1)\vartheta(y_1) + \dots + \vartheta_i(a_r)\vartheta(y_r) = 0 \quad \forall i = 1, \dots, n.$$

Multiplying $(*)$ by $\vartheta(a_1)$ and $(**)$ by a_1 and substracting, we get

$$[y_2\vartheta(y_1) - \vartheta(y_2)y_1]\vartheta_i(a_2) + \dots + [y_r\vartheta(y_1) - \vartheta(y_r)y_1]\vartheta_i(a_r) = 0$$

for all $i = 1, \dots, n$ which contradicts the minimality of r. Therefore

$$y_j\vartheta(y_1) - y_1\vartheta(y_j) = 0 \Leftrightarrow y_j y_1^{-1} = \vartheta(y_j y_1^{-1}) \quad \forall j = 1, \dots, r$$

for all $\vartheta \in H$. That means we can find some $z_1, \dots, z_r \in \mathrm{Fix}_E(H)$ and some $k \in E$ so that $y_j = kz_j$ for all $j = 1, \dots, r$. Then, for $i = 1$, $(*)$ becomes

$$kz_1 a_1 + \dots + kz_r a_r = 0 \overset{k \neq 0}{\Leftrightarrow} z_1 a_1 + \dots + z_r a_r = 0$$

which contradicts the linear independence of $\{a_1, \dots, a_{n+1}\}$. Therefore $m \leqslant n$ and we conclude that $m = n$. ◇

Corollary 2.4.5. *For any finite field extension $k \leqslant E$ and any subgroup H of* $\mathrm{Aut}(E/k)$*,*

$$H = \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big).$$

Proof. We have $H \subseteq \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)$ and

$$|\mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)| \overset{2.4.3}{\leqslant} [E : \mathrm{Fix}_E(H)] \overset{2.4.4}{=} |H| \overset{2.1.3}{<} \infty.$$

Therefore $H = \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big)$. ◇

2.5 Galois extensions I

It remains to examine the extensions for which (2.2) holds. These extensions are called *Galois extensions* because they naturally generalize the setting Galois used to work in, to abstract fields.

Definition (1st definition of Galois extensions). A field extension $k \leqslant E$ is called **Galois** if

$$L = \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)$$

for every subextension L of $k \leqslant E$. In this case we write $\mathrm{Gal}(E/k)$ for $\mathrm{Aut}(E/k)$ and call it the **Galois group** of the extension.

Example 2.5.1. The extension $\mathbb{R} \leqslant \mathbb{R}(i)$ of Ex. 2.3.2 is Galois as we already saw. ◀

Counterexample 2.5.2. The extensions $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{F}_2(t^2) \leqslant \mathbb{F}_2(t)$ of Ex. 2.3.4 and 2.3.5 respectively are *not* Galois. ◀

This definition gives us no information on the structure of a Galois extension and is in general hard to work with especially since the defining condition (2.2) has to be checked for *every* intermediate field L. We want to understand the structure of Galois extensions better and see if we can simplify their definition. This is done in the next section where we will see a number conditions equivalent to (2.2) that will help us understand Galois extensions better.

Chapter 3
Galois Extensions

3.1 Galois extensions II

Turning our attention to

$$L = \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)\ \forall L : k \leqslant L \leqslant E \tag{2.2}$$

and why that failed to hold in 2.3.4 and 2.3.5 for $L = k$, we find that, contrary to the previous discussion, the automorphism group in both cases is too small and thus contains little information about the field extension in the sense that it does not match its upper bound set in Prop. 2.4.2:

$$|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1 < 3 = \partial m(\sqrt[3]{2}, \mathbb{Q}) = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$$

and

$$|\mathrm{Aut}\big(\mathbb{F}_2(t)/\mathbb{F}(t^2)\big)| = 1 < 2 = \partial m\big(t, \mathbb{F}_2(t^2)\big) = [\mathbb{F}_2(t) : \mathbb{F}_2(t^2)].$$

Therefore it would be reasonable to suspect that if $|\mathrm{Aut}(E/L)|$ equals $[E : L]$ then (2.2) holds. In fact, the conditions

$$L = \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)\ \forall L : k \leqslant L \leqslant E$$

and

$$|\mathrm{Aut}(E/L)| = [E : L]\ \forall L : k \leqslant L \leqslant E$$

are equivalent for *finite* extensions.

Proposition 3.1.1. *Suppose $k \leqslant E$ is a finite extension and L is a subextension, i.e. $k \leqslant L \leqslant E$. Then*

$$L = \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big) \quad \textit{iff} \quad |\mathrm{Aut}(E/L)| = [E : L].$$

Proof.($\Rightarrow$) Suppose $L = \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)$. Since $\mathrm{Aut}(E/L)$ is a subgroup of the finite group $\mathrm{Aut}(E/k)$ (and therefore a finite subgroup of $\mathrm{Aut}(E)$), 2.4.4 implies that

$$|\mathrm{Aut}(E/L)| = [E : \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)] = [E : L].$$

($\Leftarrow$) For the contrary we assume that $|\mathrm{Aut}(E/L)| = [E : L]$. By 2.4.4 again we have that

$$[E : L] = |\mathrm{Aut}(E/L)| = [E : \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)].$$

Since, by (2.4), $L \subseteq \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)$, 1.1.4 gives us that

$$[E : L] = \underbrace{[E : \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)]}_{=[E:L]}[\mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big) : L] < \infty$$

and therefore $[\mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big) : L] = 1$ which means that $\mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big) = L$. ◇

Definition (2nd definition of Galois extensions - *finite* case). A *finite* field extension $k \leqslant E$ is called **Galois** if

$$|\mathrm{Aut}(E/L)| = [E : L] \tag{3.1}$$

for every subextension L of $k \leqslant E$. In this case we write $\mathrm{Gal}(E/k)$ for $\mathrm{Aut}(E/k)$ and call it the **Galois group** of the extension.

Example 3.1.2. The extension $\mathbb{R} \leqslant \mathbb{R}(i)$ of Ex. 2.3.2 is Galois because, as we saw, $\mathrm{Aut}(\mathbb{R}(i)/\mathbb{R})$ has only two elements (the identity function $z \mapsto z$ and the complex conjugation $z \mapsto \overline{z}$) and therefore

$$|\mathrm{Aut}(\mathbb{R}(i)/\mathbb{R})| = 2 = \partial m(i, \mathbb{R}) = [\mathbb{R}(i) : \mathbb{R}].$$ ◂

Counterexample 3.1.3. In the beginning of this section we saw that the condition (3.1) does not hold for the extensions $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{F}_2(t^2) \leqslant \mathbb{F}_2(t)$ so these are *not* Galois. ◂

But there is also a different path we can take to define Galois extensions, one that reveals more about these extensions and how their study arise naturally in Galois' work.

To give some motivation for the work that follows, lets see what it means for a *finite* and *simple* extension to be Galois using the definitions we have formulated so far. Since simple algebraic extensions are the building blocks of finite extensions, the next example will be useful to generalize the ideas to arbitrary extensions.

Example 3.1.4. Suppose $k \leqslant k(a)$ is a simple algebraic extension. We saw in 2.4.2 that

$$|\mathrm{Aut}(k(a)/k)| \leqslant [k(a) : k] = \partial m(a,k).$$

If $k \leqslant k(a)$ is Galois then $|\mathrm{Gal}(k(a)/L)| = [k(a) : L]$ for every subextension L and in particular

$$|\mathrm{Gal}(k(a)/k)| = [k(a) : k] = \partial m(a,k). \tag{3.2}$$

But we know that every $\sigma \in \mathrm{Gal}(k(a)/k)$ is determined by its action on a and $\sigma(a)$ is a root of $m(a,k)$. So by (3.2), there must be $\partial m(a,k)$ *distinct* elements in $\mathrm{Gal}(k(a)/k) \Leftrightarrow \sigma(a)$ takes *exactly* $\partial m(a,k)$ *distinct values*. In other words:

- *every* root of $m(a,k)$ *must lie in* $k(a)$ and
- there aren't any repetitions, i.e. *there are no multiple roots.*

It is not hard to see that the converse also holds. If every root of $m(a,k)$ lies in $k(a)$ and there are no multiple roots then

$$|\mathrm{Aut}(k(a)/k)| = \partial m(a,k) = [k(a) : k]$$

and the extension $k \leqslant F(k)$ is Galois. ◂

3.2 Normal extensions

In the last example, we saw that if a finite simple extension $k \leqslant k(a)$ is Galois then all the roots of $m(a,k)$ are inside $k(a)$. We give extensions with the suitably generalized property a name.

Definition. A field extension $k \leqslant E$ is **normal** if it is algebraic and $m(a,k)$ splits in E for every $a \in E$.

