GALOIS THEORY

v1, ©03 Jan 2021 Alessio Corti[*]

Contents

[*] This text is an account of Galois theory as presented in my MP11 lecture course at Imperial College London (Easter terms 2018, 2019, 2020 & 2021). I thank the students who attended those courses, and my class assistant Giulia Gugiatti for correcting many mistakes.

1 Elementary theory of field extensions

1.1 The category of fields and finite extensions

There is a **category** of fields where: **objects** are fields, **morphisms** are **field (homo-)morphisms**.

Remark 1. Every morphism $\sigma\colon K \to L$ of fields is *injective*.

For two fields K, L, we denote by $\mathrm{Emb}(K, L)$ the set of field morphisms from K to L. We call the elements of the set $\mathrm{Emb}(K, L)$ *emb*eddings — to remind ourselves constantly that all morphisms of fields are injective.

In Galois theory, there is almost always a given field k — called the *ground field* — in the background, and we take it for granted that all fields in sight come with a given morphism $\sigma\colon k \to K$. In this situation we omit σ from the notation and we just say that $k \subset K$ is an **extension** of fields.

We almost always work with a variant of the category of fields where we *fix* a ground field k and we work in the category whose **objects** are extensions of k, and for two objects $k \subset K$ and $k \subset L$, **morphisms** are understood as embeddings *over* k, that is, embeddings that restrict to the identity of k. We denote by

$$\mathrm{Emb}_k(K, L) = \{f \in \mathrm{Emb}(K, L) \mid \forall a \in k,\ f(a) = a\}$$

the set of field embeddings $f\colon K \to L$ over k, and we call the elements of this set k-embeddings of K in L.[1]

1.2 Degree and the tower law

An important philosophical observation The earlier you understand this, the better. The field structure is baroque: a field has **two** operations and they satisfy this weird distributive property. On the other hand, vector spaces, groups and their representations are simpler structures and hence they are easier to work with: there are fewer ways to go down a rabbit-hole and hence it is easier to keep on the right path.

Remark 2. If $K \subset L$ is a field extension, then L is a K-**vector space**.

Definition 3. The *degree* of an extension $K \subset L$ is the quantity:

$$[L : K] = \dim_K L$$

(the dimension of L as a vector space over K).

A field extension is *finite* if $[L : K] < \infty$.

[1] The reason for the expression "over k" is that at the blackboard or on paper we paint an element $\sigma \in \mathrm{Emb}_k(K, K)$ like so:

$$\begin{tikzcd}
K \arrow[rr, "\sigma"] & & K \\
& k \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

with K *above* (over) k.

Remark 4. (a) If $[L : K] = 1$ then $K = L$;

(b) If $k \subset K$ is finite, then every element of $\mathrm{Emb}_k(K, K)$ is surjective,[2] hence it is an isomorphism. In other words $\mathrm{Emb}_k(K, K) = \mathrm{Aut}_k(K, K)$ is the **group** of *automorphisms* of K over k. The k-vector space K is a k-**linear representation** of this group.

From now on in these notes, unless explicitly stated otherwise, all field extensions are understood to be finite.

Definition 5. If $k \subset K$ is a (finite) extension of fields, then the group $G = \mathrm{Emb}_k(K, K)$ is called the *Galois group* of the extension.

Theorem 6 (tower law)**.** *For a tower*[3] $K \subset L \subset M$ *of extensions*[4]

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

□

Remark 7. In general the degree $[L : K]$ of a field extension depends on the embedding $x \colon K \to L$ that we use to put K in L. When we want to be precise about this we may write $\deg(x)$, the degree of x. For example, the embedding $x \colon K(t) \to K(t)$ where $x(t) = t^d$ has degree $\deg(x) = d$. We could not get away with a poor choice of notation if it were not that in the context of interest to us, the degree $[L : K]$ in fact only depends on K and L and not on the embedding $x \colon K \to L$. Indeed, if all fields are (finite!) extensions of a fixed ground field k, then for $k \subset K$, $k \subset L$, if $x \colon K \to L$ is a k-embedding, then by the tower law:

$$\deg(x) = \frac{[L : k]}{[K : k]}$$

1.3 Elementary theory of field extensions

Elsewhere in this text I use the following facts freely and refer to them by bold numerals like so [**ix**].