Example 3.2.1. If $k \leqslant E$ is an arbitrary field extension such that $[E : k] = 2$, then the extension is normal. First of all, the extension is finite hence algebraic. Let $a \in E \setminus k$.* Since $[E : k] = 2$, from

$$[E : k] = [E : k(a)][k(a) : k]$$

we get $E = k(a)$ and consequently $\partial m(a, k) = 2$. The minimal polynomial $m = m(a, k)$ has a root in E and has degree 2 so it splits over E. Since a was arbitrary, the extension is normal. ◂

Example 3.2.2. The extension $\mathbb{R} \leqslant \mathbb{R}(i)$ of Ex. 2.3.2 is normal since $[\mathbb{R}(i) : \mathbb{R}] = 2$. ◂

Counterexample 3.2.3. The extension $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2})$ of Ex. 2.3.4 is *not* normal. The two complex roots of $m(\sqrt[3]{2}, \mathbb{Q}) = x^3 - 2$ are not in $\mathbb{Q}$. ◂

Example 3.2.4. The extension $k \leqslant k_{sep}$ is normal. Take some $a \in k_{sep}$ and $m = m(a, k)$. If $a_1, \dots, a_r$ are the roots of m in the algebraic closure $\overline{k}$ of k, then every a_i is in k_{sep}. For $a_i \notin k_{sep}$ implies that a_i is not separable over k, i.e. $m(a_i, k)$ is not separable which is absurd since $m(a_i, k) = m$. ◂

Normal extensions have nice equivalent formulations that are sometimes more appropriate to work with, depending on the context.

Lemma 3.2.5. *Let $k \leqslant E$ be an algebraic extension. The following are equivalent*

1. *Every irreducible polynomial $p(x) \in k[x]$ that has a root in E splits.*
2. *E is normal over k.*
3. *E is the splitting field of a set of polynomials over k.*
4. *If $\tau : E \to \overline{E}$ is a k-homomorphism then $\tau(E) = E$.*
5. *If $k \leqslant L_1 \leqslant E \leqslant L_2$ is a tower of fields and $\sigma : L_1 \to L_2$ is a k-homomorphism, then $\sigma(L_1) \subseteq E$ and we can find some $\tau \in \mathrm{Aut}(E/k)$ that extends σ.*

Proof. (i)⇒(ii)⇒(iii): It is immediate. Every minimal polynomial is irreducible and E being normal over k implies that E is the splitting field of $\{m(a, k) : a \in E\}$.

* The case $a \in k$ is trivial.

(iii)⇒(iv): If E is the splitting field of some $S \subseteq k[x]$ then so is $\tau(E)$ in $\overline{E}$ by the Extension Theorem for splitting fields. But then both E and $\tau(E)$ are generated over k by the same roots. Hence $E = \tau(E)$.

(iv)⇒(v): Suppose $k \leqslant L_1 \leqslant E \leqslant L_2$ is a tower of fields and $\sigma : L_1 \to L_2$ is a k-homomorphism. Since $k \leqslant E$ is algebraic, so is $k \leqslant L_1$ and, therefore, so is $k \leqslant \sigma(L_1)$ (any $a = \sigma(x) \in \sigma(L_1)$ is the root of $\widetilde{\sigma}[m(x,k)]$). If we take

$$k' = \{x \in L_2 : x \text{ is algebraic over } k\}$$

and its algebraic closure $\overline{k'}$ then E, being a subextension of $k \leqslant k'$, can be embedded in $\overline{k'}$ so $\overline{k'} = \overline{E}$ by the uniqueness of algebraic closures. By the Extension Theorem for algebraic closures, there is some $\rho : \overline{k'} \to \overline{k'}$ that extends σ, i.e. $\rho|_{L_1} = \sigma$. Take

$$\tau = \rho|_E : E \to \overline{k'} = \overline{E}.$$

By our hypothesis, $\tau(E) = E$ so $\sigma(L_1) = \rho|_{L_1}(L_1) = \rho|_E(L_1) = \tau(L_1) \subseteq \tau(E) = E$, τ extends σ, and $\tau|k = \sigma|k = \mathrm{id}_k$; that is, $\tau \in \mathrm{Aut}(E/k)$.

(v)⇒(i): Take an irreducible polynomial $p(x) \in k[x]$ and a root $a \in E$ of p. Then we have the tower

$$k \leqslant k(a) \leqslant E \leqslant \overline{E}$$

and we can find another root $b \in \overline{E}$ of $p(x)$ and a k-homomorphism $\sigma : k(a) \to \overline{E}$ such that $\sigma(a) = b$ (define $f(a) \overset{\sigma}{\mapsto} f(b)$ for all $f(a) \in k(a)$). By our hypothesis, $\sigma\big(k(a)\big) \subseteq E$ so $b \in E$ and p splits in E. ◇

As a property of great interest, following 1.8.5, we also want to know how normality behaves under subextensions.

Proposition 3.2.6. *Let $k \leqslant L \leqslant E$ be a tower of fields. If $k \leqslant E$ is normal, then so is $L \leqslant E$.*

Proof. From 1.8.5, $L \leqslant E$ is algebraic. And if $m(a,k)$ splits in E then so does $m(a,L)$ since $m(a,L) | m(a,k)$ and $k[x]$ is a U.F.D. ◇

3.3 Separable extensions

We also saw that if $k \leqslant k(a)$ is a Galois extension then $m(a,k)$ has no multiple roots in $k(a)$. We will, as before, generalize this property to arbitrary extensions.

Definition. An irreducible polynomial $p(x) \in k[x]$ is called **separable over** k if it has no repeating roots in its splitting field. A polynomial $f(x) \in k[x]$ is **separable over** k if every one of its irreducible factors is separable. Otherwise, f is called **inseparable**.

Definition. An element $a \in E$ of an algebraic field extension $k \leqslant E$ is a **separable element over** k if $m(a,k)$ is separable over k. A **separable extension** is an *algebraic* field extension whose elements are all separable. Again an element that is not separable is called **inseparable** and an extension with inseparable elements is called **inseparable extension**.

Remark. An easy way to see if a polynomial is separable or not is by using the derivative criterion. For any polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

we define its **formal derivative** the usual way, namely

$$f'(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1.$$

It is easy to see now that $f(x)$ *is separable if and only if* $(f, f') = 1$.

Example 3.3.1. Every extension over a field of characteristic zero is separable. Suppose $k \leqslant E$ is an extension with $\mathrm{char}(k) = 0$ and let $a \in E$. If $m = m(a,k)$ had a multiple root b then $m(b) = 0$ and $m'(b) = 0$. But m is also the minimal polynomial of b since it is irreducible; the relation $m'(b) = 0$ contradicts the minimality of ∂m. Therefore m is separable. ◂

Example 3.3.2. The extension $\mathbb{R} \leqslant \mathbb{R}(i)$ of Ex. 2.3.2 is separable since $\mathrm{ch}(\mathbb{R}) = 0$. ◂

Counterexample 3.3.3. The field extension $\mathbb{F}_2(t^2) \leqslant \mathbb{F}_2(t)$ of Ex. 2.3.5 is *inseparable*. As we saw, the minimal polynomial

$$m\big(t, \mathbb{F}_2(t^2)\big)(x) = x^2 - t^2 = (x-t)^2$$

has a double root. Observe that in this example, the characteristic is positive. ◂

Example 3.3.4. Suppose k is a field and $\overline{k}$ is the algebraic closure of k. We define the **separable closure** k_{sep} of k to be the compositum of all simple separable extensions of k in $\overline{k}$. Obviously, k_{sep} is a separable extension of k. ◀

It should come as no surprise that we want to study separability under subextensions.

Proposition 3.3.5. *For a tower of fields $k \leqslant L \leqslant E$, if $k \leqslant E$ is separable then so is $L \leqslant E$.*

Proof. From 1.8.5, $L \leqslant E$ is algebraic; if the roots of $m(a,k)$ are all simple then so are the roots of $m(a,L)$ since $m(a,L)|m(a,k)$. ◇

3.4 Galois extensions III

We are ready to give the last and most important definition of Galois extensions.

Using the new terminology we now have, we restate the result of Ex. 3.1.4: *a simple algebraic extension is Galois if and only if it is normal and separable*. It is not a surprise that this result also holds for arbitrary extensions.

First let's see how the transitivity results for algebraic, normal and separable extensions allow us to simplify the first definition of Galois extensions we gave.

Proposition 3.4.1. *Let $k \leqslant E$ be an algebraic extension. The following are equivalent*

1. $k = \mathrm{Fix}_E\big(\mathrm{Aut}(E/k)\big)$.
2. *The extension $k \leqslant E$ is both normal and separable.*

Proof. (i)⇒(ii): We will show that an arbitrary $a \in E$ is normal and separable. Take its minimal polynomial $m = m(a,k)$. If $\{a_1, \ldots, a_r\}$ are the roots of m in E, the set $S = \{\sigma a_i : \sigma \in \mathrm{Aut}(E/k)\}$ is finite and the polynomial

$$f(x) = \prod \big(x - \sigma(a_i)\big) \in E[x],$$

where the product is taken over the distinct elements of S, is fixed by any element of $\mathrm{Aut}(E/k)$. So the coefficients of f lie in $\mathrm{Fix}_E\big(\mathrm{Aut}(E/k)\big) = k$. We thus deduce that $m|f$ so m splits over k and has no multiple roots.

(ii)⇒(i): If $k \leqslant E$ is separable, then E is contained in k_{sep}. In that case every $\sigma \in \mathrm{Aut}(k_{sep}/k)$ satisfies $\sigma(E) \subseteq E$. Indeed, the extension is normal hence every $a \in E$ is normal and $\sigma(a)$ is a root of $m(a,k)$ and thus $\sigma(E) \subseteq E$.