The topics are: **minimal polynomials** [**i-v**]; **splitting fields** [**vi-ix**]; **separable polynomials** [**x-xiii**].

[2] This follows immediately from the rank-nullity formula.

[3] The situation of two extensions $K \subset L$ and $L \subset M$ is called a "tower." The reason for this expression is that at the blackboard or on paper we tend to paint this vertically as a two-storey tower:

$$\begin{tikzcd} M \\ L \arrow[u] \\ K \arrow[u] \end{tikzcd}$$

The tower pictured here only has two stories but you can easily imagine a multi-storey tower.

[4] **On punctuation at the end of displayed formulas** I have been typesetting mathematics for a very long time. It is likely that I have thought about the rules of punctuation at the end of displayed formulas longer and harder than you. The main difficulty is that there are too many cases. I have decided that I never put punctuation at the end of displayed formulas. This rule has the double advantage that it is simple and it is easy to follow consistently. We are not discussing this.

1.3.1 Minimal polynomials

(i) For $K \subset L$, all $a \in L$ have a *minimal polynomial* $f_a = f \in K[X]$: by definition, f is the unique *monic* generator of the kernel ideal of the evaluation-at-a homomorphism $\varphi_a = \varphi\colon k[X] \to L$. By definition, the ring $K[a] \subset L$ is the image of φ. The homomorphism φ induces by passing to the quotient a ring isomorphism

$$[\varphi]\colon K[X]/(f) \xrightarrow{\cong} k[a]$$

Because $[\varphi]$ is (by construction) injective, and because L is a field, hence as a ring it is an integral domain, it follows that $k[X]/(f)$ is also an integral domain, and hence (f) is a prime ideal, and hence f is *irreducible.* It follows from this that $k[X]/(f)$ is a field, and hence $k[a] \subset L$ is a field and $k[a] = k(a)$ is the smallest subfield of L that contains a.

(ii) Conversely, given an irreducible $f \in K[X]$ there is a field extension $K \subset K(a) = K[X]/(f)$ such that $a = [x]$ is a root of f. If f is also monic, then f is the minimal polynomial of a;

(iii) Let $K \subset K(a)$ be as in [**i**] or [**ii**] and let $f \in K[X]$ be the minimal polynomial of a. For all extensions $K \subset L$, there is a canonical bijection:

$$\{b \in L \mid b \text{ is a root of } f\} \xrightarrow{=} \operatorname{Emb}_K\left(K(a), L\right)$$

that maps a root b to the unique K-embedding $\varphi\colon K(a) \to L$ such that $\varphi(a) = b$;

(iv) In [**i**] and [**ii**] $[K(a) : K] = \deg f$;

(v) If $K \subset L \subset M$ and $a \in M$ then the minimal polynomial of a over L divides the minimal polynomial of a over K.

1.3.2 Splitting fields

(vi) For all $f \in K[X]$ — not necessarily irreducible — there is a field extension $K \subset L$ such that:

(a) The polynomial f splits completely in $L[X]$;

(b) $L = K(a_1, \dots a_n)$ where the a_i are the roots of f in L.

An extension $K \subset L$ satisfying properties (a) and (b) is called a *splitting field* of f.

(vii) Let $f \in K[x]$ be a polynomial, and let

(a) $K \subset M$ be a field extension in which f splits completely, and

(b) $K \subset E = K(a_1, \dots, a_m)$ a field extension generated by roots a_i of f,

then the set $\operatorname{Emb}_K(E, M)$ is not empty. It follows from this that any two splitting fields of $f \in K[X]$ are K-isomorphic; it is important to understand that the isomorphism is not canonical, but it sends a root of f to a root of f.

(viii) If $K \subset L$ is a splitting field of a polynomial $f \in K[X]$ then the group $G = \mathrm{Emb}_K(L, L)$ is a subgroup of the symmetric group on the roots of f. If, in addition, $f \in K[X]$ is **irreducible**, then this group acts **transitively** on the roots;

(ix) Let K be a field. The following are equivalent for $f, g \in K[X]$:

(a) The polynomials f, g are coprime as elements of $K[X]$;

(b) There exists an extension $K \subset L$ such that the polynomials f, g are coprime as elements of $L[X]$;

(c) For all extensions $K \subset L$, the polynomials f, g are coprime as elements of $L[X]$;

(d) For all extensions $K \subset L$, the polynomials f, g have no common root in L;

(e) There exists an extension $K \subset L$ in which: (I) both f and g split completely, and (II) f and g have no common root.

1.3.3 Separable polynomials and the Jacobian criterion

(x) By definition a polynomial $f \in K[X]$ is *separable* if it has $n = \deg f$ distinct roots (in a — and hence by [**vii**] in all — splitting field $K \subset L$). The **Jacobian criterion**: a polynomial f is separable if and only if f and Df (the *derivative*[5] of f) are coprime;

(xi) An irreducible polynomial $f \in K[X]$ is not separable if and only if (a) K has characteristic $p > 0$ and (b) there is a polynomial (necessarily irreducible) $h \in K[X]$ such that $f(X) = h(X^p)$;

(xii) For $K \subset L$, an element $a \in L$ is *separable over* K if the minimal polynomial $f \in K[X]$ of a over K is a separable polynomial;

(xiii) If $k \subset K \subset L$ and $a \in L$ is separable over k, then by [**v**] it is also separable over K.

2 Axiomatics

The following correspond roughly to Grothendieck's axioms for a Galois category. The only nontrivial ones are Axiom 1, Axiom 4 and Axiom 5. The proof is postponed till Sec. 5.

Axiom 1 Fix a field k. The category of algebraic field extensions $k \subset K$ finite over k has an initial object (the field k) and for all pairs of objects $k \subset K$ and $k \subset L$, $\mathrm{Emb}_k(K, L)$ is finite.[6]

[5] For all fields K there exists a derivation $D\colon K[X] \to K[X]$ uniquely specified by the properties:

(1) D is K-linear, that is, for all $a, b \in K$ and $f, g \in K[X]$ $D(af + bg) = aDf + bDg$,

(2) D satisfies the Leibnitz rule, that is, for all $f, g \in K[X]$ $D(fg) = (Df)g + fDg$.

[6] In fact, it is shown in Lemma 18 that $|\mathrm{Emb}_k(K, L)| \leq [K : k]$.

Axiom 2 Every morphism is injective. Also: every k-morphism from K to K is an isomorphism, that is, $\mathrm{Emb}_k(K, K)$ is a group. For all fields Ω the (right) action of $\mathrm{Emb}_k(K, K)$ on $\mathrm{Emb}_k(K, \Omega)$ is free.[7]

Axiom 3 Fibered products exist. (These are just "intersections" in a bigger field.) Also, "framed" pushouts exist. (If $x_1 \colon K \hookrightarrow L_1$, $x_2 \colon K \hookrightarrow L_2$ are contained in a bigger field Ω, then it makes sense to take the "product"—which in fact categorically is a pushout—$L_1L_2 \subset \Omega$: this is the subfield of Ω generated by L_1 and L_2 applying all field operations; alternatively it is the smallest subfield of Ω containing both L_1, L_2.)

Axiom 4 For all pairs of finite extensions $K \subset L$, $K \subset M$ there is a field extension $K \subset \Omega$, and a commutative diagram:[8]

$$\begin{tikzcd}
 & L \arrow[dr] & \\
K \arrow[ur] \arrow[dr] & & \Omega \\
 & M \arrow[ur] &
\end{tikzcd}$$

Axiom 5 For every field L and finite subgroup $G \leq \mathrm{Aut}\, L$, it makes sense to take the fixed field $K = L^G$, and the natural inclusion $G \hookrightarrow \mathrm{Emb}_K(L, L)$ is an isomorphism.[9]

3 Fundamental Theorem

The aim of this section is to state and prove the Fundamental Theorem of Galois theory from the axioms.