We will show that every element not in k is moved by some automorphism. Given any $a \in E\backslash k$ we can find an element $\sigma \in \mathrm{Aut}(k_{sep}/k)$ with $\sigma(a) \neq a$ since k_{sep} is normal. But if σ preserves E, the restriction $\sigma|_E \in \mathrm{Aut}(E/k)$ and $\sigma|_E(a) \neq a$. So $\mathrm{Fix}_E\big(\mathrm{Aut}(E/k)\big) = k$ ◇

Now the above proposition enables us to restate the *first* definition of a Galois extension without the universal quantifier.

Corollary 3.4.2. *An algebraic extension $k \leqslant E$ is Galois if and only if $k = \mathrm{Fix}_E\big(\mathrm{Aut}(E/k)\big)$.*

Proof.(⇒) Immediate from the definition. Take $L = k$.

(⇐) If $k = \mathrm{Fix}_E\big(\mathrm{Aut}(E/k)\big)$ then the proposition tells us that $k \leqslant E$ is normal and separable. By the transitivity results, so is $L \leqslant E$ for every intermediate field L of $k \leqslant E$ and therefore, by the proposition again, $L = \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big)$ for every intermediate field L. ◇

Definition (3rd definition of Galois extensions). A field extension $k \leqslant E$ is called **Galois** if

$$k = \mathrm{Fix}_E\big(\mathrm{Aut}(E/k)\big).$$

In this case we write $\mathrm{Gal}(E/k)$ for $\mathrm{Aut}(E/k)$ and call it the **Galois group** of the extension.

For finite extensions we can still use the second equivalent definition and again, as a consequence of the previous proposition, we can drop the quantifier as well.

Once more, using the proposition and the transitivity results we have the most important result of this section.

Corollary 3.4.3. *An algebraic extension $k \leqslant E$ is Galois if and only if it is normal and separable.*

Proof. Immediate from Prop. 3.4.1 and Cor. 3.4.2. ◇

Definition (4th definition of Galois extensions). A field extension $k \leqslant E$ is called **Galois** if it is both normal and separable. In this case we write $\mathrm{Gal}(E/k)$ for $\mathrm{Aut}(E/k)$ and call it the **Galois group** of the extension.

Example 3.4.4. The extension $\mathbb{R} \leqslant \mathbb{R}(i)$ of Ex. 2.3.2 is Galois. ◂

Example 3.4.5. The separable closure k_{sep} of k is a Galois extension of k. By its definition, it is the maximal Galois extension of k in the sense that any other Galois extension of k is contained in k_{sep}. ◂

Counterexample 3.4.6. The extension $\mathbb{Q} \leqslant \mathbb{Q}(\sqrt[3]{2})$ of Ex. 2.3.4 is *not* normal hence *not* Galois. ◂

Counterexample 3.4.7. The extension $\mathbb{F}_2(t^2) \leqslant \mathbb{F}_2(t)$ of Ex. 2.3.5 is *not* separable hence *not* Galois. ◂

In view of the last definition, we finish with the last transitivity result (essentially a rephrasing of 3.2.6 and 3.3.5).

Corollary 3.4.8. *If $k \leqslant L \leqslant E$ is a tower of fields and $k \leqslant E$ is Galois, then so is $L \leqslant E$.*

Convention. From now on, when we refer to an automorphism group as Galois group we will always mean that the extension is Galois.

Chapter 4
The Fundamental Theorem

We have reached the first important classification theorem, the Fundamental Theorem of Galois Theory for *finite* Galois extensions. We will focus only on the part of the Fundamental Theorem that concerns the Galois correspondence since it is the *correspondence* we are mainly interested in.

Theorem 4.0.1 (Fundamental Theorem of Galois Theory for finite exte
For a finite Galois extension $k \leqslant E$, the Galois-Artin correspondence

$$\{L : \ k \leqslant L \leqslant E\} \rightleftarrows \{H : \ H \leqslant \mathrm{Gal}(E/k)\}$$

is bijective, i.e. the maps $\mathrm{Aut}(E/\bullet)$ *and* $\mathrm{Fix}_E(\bullet)$ *are mutual inverses, and order reversing.*

Proof. Immediate from Proposition 2.2.4, Corollary 2.4.5 and Corollary 3.4.3. ◇

Having established a bijective correspondence, the remaining part illustrates of the theorem how we can derive information about the extension using its Galois group and the Galois correspondence.

Theorem 4.0.2 (Fundamental Theorem of Galois Theory for finite exte
If L is a subextension of a finite Galois extension $k \leqslant E$, then $L \leqslant E$ is Galois and

$$[E : L] = |\mathrm{Gal}(E/L)| \quad \textit{and} \quad [L : k] = [\mathrm{Gal}(E/k) : \mathrm{Gal}(E/L)].$$

Moreover, the extension $k \leqslant L$ is normal if and only if $\mathrm{Gal}(E/L)$ *is a normal subgroup of* $\mathrm{Gal}(E/k)$*. In that case*

$$\mathrm{Gal}(L/k) \cong \mathrm{Gal}(E/k)/\mathrm{Gal}(E/L).$$

Proof. $L \leqslant E$ is Galois from 3.4.8. Therefore, from the definition of finite Galois extensions, we have

$$[E : L] = |\operatorname{Gal}(E/L)|$$

and, using Prop. 1.1.4, we get

$$[L : F] = \frac{[E : F]}{[E : L]} = \frac{|\operatorname{Gal}(E/F)|}{|\operatorname{Gal}(E/L)|} = [\operatorname{Gal}(E/F) : \operatorname{Gal}(E/L)]$$

where the last equality is Lagrange's* theorem for finite groups.

For the second assertion it is not hard to show that

$$\sigma \operatorname{Gal}(E/L)\sigma^{-1} = \operatorname{Gal}\big(E/\sigma(L)\big) \tag{4.1}$$

for all $\sigma \in \operatorname{Gal}(E/F)$. Indeed, given $\tau \in \operatorname{Gal}(E/L)$ and $x \in L$,

$$(\sigma\tau\sigma^{-1})\big(\sigma(x)\big) = (\sigma\tau)(x) = \sigma(x) \quad \forall \sigma \in \operatorname{Gal}(E/F)$$

so $\sigma \operatorname{Gal}(E/L)\sigma^{-1} \subseteq \operatorname{Gal}\big(E/\sigma(L)\big)$. Similarly,

$$\sigma^{-1} \operatorname{Gal}\big(E/\sigma(L)\big)\sigma \subseteq \operatorname{Gal}\big(E/\sigma^{-1}\sigma(L)\big) = \operatorname{Gal}(E/L)$$

which proves (4.1).

Suppose now that the extension $F \leqslant L$ is normal. To show that $\operatorname{Gal}(E/L)$ is a normal subgroup of $\operatorname{Gal}(E/F)$, it suffices to show that $\sigma(L) = L$ for all $\sigma \in \operatorname{Gal}(E/F)$ since we would then have

$$\sigma \operatorname{Gal}(E/L)\sigma^{-1} \overset{(4.1)}{=} \operatorname{Gal}\big(E/\sigma(L)\big) = \operatorname{Gal}(E/L).$$

Given $\sigma \in \operatorname{Gal}(E/F)$ and $a \in L$, $\sigma(a)$ is a root of $m(a, F)$ which is in L since $F \leqslant L$ is normal. So $\sigma(L) \subseteq L$. But σ is injective and the extensions are all finite. Hence $\sigma(L) = L$.

For the contrary, suppose the extension $F \leqslant L$ is normal. In that case, the restriction map

$$\bullet|_L : \operatorname{Gal}(E/F) \to \operatorname{Gal}(L/F) : \sigma \mapsto \sigma|_L$$

is a well defined group homomorphism. The kernel of this homomorphism is

$$\ker = \{\sigma \in \operatorname{Gal}(E/F) : \sigma|_L = \mathrm{id}_L\} = \operatorname{Gal}(E/L).$$

So $\operatorname{Gal}(E/L) \lhd \operatorname{Gal}(E/F)$. Furthermore, the map $\bullet|_L$ is surjective by the Isomorphism Extension Theorem. Therefore, by the First Isomorphism Theorem for Groups,

$$\operatorname{Gal}(L/F) \cong \operatorname{Gal}(E/F)/\operatorname{Gal}(E/L). \qquad \diamond$$

* Joseph-Louis Lagrange (1736–1813)

Chapter 5
Krull's Galois Theory

5.1 The Galois correspondence for infinite extensions

Let us now drop the finiteness assumption. Suppose $k \leqslant E$ is a possibly *infinite* but still *algebraic* field extension and consider the Galois correspondence

$$\{\text{subextensions } k \leqslant L \leqslant E\} \rightleftarrows \{\text{subgroups } H \leqslant \mathrm{Aut}(E/k)\}.$$

$$\begin{array}{ccc} E & & \mathrm{Aut}(E/k) \\ | & \xrightarrow[L \mapsto \mathrm{Aut}(E/L)]{\mathrm{Aut}(E/\bullet)} & | \\ L & & H \\ | & \xleftarrow[\mathrm{Fix}_E(H) \hookleftarrow H]{\mathrm{Fix}_E(\bullet)} & | \\ k & & \{\mathrm{id}_E\} \end{array}$$

Proposition 2.2.4 did not assume any finiteness, so the correspondence is *order reversing* even for infinite extensions. Furthermore, the inclusions

$$H \subseteq \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big) \ \forall H \leqslant \mathrm{Aut}(E/k) \tag{2.3}$$

and

$$L \subseteq \mathrm{Fix}_E\big(\mathrm{Aut}(E/L)\big) \ \forall L : k \leqslant L \leqslant E \tag{2.4}$$

are still valid since they are independent of the degree of the extension too.

Our aim once more is to examine for which extensions $k \leqslant E$, $\mathrm{Aut}(E/\bullet)$ and $\mathrm{Fix}_E(\bullet)$ are mutually inverse, i.e. for which extensions the relations

$$H = \mathrm{Aut}\big(E/\mathrm{Fix}_E(H)\big) \ \forall H \leqslant \mathrm{Aut}(E/k) \tag{2.1}$$

and

$$L = \mathrm{Fix}_E\left(\mathrm{Aut}(E/L)\right) \ \forall L : k \leqslant L \leqslant E \tag{2.2}$$

hold. We have already seen that (2.2) holds if and only if the extension is normal and separable and both normality and separability are defined independently of the degree of an extension. So we turn our focus to (2.1).

5.2 The Galois group of an infinite extension

We saw in Cor. 2.4.5 that when $k \leqslant E$ is a finite extension, $\mathrm{Aut}(E/k)$ is also finite and (2.1) holds.

But when we drop the finiteness assumption, the theory breaks. First of all, $\mathrm{Aut}(E/k)$ is no longer finite. To prove this, we first need a variant of the *Primitive Element Theorem*. The proof we present is taken from [**37**].

Proposition 5.2.1 (The Primitive Element Theorem). *If $k \leqslant E$ is a finite separable extension, then there is some element $\gamma \in E$ such that $E = k(\gamma)$.*

Such an element γ is called a **primitive element**, hence the name of the theorem.

Proof. Since $k \leqslant E$ is finite, there are $m \in \mathbb{N}$ and $a_1, \dots, a_m \in E$ such that $E = k(a_1, \dots, a_m)$.

If k is finite then so is E and it is easy to check that any generator γ of the cyclic group E^* will do.

If k is infinite we proceed with induction on m. Suppose $E = k(a, b)$ and that $m(a, k)$ and $m(b, k)$ have roots $a = a_1, \dots, a_r$ and $b = b_1, \dots, b_s$ in some extension of E (such extension can be constructed using Prop. 1.9.3 twice in a row). Using the separability of a and b we can prove that $\gamma = a + \lambda b$ is a primitive element for all $\lambda \in k$ except when

$$\lambda = \frac{a_i - a}{b - b_j}, \ \ i = 1, \dots, r, \ j = 1, \dots, s$$

which are finitely many exceptions in an infinite field. The inductive step is now immediate. ◇

Proposition 5.2.2. *If $k \leqslant E$ is an infinite Galois extension then* $\mathrm{Gal}(E/k)$ *is also infinite.*

Proof. If $G = \mathrm{Gal}(E/k)$ were finite, say $|G| = n$ for some $n \in \mathbb{N}$, then $\sigma^n = \mathrm{id}_E$ for all $\sigma \in G$, which implies that

$$\sigma(a^n) = \sigma^n(a) = \mathrm{id}_E(a) = a \ \forall a \in E. \tag{5.1}$$

Therefore, if $a \in E$ then (using the fact that a is algebraic over k since $k \leqslant E$ is Galois)

$$[k(a) : k] = \partial m(a, k) \leqslant n$$

because if $\partial m(a,k) > n$, any $\sigma \in G$ acting on $m(a,k)(a) = 0$ yields a monic polynomial which is zero at a and whose degree is smaller than $\partial m(a,k)$ (any power of a greater than n becomes less than n from (5.1)) - a contradiction. But if $[k(a) : k] \leqslant n$ for all $a \in E$, then we can choose an element $a_0 \in E$ whose degree over k, $[k(a_0) : k] = m_0 \leqslant n$ is maximal among the degrees of elements of E. In that case we can prove that $E = k(a_0)$. Indeed, if not, there would be some $b_0 \in E \setminus k(a_0)$. Looking at the tower of fields

$$k \leqslant k(a_0) \leqslant k(a_0, b_0) \leqslant E$$

we conclude that $k \leqslant k(a_0, b_0)$ is separable (since $k \leqslant E$ is Galois, hence separable and using 3.3.5). Moreover, $[k(a_0) : k] = m_0$ maximal and finite, and since b_0 is algebraic over k, it is also algebraic over $k(a_0)$. That means, using 1.8.1, that $k(a_0) \leqslant k(a_0, b_0)$ is also of finite degree. From 1.1.4, we conclude that

$$[k(a_0, b_0) : k] = [k(a_0, b_0) : k(a_0)][k(a_0) : k] > m_0$$

But from the primitive element theorem, as $k \leqslant k(a_0, b_0)$ is separable and finite, there exists some $\gamma \in E$ such that $k(a_0, b_0) = k(\gamma)$. The above arguments imply that

$$[k(\gamma) : k] > m_0$$

which contradicts the maximality of m_0 among the degrees of elements of E. Therefore $E = k(a_0)$; under these circumstances, E is a finitely generrated, algebraic extension of k, hence finite over k - a contradiction.$\diamond$

Our informal discussion in 2.3.3 should have prepared us to understand why infinite Galois groups do not behave well; they have too many subgroups so not every subgroup can arise as an automorphism group of some intermediate field.

Counterexample 5.2.3. Consider the extension

$$\mathbb{Q} \leqslant \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \ldots) = E$$

constructed by adjoining the roots of all equations of the form $x^2 - p = 0$ where p is a prime number. It is easy to see that $\mathbb{Q} \leqslant E$ is normal (by definition) and separable (we are in characteristic 0), hence Galois. So (2.2) holds. It is in (2.1) where the correspondence breaks because $\mathrm{Aut}(E/\bullet)$ is *not* onto, i.e. not every subgroup can arise as an automorphism group. Let's see why.

We will focus on extensions of $\mathbb{Q}$ of degree 2 inside E, i.e. **quadratic number fields** inside E. It is not hard to see what a quadratic number field looks like in general. If $[L : \mathbb{Q}] = 2$ then $L \neq \mathbb{Q}$ and we can find some $a \in L \setminus \mathbb{Q}$. From

$$[L : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = [L : \mathbb{Q}] = 2,$$

we can deduce that $L = \mathbb{Q}(a)$. Therefore

$$2 = [L : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}] = \partial m(a, \mathbb{Q})$$

so $m(a, \mathbb{Q}) = x^2 + d$ or, equivalently, $a = \sqrt{d}$ for some square-free $d \in \mathbb{Q}$. The converse also holds; namely, any field of the form $\mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Q}$ square-free, is an algebraic number field. So there are countably many quadratic number fields, hence *countably many quadratic number fields inside* E.

By Theorem 4.0.2, any quadratic field L is mapped through $\mathrm{Aut}(E/\bullet)$ to a subgroup $\mathrm{Gal}(E/L)$ of index

$$[\mathrm{Gal}(E/\mathbb{Q}) : \mathrm{Gal}(E/L)] = [L : \mathbb{Q}] = 2$$

in $\mathrm{Gal}(E/\mathbb{Q})$ and only quadratic number fields can be mapped to subgroups of $\mathrm{Gal}(E/\mathbb{Q})$ of index 2.

But, any $\sigma \in G = \mathrm{Gal}(E/\mathbb{Q})$ is determined by its action on the square roots and, since $\sigma(\sqrt{p})$ is also a root of $m(\sqrt{p}, \mathbb{Q}) = x^2 - p$, we have

$$\sigma(\sqrt{p}) = \pm\sqrt{p} \quad \forall \text{ prime } p.$$

We can therefore deduce that, as groups, $G \cong \prod_{i=1}^{\infty} \mathbb{Z}_2$. Indeed the map

$$\begin{aligned} \Phi : \prod_{i=1}^{\infty} \mathbb{Z}_2 &\to \mathrm{Gal}(E/\mathbb{Q}) \\ (a_i)_{i=1}^{\infty} &\mapsto \sigma : \sigma(\sqrt{p_i}) = (-1)^{a_i}\sqrt{p_i}, \end{aligned}$$

where p_i is the i-th prime number, is easily seen to be a group isomorphism. So G is uncountable.* Moreover, G is an infinite dimensional vector space over $\mathbb{Z}_2$, which implies that its dual space $\mathrm{Hom}_{\mathbb{Z}_2}(G, \mathbb{Z}_2)$ is uncountable.** The kernels of all these (uncountably many) linear functionals are subgroups of G of index 2. So we have *uncountably many subgroups of G of index* 2.

Since there only countably many extensions of $\mathbb{Q}$ of degree 2 inside E but uncountably many subgroups of G of index 2, $\mathrm{Aut}(E/\bullet)$ cannot be onto and (2.1) cannot hold. ◂

So when the extension is infinite, its Galois group is also infinite and the Galois correspondence may not be bijective as the previous example suggests. A natural question to ask is whether there are infinite Galois extensions for which the correspondence *is* bijective. We shall see that answer is *no*.

We therefore need to find a way to distinguish among the subgroups that *can* arise as Galois groups and the subgroups that *cannot*.

This is done by defining a topology on $\mathrm{Gal}(E/k)$, the *Krull topology*,† which distinguishes between "good" and "bad" subgroups. In particular, the subgroups that are *closed* with respect to the Krull topology will be exactly those which arise as Galois groups.