Definition 8. $k \subset K$ is *normal* if: For all Ω any two k-embeddings x_1, $x_2 \colon K \to \Omega$ differ by a k-automorphism of K. More formally, for all $x \in \mathrm{Emb}_k(K, \Omega)$, the naturally induced

$$x_\star \colon \mathrm{Emb}_k(K, K) \to \mathrm{Emb}_k(K, \Omega) \quad \text{defined as: } x_\star \colon \sigma \mapsto x \circ \sigma$$

[7] $f \colon K \to \Omega$ is injective if for all pairs of morphisms g_1, $g_2 \colon L \to K$, $f \circ g_1 = f \circ g_2$ implies $g_1 = g_2$. Now $f \in \mathrm{Emb}_k(K, \Omega)$ is fixed by some $g \in \mathrm{Emb}_k(K, K)$ if and only if $f \circ g = f \circ \mathrm{id}_K$ and then, because f is injective, $g = \mathrm{id}_K$.

[8] This field has no universal property and it is not unique. For example consider $K = \mathbb{Q}$, $L = M = \mathbb{Q}[X]/(X^3 - 2)$. We can take $\Omega = \mathbb{Q}(\sqrt[3]{2})$, $i_1 = i_2 \colon L \to \Omega$ both mapping $[X]$ to $\sqrt[3]{2}$, but we can also take $\Omega = \mathbb{Q}\left(\sqrt[3]{2}, \mathtt{i}\sqrt{3}\right)$, with $i_1 \colon L \to \Omega$ mapping $[X]$ to $\sqrt[3]{2}$ and $i_2 \colon L \to \Omega$ mapping $[X]$ to $\frac{-1+\mathtt{i}\sqrt{3}}{2}\sqrt[3]{2}$. This example shows that the intersection and product of L and M in Ω are not determined (even up to noncanonical isomorphism) by L and M. This axiom substitutes for the non-existent fibered co-product. Indeed the tensor product of rings $K \otimes_k L$ is not a field.

[9] This is half the Fundamental Theorem. This axiom corresponds exactly to Grothendieck's axiom (G5) for a Galois category stating "F [...] commutes with taking the quotient by a finite group action." Recall that, in Grothendieck, F is the fibre functor: for fields $F(K) = \mathrm{Emb}_k(K, \Omega)$ where Ω is an algebraic closure of k. Suppose that G is a finite group acting on K, then by naturality G acts on $F(K)$ by composing on the left. (And in fact the axioms imply that this action is free.) Axiom (G5) then states $F(K^G) = F(K)/G$. Counting elements we obtain $[K^G : k] = \frac{[K:k]}{|G|}$ and using the tower law then $[K : K^G] = |G|$. Even Grothendieck sneaks half the Fundamental Theorem into an axiom!

is bijective.[10]

In simpler words, $k \subset K$ is normal if and only if for all pairs of k-embeddings $x_1, x_2 \colon K \to \Omega$, we have

$$x_1(K) \subset x_2(K)$$

Informally: no matter where I go I can not "displace" K away from itself.

Lemma 9. *Splitting fields [**vi**] are normal.*

Proof. Let $k \subset K$ be a splitting field of the polynomial $f \in k[X]$, $K \subset \Omega$ and $x \colon K \to \Omega$ a k-embedding. We aim to prove that $x(K) \subset K$. If $a \in K$ is a root of f, then $x(a) \in \Omega$ is also a root of f, and hence $x(a) \in K$. But K is generated by roots of f, hence $x(K) \subset K$. □

The following statement is immediate from the definition:

Lemma 10. *Suppose given $k \subset K \subset L$: If $k \subset L$ is normal, then $K \subset L$ is normal.* □

Example 11. For given extensions $k \subset K \subset L$:

(1) If $k \subset L$ is normal, it does not follow that $k \subset K$ is normal. For an example, consider $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ the splitting field of the polynomial $f(X) = X^3 - 2 \in \mathbb{Q}[X]$;

(2) If $k \subset K$ and $K \subset L$ are normal, it does not follow that $k \subset L$ is normal. For an example consider $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $L = K(\sqrt{\sqrt{2}}) = \mathbb{Q}(\sqrt[4]{2})$.

Definition 12. $k \subset K$ is *separable* if: For every tower of subfields

$$k \subset K_1 \subsetneq K_2 \subset K$$

there exist: a field Ω, and at least two distinct K_1-embeddings $x, y \colon K_2 \to \Omega$.[11]

The slogan is: $k \subset K$ is separable if embeddings separate subfields.