Convention. For the rest of this section, fix $k \leqslant E$ a (possibly infinite) Galois extension and $G = \mathrm{Gal}(E/k)$ its Galois group. We define

$$\mathscr{L} = \{L : \ k \leqslant L \leqslant E, \ [L : k] < \infty \text{ and } k \leqslant L \text{ Galois}\}$$

to be the set of subextensions L of $k \leqslant E$ for which $k \leqslant L$ is a finite Galois extension and

$$\mathscr{N} = \{N \leqslant G : \ N = \mathrm{Gal}(E/L), \ L \in \mathscr{L}\}$$

to be the set of subgroups of G that can arise as Galois groups of subextensions $L \in \mathscr{L}$.

---

* Another famous argument of Cantor says that the set of all binary sequences is uncountable (its cardinality equals the continuum); see [**26**].

** If V is an infinite dimensional vector space over a field F and V^* is its dual space, then $\dim_F V^* > \dim_F V$; see [**30**].

† Named after Wolfgang Krull (1899-1971) who was the first to develop the theory for infinite Galois extensions in [**24**].

Proposition 5.2.4. *The set*

$$\mathcal{B} = \{\sigma N : \ \sigma \in G, \ N \in \mathcal{N}\}$$

constitutes a basis for a topology $\mathcal{T}$ *on* $\mathrm{Gal}(E/k)$.

Proof. In other words, we need to show that the set

$$\mathcal{T} = \left\{ \bigcup_{i \in I} \sigma_i N_i : \ \sigma_i \in G, \ N \in \mathcal{N} \right\}$$

constitutes a topology on G. Obviously $\emptyset, G \in \mathcal{T}$. For the latter consider any arbitrary extension $L \in \mathcal{L}$ with Galois group $N = \mathrm{Gal}(E/L) \in \mathcal{N}$ and write

$$G = \bigcup_{\sigma \in G} \sigma N.$$

Moreover, it is apparent that the union of an arbitrary family of elements of $\mathcal{T}$ is again in $\mathcal{T}$. It remains to show that given a finite number of elements of $\mathcal{T}$, their intersection also lies in $\mathcal{T}$. It suffices to prove our claim for only two elements of $\mathcal{T}$. From the set-theoretic equality

$$\left(\bigcup_{i \in I} \sigma_i N_i \right) \cap \left(\bigcup_{j \in J} \tau_j N_j \right) = \bigcup_{i,j} \left(\sigma_i N_i \cap \tau_j N_j \right)$$

and the fact that $\mathcal{T}$ is closed under unions, it suffices to prove that $\sigma_1 N_1 \cap \sigma_2 N_2 \in \mathcal{T}$ for any two elements of $\mathcal{B}$. In fact we will prove that this intersection lies in $\mathcal{B} \subseteq \mathcal{T}$. Observe that if $\tau \in \sigma_1 N_1 \cap \sigma_2 N_2$ then

$$\sigma_1 N_1 \cap \sigma_2 N_2 = \tau N_1 \cap \tau N_2 = \tau (N_1 \cap N_2) \in \mathcal{B}$$

since $N_1 \cap N_2 \in \mathcal{N}$. Indeed, if

$$N_1 = \mathrm{Gal}(E/L_1) \text{ and } N_2 = \mathrm{Gal}(E/L_2), \ L_1, L_2 \in \mathcal{L}$$

then $\mathrm{Gal}(E/L_1 L_2) = N_1 \cap N_2$ since

$$\begin{aligned} \rho \in N_1 \cap N_2 &\iff \rho|_{L_1} = \mathrm{id} \ \text{ and } \rho|_{L_2} = \mathrm{id} \\ &\iff L_1 \subseteq \mathrm{Fix}_E(\rho) \text{ and } L_2 \subseteq \mathrm{Fix}_E(\rho) \\ &\iff L_1 L_2 \subseteq \mathrm{Fix}_E(\rho) \iff \rho \in \mathrm{Gal}(E/L_1 L_2) \end{aligned}$$

which completes the proof ($F \leqslant L_1 L_2$ is again a finite, Galois extension).$\diamond$

Definition. The topology $\mathscr{T}$ defined in the previous proposition is called the **Krull topology**.

Example 5.2.5. The Krull topology of a finite Galois extension is the discrete topology; that is, every subgroup of its Galois groups is both open and closed.* Indeed, if $k \leqslant E$ is finite with Galois group G then $E \in \mathscr{L}$ and $\mathrm{Gal}(E/E) = \{\mathrm{id}_E\} \in \mathscr{N}$. Therefore

$$\{\sigma\} = \sigma\,\mathrm{Gal}(E/E) \in \mathscr{B} \quad \forall \sigma \in G.$$

That is, every singleton is open (and in particular basic); hence every subset of G is clopen. ◂

The converse of the above claim also holds.

Lemma 5.2.6. *The Krull topology is discrete if and only if the extension is finite.*

Proof. See [**38**], Proposition 3.12.8. ◇

We will now prove our claim that the closed subsets of G in the Krull topology are exactly those that can arise as Galois groups of subextensions.

This result and the above lemma imply that *there are no infinite Galois extensions for which* (2.1) *holds*.

Proposition 5.2.7. *If $H \subseteq G$ then $\mathrm{Gal}(E/\mathrm{Fix}_E(H)) = \overline{H}$, the closure of H in the Krull topology.*

Proof. To simplify the notation, set $H' = \mathrm{Gal}(E/\mathrm{Fix}_E(H))$. In order to prove that $\overline{H} = H'$ we need to show two inclusions. For the inclusion $\overline{H} \subseteq H'$, we need only prove that H' is closed. Indeed, we have already established that $H \subseteq H'$ which implies that $\overline{H} \subseteq \overline{H'}$; therefore, if we prove that H' is closed then $H' = \overline{H'}$ and the inclusion $\overline{H} \subseteq \overline{H'}$ becomes $\overline{H} \subseteq H'$ which is exactly what we want. To prove that H' is closed take some $\sigma \in G \setminus H'$. Now

$$\sigma \in G \setminus H' \Rightarrow \exists a \in \mathrm{Fix}_E(H') : \ \sigma(a) \neq a$$

* A set that is both open and closed with respect to some topolgy is called **clopen**.

Take some $L \in \mathscr{L}$ such that $a \in L$ and set $N = \mathrm{Gal}(E/L) \in \mathscr{N}$. The set σN is a basic open set containing σ and is disjoint from H' since

$$\tau(a) = a \ \forall \tau \in N \text{ and } \sigma\tau(a) = \sigma(a) \neq a$$

Therefore, $G \setminus H'$ is open, hence H' is closed. For the other inclusion, $H' \subseteq \overline{H}$, set $L = \mathrm{Fix}_E(H)$ and let $\sigma \in H'$ and $N \in \mathscr{N}$. If $K = \mathrm{Fix}_E(N) \in \mathscr{L}$ and $H_0 = \{\tau|_K : \tau \in H\} \leqslant \mathrm{Gal}(K/k)$, then, since

$$\mathrm{Fix}_K(H_0) = \mathrm{Fix}_K(H) \cap K = L \cap K,$$

the Fundamental Theorem for the finite Galois extensions implies that $H_0 = \mathrm{Gal}(K/K \cap L)$. Now $\sigma \in H'$, so $\sigma|_L = \mathrm{id}_L$ and $\sigma|_K \in H_0$. Therefore, there is some $\tau \in H$ such that $\tau|_K = \sigma|_K$. Thus $\sigma^{-1}\tau \in \mathrm{Gal}(E/K) = N$, so $\tau \in \sigma N \cap H$. In other words, every basic open neighborhood σN of $\sigma \in H'$ meets H, so $\sigma \in \overline{H}$. ◇

From the above proposition, the Galois correspondence between

$$\{\text{subextensions } k \leqslant L \leqslant E\} \rightleftarrows \{\text{closed subgroups } H \leqslant \mathrm{Aut}(E/k)\}$$

is bijective. Hence we have proved the analogue of Theorem 4.0.1 for infinite extensions.

Theorem 5.2.8 (Fundamental Theorem of Galois Theory for infinite ext
If $k \leqslant E$ is a (possibly infite) Galois extension, the correspondence

$$\{L : k \leqslant L \leqslant E\} \rightleftarrows \{H : H \leqslant \mathrm{Gal}(E/k),\ H \text{ closed}\}$$

is bijective, i.e., the maps $\mathrm{Aut}(E/\bullet)$ *and* $\mathrm{Fix}_E(\bullet)$ *are mutual inverses, and order reversing.*

Proof. Immediate from Proposition 2.2.4, Corollary 2.4.5 and Proposition 5.2.7. ◇

We can also establish an analogue of Theorem 4.0.2.

Theorem 5.2.9 (Fundamental Theorem of Galois Theory for infinite ext
If L is a subextension of $k \leqslant E$, then $L \leqslant E$ is Galois and if $H = \mathrm{Gal}(E/L)$ then

$$|G : H| < \infty \Leftrightarrow H \text{ is open} \Leftrightarrow [L : k] < \infty$$

and in that case, $|G : H| = [L : k]$. *Moreover, the extension* $k \leqslant L$ *is normal (hence Galois) if and only if* $\mathrm{Gal}(L/k)$ *is a normal subgroup of* $\mathrm{Gal}(E/k)$. *In that case*

$$\mathrm{Gal}(L/k) \cong \mathrm{Gal}(E/k)/\mathrm{Gal}(E/L)$$

If we endow $\mathrm{Gal}(E/k)/\mathrm{Gal}(E/L)$ *with the quotient topology then the above isomorphism is a homeomorphism.*

We must note however, that in order to prove the second part of the Fundamental Theorem we need more information on the Krull topology. In particular we need

Proposition 5.2.10. *The set* G *endowed with the Krull topology is Hausdorff, compact and totally disconnected.*

The proofs of these propositions are given in the next paragraph. A last remark is in order before we proceed.

Remark. Krull's Galois Theory is a generalization of the Galois Theory for finite extensions. If $k \leqslant E$ is a finite Galois extension then the Krull topology on $\mathrm{Gal}(E/k)$ is the discrete topology; hence every subgroup is clopen and we retrieve Theorems 4.0.1 and 4.0.2.

5.3 Profinite topological groups

The previous discussion of infinite Galois Theory is somewhat elementary and probably raises more questions than it answers. One might wonder for example how did we come up with the Krull topology or even why did we use topology to begin with.

To see how our work in infinite Galois Theory comes naturally, we need the notion of a *profinite topological group*. For a more elaborate study of profinite groups and how they are related to Galois Theory we refer the reader to [**49**].

Definition. A **topological group** is a group G endowed with a topology such that the maps

$$\cdot : G \times G \to G : (g,h) \mapsto gh \quad \text{and} \quad {}^{-1} : G \to G : g \mapsto g^{-1}$$

are continuous. A **homomorphism of topological groups** is a *group homomorphism* that is also *continuous*.

Thus a topological group is a group that is also a topological space for which the group structure and the topology are compatible in the sense described above and a homomorphism of topological groups is a map that respects both the group structure and the topology.

Example 5.3.1. If $k \leqslant E$ is a Galois extension, $\mathrm{Gal}(E/k)$ endowed with the Krull topology is a topological group.

If the extension is finite, so is $\mathrm{Gal}(E/k)$ and therefore its Krull topology is the discrete topology. Hence the maps $(g,h) \mapsto gh$ and $g \mapsto g^{-1}$ are (trivially) continuous.

The interesting case is when $k \leqslant E$ is infinite. Suppose $(g,h) \in G \times G$ and take a basic open neighborhood $gh\,\mathrm{Gal}(E/L)$ of gh. Then, the basic open neighborhood $g\,\mathrm{Gal}(E/L) \times h\,\mathrm{Gal}(E/L)$ of (g,h) is contained in $gh\,\mathrm{Gal}(E/L)$ through the map $(g,h) \mapsto gh$. The element (g,h) was arbitrary, therefore $(g,h) \mapsto gh$ is continuous.

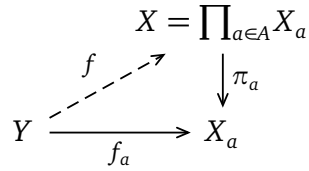
Similarly, if $g \in G$ and $g^{-1}\,\mathrm{Gal}(E/L)$ is a basic open neighborhood of g^{-1}, then the open neighborhood $g\,\mathrm{Gal}(E/L)$ of g is contained in $g^{-1}\,\mathrm{Gal}(E/L)$ through the map $g \mapsto g^{-1}$. The element g was arbitrary, therefore $g \mapsto g^{-1}$ is also continuous. ◂

Proposition 5.3.2. *A subgroup of topological group is a topological group.*

Proof. Let G be a topological group and $H \leqslant G$. Recall from General Topology that *the restriction of a continuous map is continuous*. Therefore the restrictions $\cdot|_H : H \times H \to G$ and ${}^{-1}|_H : H \to G$ are continuous. But since H is a subgroup of G, their range is H, i.e. $\cdot|_H : H \times H \to H$ and ${}^{-1}|_H : H \to H$ so H is a topological group. ◇

Proposition 5.3.3. *The product $G = \prod_{a\in A} G_a$ of a family $\{G_a\}_{a\in A}$ of topological groups is a topological group when endowed with the product topology.*

Before proving that, recall from General Topology that if $\{X_a\}_{a\in A}$ is a family of topological spaces, then $X = \prod_{a\in A} X_a$ endowed with the product topology is a topological space. X (with projections $\pi_a : X \to X_a$) has the universal property that for every other topological space Y and every family $f_a : Y \to X_a$ of continuous maps, there is a unique continuous map $f : Y \to X$ so that the following diagram commutes.



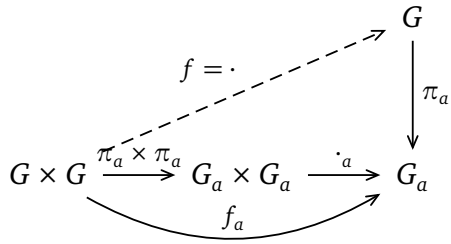
Proof. First of all, recall from Group Theory that $G = \prod_{a\in A} G_a$ is a group with multiplication defined componentwise, i.e.

$$(g_a)_{a\in A} \cdot (h_a)_{a\in A} = (g_a \cdot h_a)_{a\in A}.$$

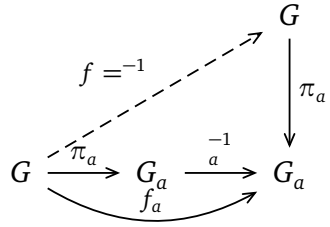
To show that $\cdot : G \times G \to G$ is continuous take $Y = G \times G$ and f_a to be the composition

$$G \times G \xrightarrow{\pi_a \times \pi_a} G_a \times G_a \xrightarrow{\cdot_a} G_a \qquad \diamond$$

in the universal property of the product topology. Then $\cdot$ is the unique map f, hence continuous.



Similarly, to prove that $^{-1} : G \to G$ is continuous take $Y = G$ and f_a to be the composition $G \xrightarrow{\pi_a} G_a \xrightarrow{^{-1}_a} G_a$.



We are not interested in topological groups in general but rather in a spacial kind of topological groups, profinite groups.

Definition. An **inverse system of topological groups** is a pair of families $(\{G_a\}_{a\in A}, \{\phi_b^a\}_{a\leqslant b\in A})$ indexed by some *directed set*[a] $(A, \leqslant)$, where $\{G_a\}_{a\in A}$ is a family of topological groups and for every $a \leqslant b \in A$, ϕ_b^a is a continuous group homomorphism $G_b \to G_a$ such that

1. $\phi_a^a = \mathrm{id}_{G_a}$
2. $\phi_c^a = \phi_b^a \circ \phi_c^b$ for all $a \leqslant b \leqslant c \in A$.

We shall write (G_a, ϕ_b^a) for an inverse system of topological groups.

[a] Recall that a **directed set** is a partially ordered set $(A, \leqslant)$ with the property that for every $a, b \in A$ there is some $c \in A$ such that $a \leqslant c$ and $b \leqslant c$.

Definition. Suppose (G_a, ϕ_b^a) is an inverse system of topological groups. The **inverse limit** of the system is the subset of the product $\prod_{a\in A} G_a$ consisting of sequences (g_a) such that $\phi_b^a(g_b) = g_a$ for all $a \leqslant b$. The inverse limit is usually denoted by $\varprojlim G_a$.

Lemma 5.3.4. *If (G_a, ϕ_b^a) is an inverse system of topological groups, then the inverse limit $\varprojlim G_a$ is a subgroup of $\prod_{a\in A} G_a$.*

Proof. First of all, $\varprojlim G_a \neq \emptyset$. Indeed, $(e_a)_{a\in A} \in \varprojlim G_a$ since $\phi_b^a : G_b \to G_a$ is a group homomorphism and therefore sends $e_b \mapsto e_a$ for every $a \leqslant b$.

Furthermore, for every $(g_a), (h_a) \in \varprojlim G_a$,

$$(g_a) \cdot (h_a)^{-1} = (g_a) \cdot (h_a^{-1}) = (g_a \cdot h_a^{-1}) \in \varprojlim G_a$$

because for every $a \leqslant b$,

$$\phi_b^a(g_b \cdot h_b^{-1}) = \phi_b^a(g_b) \cdot \phi_b^a(h_b^{-1}) = \phi_b^a(g_b) \cdot \phi_b^a(h_b)^{-1} = g_a h_a^{-1}.$$

Therefore $\varprojlim G_a \leqslant \prod_{a\in A} G_a$. ◇

Corollary 5.3.5. *The inverse limit $\varprojlim G_a$ is a topological group.*

Proof. Immediate from Propositions 5.3.2 and 5.3.3, and the previous lemma. ◇

Profinite topological groups are a special kind of inverse limit.

Definition. The inverse limit of a system of *finite* topological groups (endowed with the *discrete* topology) is called a **profinite** (**topological**) **group**.

Corollary 5.3.6. *Profinite groups are topological groups.*

Example 5.3.7. Every finite topological group G is profinite. Just take (G_a, ϕ_b^a) to be (G, id_G). ◀

Example 5.3.8. The Galois group $\mathrm{Gal}(E/k)$ of a Galois extension $k \leqslant E$ is a profinite group.

If the extension is finite then so is $\mathrm{Gal}(E/k)$ and the assertion follows from the previous example.