Lemma 13. *If $k \subset K$ is a splitting field of a separable polynomial [**x**], then $k \subset K$ is separable.*

Sketch of proof. This is Corollary 49, but that is not for some time, the result is not very difficult, and it is needed to make sense of the statement of the Fundamental Theorem, so I give a sketch now, with details to be discussed later.

In Definition 43 we define the separable degree $[K : k]_s$ of an extension $k \subset K$ to be the number of elements of the set $\mathrm{Emb}_k(K, \Omega)$ of k-embeddings of K into a field Ω such that $k \subset \Omega$ is a normal extension that also contains K. In Sec. 9 it is shown that the

[10] The function $(x, \sigma) \mapsto x \circ \sigma$ is in fact a right group action $X \times G \to G$, where $X = \mathrm{Emb}_k(K, \Omega)$ and $G = \mathrm{Emb}_k(K, K)$. Axiom 2 states that this action is free. An extension $k \subset K$ is normal if and only if, for all Ω, $X = \mathrm{Emb}_k(K, \Omega)$ is a G-torsor.

[11] This definition substitutes for Grothendieck's axiom (G6) for a Galois category (Stating that if $F(u)$ is an isomorphism then u is an isomorphism). The category of separable field extensions is a Galois category in the sense of Grothendieck but the category of all extensions (separable and inseparable) is not.

separable degree is well-defined and that it satisfies the tower law. Note that, by Lemma 18, $[K:k]_s \leq [K:k]$.

It follows from the tower law that if $[K:k]_s = [K:k]$ then $k \subset K$ is separable.

Now if a is separable over k (this just means that the minimal polynomial of a over k is separable), then by [**iii**]: $[k(a):k]_s = [k(a):k]$. Now if $k \subset K$ is a splitting field of a separable polynomial $f \in k[X]$ then $K = k(a_1, \dots, a_m)$ where the a_i are roots of f. We break up the extension $k \subset K$ into a sequence of primitive extensions:

$$k \subset k(a_1) \subset k(a_1, a_2) \subset \cdots \subset k(a_1, \dots, a_m) = K$$

where a_i is separable over k and hence also separable over $k(a_1, \dots, a_{i-1})$. By the tower laws for the ordinary and the separable degrees, $[K:k]_s = [K:k]$. □

The following is immediate from the definition:

Lemma 14. *For $k \subset K \subset L$, if $k \subset L$ is separable, then $K \subset L$ and $k \subset K$ are separable.* □

(The converse is also true, see Theorem 48(II).)

Theorem 15 (Fundamental Theorem of Galois theory)**.** *If $k \subset K$ is normal and separable then the correspondence between subfields and subgroups holds.*[12]

Proof. Write $G = \operatorname{Emb}_k(K, K)$ the *Galois group* of the extension. One defines functions:

$$\text{For } H \leq G: \quad H \mapsto H^\star = \big\{a \in K \mid \forall\, g \in H,\, g(a) = a\big\}$$

and

$$\text{For } k \subset L \subset K: \quad L \mapsto L^\dagger = \{g \in G \mid \forall\, a \in L,\, g(a) = a\}$$

and the task is naturally split into two halves:

First Half For all H, $(H^\star)^\dagger = H$. This is just Axiom 5;

Second Half For all L, $(L^\dagger)^\star = L$.

We need to prove the second half. Since $L \subset K$ is normal and separable, it is enough to show that $G^\star = k$.

Let $k \subset F = G^\star$; I show that for all $K \subset \Omega$, the set $\operatorname{Emb}_k(F, \Omega)$ consists of the obvious inclusion $F \subset K \subset \Omega$ and hence — because we are assuming that the extension is separable — it must be that $k = F$.