Suppose the extension is infinite. The pair $(\mathscr{L}, \subseteq)$ is a directed set. Indeed, for every $L_1, L_2 \in \mathscr{L}$, their compositum $L_3 = L_1 L_2 \in \mathscr{L}$ (for $i = 1, 2$, L_i is a finite Galois extension of k, so it is generated by a finite set S_i of elements whose minimal polynomials are separable and split over k; L_3 is then generated by $S_1 \cup S_2$ and therefore $L_3 \in \mathscr{L}$) and $L_1 \subseteq L_3$, $L_2 \subseteq L_3$.

For every $L \in \mathscr{L}$ take the finite group $\mathrm{Gal}(L/k)$ endowed with the discrete topology and for every $L_1 \subseteq L_2 \in \mathscr{L}$ consider the restriction homomorphism

$$\phi_{L_2}^{L_1} : \mathrm{Gal}(L_2/k) \to \mathrm{Gal}(L_1/k) : \sigma \mapsto \sigma|_{L_1} \quad \forall \sigma \in \mathrm{Gal}(L_2/k).$$

Thus we have an inverse system $(\mathrm{Gal}(L/k), \phi_{L_2}^{L_1})$ of topological groups. We will show that

$$\mathrm{Gal}(E/k) \cong \varprojlim \mathrm{Gal}(L/k),$$

that is, they are isomorphic as groups and homeomorphic as topological spaces.

Define

$$\begin{aligned} \vartheta : \mathrm{Gal}(E/k) &\to \varprojlim \mathrm{Gal}(L/k) \\ \sigma &\mapsto (\sigma|_L)_{L \in \mathscr{L}}. \end{aligned}$$

The map ϑ is obviously well defined.

ϑ is also a group homomorphism since

$$\sigma|_L \tau|_L = (\sigma\tau)|_L.$$

We will show that the kernel of ϑ is trivial so ϑ is injective. Suppose $\sigma \in \mathrm{Gal}(E/k)$ such that $\sigma|_L = \mathrm{id}_L$ for all $L \in \mathscr{L}$. Then $\sigma = \mathrm{id}_E$. Indeed, for every $x \in E$ take the splitting field L_x of $m(x,k)$. It is immediate that $L_x \in \mathscr{L}$. The hypothesis $\sigma|_{L_x} = \mathrm{id}_{L_x}$ implies that $\sigma(x) = \sigma|_{L_x}(x) = x$. The element $x \in E$ was arbitrary, therefore $\sigma = \mathrm{id}_E$.

To show that ϑ is surjective take some $(\tau_L) \in \varprojlim \mathrm{Gal}(L/k)$ and define

$$\sigma : E \to E : \sigma(x) = \tau_{L_x}(x) \quad \forall x \in E.$$

It is a trivial procedure to show that $\sigma \in \mathrm{Gal}(E/k)$ and, by its definition, $\vartheta(\sigma) = (\sigma|_L) = (\tau_L)$.

ϑ is continuous and open. The basic open sets of $\mathrm{Gal}(E/k)$ are of the form σN where $N = \mathrm{Gal}(E/L) \in \mathscr{N}$ for some $L \in \mathscr{L}$ and $\sigma \in \mathrm{Gal}(E/k)$. The topology of $\varprojlim \mathrm{Gal}(L/k)$ is, by definition of the product and the subspace topology, the smallest topology that contains the sets $\pi_L^{-1}(\{\tau\})$ where $L \in \mathscr{L}$, $\pi_L : \mathrm{Gal}(E/k) \to \mathrm{Gal}(L/k)$ is the usual projection (restriction) and $\tau \in \mathrm{Gal}(L/k)$. We compute

$$\begin{aligned}
\vartheta^{-1}\big(\pi_L^{-1}(\{\tau\})\big) &= \{\sigma \in \mathrm{Gal}(E/k) : \sigma|_L = \tau\} \\
&= \{\sigma \in \mathrm{Gal}(E/k) : \sigma \text{ extends } \tau \text{ to } E\} \\
&= \bigcup_{\sigma \in \mathrm{Gal}(E/k)} \sigma\,\mathrm{Gal}(E/L)
\end{aligned}$$

which is a union of open sets in $\mathrm{Gal}(E/k)$, hence open. So ϑ is continuous. Moreover,

$$\begin{aligned}
\vartheta(\sigma N) &= \{(\sigma\tau_H)_{H\in\mathscr{L}} : \tau_H|_L = \mathrm{id}_{H\cap L}\} \\
&= \{(\tau_H)_{H\in\mathscr{L}} : \sigma^{-1}\tau_H|_L = \mathrm{id}_{H\cap L}\} \\
&= \{(\tau_H)_{H\in\mathscr{L}} : \tau_H|_L = \sigma|_{H\cap E}\} \\
&= \pi_H^{-1}(\{\sigma|_E\})
\end{aligned}$$

so the image of a basic open set is open in $\varprojlim \mathrm{Gal}(L/k)$. Therefore ϑ is open. ◂

The Krull topology has some nice properties which can now be almost immediately derived.

Recall from General Topology that a space X is called **compact** if every open cover of X has a finite subcover, **Hausdorff*** if for every $x, y \in X$

* Named after Felix Hausdorff (1868–1942).

there are open sets V_x, V_y such that $x \in V_x$, $y \in V_y$ and $V_x \cap V_y = \emptyset$, and **totally disconnected** if its only connected components are the singletons. It is immediate that *every finite space equipped with the discrete topology is compact, Hausdorff and totally disconnected*. The not (at all) obvious results we will need are

1. *Any product of compact spaces is compact.**
2. *Any product of Hausdorff spaces is Hausdorff.*
3. *Any product of totally disconnected spaces is totally disconnected.*
4. The subspace of a compact space need not be compact; for example $[0,1]$ is compact while $(0,1)$ is not. However, *a closed subspace of a compact space is compact.*
5. *The subspace of a Hausdorff space is Hausdorff.*
6. *The subspace of a totally disconnected space is totally disconnected.*
7. *If $f, g : X \to Y$ are continuous maps and Y is Hausdorff, then the set*
$$\{x \in X : f(x) = g(x)\}$$
is a closed subset of X.

Lemma 5.3.9. *$\varprojlim G_a$ is a closed subset of $\prod_{a\in A} G_a$.*

Proof. Write $\varprojlim G_a$ as

$$\begin{aligned}\varprojlim G_a &= \{(g_a) \in \prod_{a\in A} G_a : \phi_b^a(g_b) = g_a \ \forall b > a\} \\ &= \bigcap_{b>a} \{(g_a) \in \prod_{a\in A} G_a : \phi_b^a \circ \pi_b(g_b) = \pi_a(g_a)\}\end{aligned}$$

and apply (vii) for $f = \phi_b^a \circ \pi_b$ and $g = \pi_a$ as continuous functions $\prod_{a\in A} G_a \to G_a$. $\varprojlim G_a$ is then closed as the intersection of closed subsets of $\prod_{a\in A} G_a$. ◇

Corollary 5.3.10. *The Galois group of an extension $k \leqslant E$ endowed with the Krull topology is a compact, Hausdorff and totally disconnected space.*

We can now prove the second part of the Fundamental Theorem of infinite Galois Theory.

* This is Tychonoff's theorem, named after Andrey Nikolayevich Tikhonov (1906-1993).

Theorem 5.3.11 (Fundamental Theorem of Galois Theory for infinite ex
If L is a subextension of $k \leqslant E$, then $L \leqslant E$ is Galois and if $H = \mathrm{Gal}(E/L)$ then

$$|G : H| < \infty \iff H \text{ is open} \iff [L : k] < \infty$$

and in that case, $|G : H| = [L : k]$. Moreover, the extension $k \leqslant L$ is normal (hence Galois) if and only if $\mathrm{Gal}(L/k)$ is a normal subgroup of $\mathrm{Gal}(E/k)$. In that case

$$\mathrm{Gal}(L/k) \cong \mathrm{Gal}(E/k)/\mathrm{Gal}(E/L)$$

If we endow $\mathrm{Gal}(E/k)/\mathrm{Gal}(E/L)$ with the quotient topology then the above isomorphism is a homeomorphism.

Proof. Suppose $[G : H] = m < \infty$. If the left cosets of H in G are $\{H, g_1H, \ldots, g_mH\}$ then

$$G \setminus H = \bigsqcup_{i=1}^{m} g_iH$$

which is a finite union of closed subsets of G. Indeed, $H = \mathrm{Gal}(E/L)$ is closed as the Galois group of some subextension and the map

$$\cdot|_{\{g_i\}\times H} : \{g_i\} \times H \to gH \subseteq G : h \mapsto g_ih$$

is bijective and continuous as the restriction of a continuous map. Therefore g_iH is closed for every $i = 1, \ldots, m$. Thus $G \setminus H$ is closed which implies that H is open.

Suppose now that H is an open subgroup of G. Then $\mathrm{id}_E \in H$ so there is some basic open neighborhood $N = \mathrm{Gal}(E/S) \in \mathscr{N}$, $S \in \mathscr{L}$, so that $\mathrm{id}_E \in N \leqslant H$. In that case,

$$\begin{aligned} N \leqslant H &\Rightarrow \mathrm{Fix}_E(H) \leqslant \mathrm{Fix}_E(N) \\ &\Rightarrow \underbrace{\mathrm{Fix}_E\big(\mathrm{Gal}(E/L)\big)}_{=L \text{ since } E/L \text{ is Galois}} \leqslant \underbrace{\mathrm{Fix}_E\big(\mathrm{Gal}(E/S)\big)}_{=S \text{ since } E/S \text{ is Galois}} \\ &\Rightarrow L \leqslant S \end{aligned}$$

and since $S \in \mathscr{N}$, that is, S is finite over k, so is L.

Lastly, suppose that $[L : k] < \infty$. Take E_f to be the splitting field of all the minimal polynomials of the generators of L over k. Then $E_f \in \mathscr{L}$

and $k \leqslant L \leqslant E_f \leqslant E$. Set $N = \mathrm{Gal}(E/E_f) \in \mathscr{N}$. Similarly to the proof of the fundamental theorem for finite extensions, the map

$$\vartheta_{E_f} : \mathrm{Gal}(E/k) \to \mathrm{Gal}(E_f/k) : \sigma \mapsto \sigma|_{E_f}$$

is a surjective (from Lemma 3.2.5) group homomorphism with $\ker \vartheta_{E_f} = N$. From the 1st Isomorphism Theorem we have

$$\mathrm{Gal}(E_f/k) \cong \mathrm{Gal}(E/k)/\mathrm{Gal}(E/E_f) = G/N.$$

The inclusion $L \leqslant E_f$ now implies that $N = \mathrm{Gal}(E/E_f) \leqslant \mathrm{Gal}(E/L) = H$ and therefore

$$[G : H] \leqslant [G : N] = |G/N| = |\mathrm{Gal}(E_f/k)|$$

and $|\mathrm{Gal}(E_f/k)| < \infty$ since $k \leqslant E_f$ is finite. In particular, using the Isomorphism Theorems for Groups, Lagrange's theorem, the fundamental theorem of Galois theory for finite extensions and the multiplicativity of the degrees, we get

$$[G : H] = [G/N : H/N] = \frac{|G/N|}{|H/N|} = \frac{[E_f : k]}{[E_f : L]} = [L : k].$$

Suppose $H \lhd G$. We will show that $k \leqslant L$ is a Galois extension. It is obviously separable by the transitivity of separable extensions. It remains to show that it is normal. Let $a \in L \setminus k$ and $m = m(a, k)$ be its minimal polynomial. $k \leqslant E$ is Galois; let $b \in E$ be another root of m. We will show that $b \in L$. From the Isomorphism Extension Theorem, there is some $\sigma \in \mathrm{Gal}(E/k)$ such that $\sigma(a) = b$. Since $H \lhd G$, we have $\sigma^{-1}\tau\sigma \in H$ for every $\tau \in H$. Therefore

$$\tau(b) = \tau\sigma(a) = \sigma \underbrace{\sigma^{-1}\tau\sigma}_{\in \mathrm{Gal}(E/L)}\Big(\underbrace{a}_{\in L}\Big) = \sigma(a) = b.$$

In other words, $b \in \mathrm{Fix}_E(H) = \mathrm{Fix}_E\big(\mathrm{Gal}(E/L)\big) = L$.

For the contrary, suppose that $k \leqslant L$ is Galois. Then

$$\vartheta : G = \mathrm{Gal}(E/k) \to \mathrm{Gal}(L/k) : \sigma \mapsto \sigma|_L$$

is a surjective group homomorphism with $\ker \vartheta_L = H \lhd G$ (using analogous arguments as before, when we defined ϑ_{E_f}).

By the 1st Isomorphism Theorem, there is an isomorphism

$$\nu : G/H = \mathrm{Gal}(E/k)/\mathrm{Gal}(E/L) \xrightarrow{\cong} \mathrm{Gal}(L/k).$$

We will show that ν is a homeomorphism.

The basic open sets of $\mathrm{Gal}(L/k)$ as a subspace of G are

$$\mathscr{B}' = \{\tau\,\mathrm{Gal}(L/K)\}$$

where $k \leqslant K \leqslant L$ with $k \leqslant K$ being a finite Galois extension and $\tau \in \mathrm{Gal}(L/k)$. For every such basic open set, $\mathrm{Gal}(E/K) \in \mathscr{N}$ since $E \in \mathscr{L}$ and therefore

$$\vartheta^{-1}\big(\tau\,\mathrm{Gal}(L/K)\big) = \sigma\,\mathrm{Gal}(E/K)$$

for some $\sigma \in \mathrm{Gal}(E/k)$ that extends τ. So ϑ is continuous.

Moreover, ϑ is closed. Indeed, G is compact and $\mathrm{Gal}(L/k)$ is Hausdorff (because G is), so any closed subset of the compact G is compact and is therefore mapped through the continuous ϑ to a compact subset of the Hausdorff space $\mathrm{Gal}(L/k)$. Recall from General Topology that *any compact subset of a Hausdorff space is compact* and the assertion follows.

Now it follows at once that the isomorphism

$$\nu : G/H = \mathrm{Gal}(E/k)/\mathrm{Gal}(E/L) \xrightarrow{\cong} \mathrm{Gal}(L/k)$$

induced by ϑ is a homeomorphism by the definition of the quotient topology on G/H. ◇

Bibliography

[Art98] E. Artin. *Galois Theory*. Edited and supplemented with a selection on applications by Arthur N. Milgram. Mineola, New York: Dover Publications Inc., 1998.

[Axl15] S. Axler. *Linear Algebra Done Right*. 3 **edition**. Undergraduate Texts in Mathematics. Springer, 2015.

[Bat84] J. R. Batista. *Field Extensions and Galois Theory*. 1 **edition**. **volume** 22. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1984.

[BJ01] F. Borceux **and** G. Janelidze. *Galois Theories*. 1 **edition**. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2001.

[Bro] K. Brown. *The Primitive Element Theorem*. Cornell University, October 2010. Available at: `http://pi.math.cornell.edu/~kbrown`.

[Cona] K. Conrad. *Infinite Galois Theory*. 2020. A draft for a mini-course given at Connecticut Summer School in Number Theory. Available at: `https://ctnt-summer.math.uconn.edu`.

[Conb] K. Conrad. *The Galois Correspondence*. Available at: `https://kconrad.math.uconn.edu`.

[DF04] D. S. Dummit **and** R. M. Foote. *Abstract Algebra*. 3 **edition**. John Wiley **and** Sons Inc., 2004.

[Edw84] H. M. Edwards. *Galois Theory*. 1 **edition**. **volume** 101. Graduate Texts in Mathematics. Springer-Verlag New York, 1984.

[FR97] B. Fine **and** G. Rosenberger. *The Fundamental Theorem of Algebra*. 1 **edition**. Undergraduate Texts in Mathematics. Springer-Verlag New York, 1997.

[How06] J. M. Howie. *Fields and Galois Theory*. 1 **edition**. Springer Undergraduate Mathematics Series. Springer-Verlag London, 2006.

[Jar14] F. Jarvis. *Algebraic Number Theory*. 1 **edition**. Springer Undergraduate Mathematics Series. Springer International Publishing, 2014.

[Kie71] B. M. Kiernan. "The Development of Galois Theory from Lagrange to Artin". **in***Archive for History of Exact Sciences*: 8.1/2 (**december** 1971), **pages** 40–154.

[Kru28] W. Krull. "Galoissche Theorie der unendlichen algebraischen Erweiterungen". **in***Mathematische Annalen*: 100 (1928), **pages** 687–698

[Lan05] S. Lang. *Undergraduate Algebra*. 3rd ed. **volume** 211. Undergraduate Texts in Mathematics. Springer New York, 2005.

[Mil] J. S. Milne. *Fields and Galois Theory*. Available at: `www.jmilne.org/math`.

[Mor96] P. Morandi. *Field and Galois Theory*. 1 **edition**. **volume** 167. Graduate Texts in Mathematics. Springer-Verlag New York, 1996.

[Mos94] Y. Moschovakis. *Notes on Set Theory*. 1 **edition**. Undergraduate Texts in Mathematics. Springer-Verlag New York, 1994.

[Mun00] J. R. Munkres. *Topology*. 2 **edition**. Prentice Hall, 2000.

[Neu13] P. M. Neumann. *The mathematical writings of Évariste Galois*. corrected 2nd ed. Heritage of European Mathematics. European Mathematical Society Publishing House, 2013.

[Niv47] Ivan Niven. "A simple proof that π is irrational". **in***Bulletin of the American Mathematical Society*: 53.6 (1947), **pages** 509–509.

[Rot98] J. Rotman. *Galois Theory*. 2 **edition**. Universitext. Springer-Verlag New York, 1998.

[Ste15] I. Stewart. *Galois Theory*. 4 **edition**. CRC Press, 2015.

[Szaa] T. Szamuely. *Galois Theory after Galois*. An informal survey of some modern aspects of Galois Theory. Available at: `http://pagine.dm.unipi.it/tamas`.

[Szab] T. Szamuely. *Galois Theory: Past and Present*. 2010-11. Slides from a colloquium lecture on the occasion of the 200th anniversary of Galois' birth. Available at: `http://pagine.dm.unipi.it/tamas`.

[Sza09] T. Szamuely. *Galois Groups and Fundamental Groups*. 1 **edition**. **volume** 117. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2009.

[Wae91] B.L. van der Waerden. *Algebra. Volume I*. 1st edition. Springer New York, 1991.