Indeed consider the tower $k \subset F \subset K \subset \Omega$. For clarity denote by $\iota_{F,\Omega}\colon F \to \Omega$ the inclusion in this tower and similarly all other inclusions in the tower. Consider $y \in \operatorname{Emb}_k(F, \Omega)$. By Lemma 16(B) below, there is $x \in \operatorname{Emb}_k(K, \Omega)$ such that $y = x|F$. Because $k \subset K$ is normal, there exists $\sigma \in \operatorname{Emb}_k(K, K)$ such that $x = \iota_{K,\Omega} \circ \sigma$. By construction of F $\sigma|F$ is the identity, and therefore $y = x|F = \iota_{F,\Omega}$. □

[12] In fact more is true, namely there is an **equivalence of categories** between the category of field extensions (intermediate between k and K) and the category of subgroups of the Galois group. This fact, essential though it is, is seldom pursued to the bitter end: for subgroups H_1, H_2 of G, what is the correct definition of $\operatorname{Mor}(H_1, H_2)$ that makes this equivalence work? An important consequence of the equivalence of categories is: given $k \subset L \subset K$, then $k \subset L$ is normal if and only if the corresponding subgroup $H \leq G$ (of elements that fix L) is a normal subgroup, AND, in that case, the Galois group of $k \subset L$ is the quotient group G/H.

Lemma 16. *Suppose that $k \subset K$ is normal. Then for all given towers:*

$$k \subset F \subset K \subset \Omega$$

we have:

(A) the natural composition $c\colon \mathrm{Emb}_k(F, K) \to \mathrm{Emb}_k(F, \Omega)$ (compose with the given inclusion $K \subset \Omega$) is surjective;

(B) the natural restriction $\rho\colon \mathrm{Emb}_k(K, \Omega) \to \mathrm{Emb}_k(F, \Omega)$ (restrict to the given subfield $F \subset K$) is surjective.

Remark 17. (i) (A) states that every k-embedding $x\colon F \to \Omega$ in fact lands F in K: $x(F) \subset K$. In other words, "F can never be moved out of K." When $F = K$, this is just the definition of $k \subset K$ normal.

(ii) The following statement is a striking consequence of (A). Suppose that $f \in k[X]$ is irreducible. Then: either f has no roots in K, or it splits completely in K. Indeed suppose that f has at least one root $a \in K$. Consider the tower $k \subset k(a) = F \subset K \subset \Omega$ were f splits completely in Ω. If b is a root of f in Ω, then we want to show that $b \in K$. But we know that there is a K-isomorphism $x\colon F \to k(b) \subset \Omega$ such that $x(a) = b$. By (A) $x(F) \subset K$ and hence $b \in K$.

(iii) (B) states that every k-embedding $x\colon F \to \Omega$ extends to a k-embedding $\widetilde{x}\colon K \to \Omega$:

$$\begin{tikzcd}
K \arrow[dr, dashed, "\widetilde{x}"] & \\
F \arrow[u] \arrow[r, "x"] & \Omega \\
k \arrow[u] \arrow[ur] &
\end{tikzcd}$$

(In fact, $\widetilde{x}$ lands K in itself, but let us leave this fact aside.)

The case $K = \Omega$ is especially significant: If $k \subset K$ is normal then every embedding $x\colon F \to K$ extends to an automorphism $\sigma\colon K \to K$ — a fact that was crucial in the proof of the Fundamental Theorem.

Another way to state this fact is to say that the **left** action

$$G \times \mathrm{Emb}_k(F, K) \to \mathrm{Emb}_k(F, K)$$

(given by composition: $(\sigma, x) \mapsto \sigma \circ x$) is transitive.

(iv) The following consequence of (B) is already known to us: if $f \in k[X]$ is irreducible and splits completely in K, then G acts transitively on the roots of f. To see this, just apply the above remark to $F = k(a)$ where a is any root of f in K.

(v) It is manifestly the case that, assuming as we are that $k \subset K$ normal, (B)$\Rightarrow$(A): Indeed, given $x\colon F \to \Omega$, extend it to $\widetilde{x}\colon K \to \Omega$, and then observe that by normality $\widetilde{x}(K) \subset K$ and hence a fortiori $x(F) \subset K$, that is, F landed in the given inclusion of K in Ω.

Proof. By Remark 17(v) we only need to prove (B). Let $x\colon F \to \Omega$: we want to show that x is the restriction of some $\widetilde{x}\colon K \to \Omega$. First, use Axiom 4 to construct a commutative diagram:

$$\begin{tikzcd}
K \arrow[r, dashed, "y_2"] & \widetilde{\Omega} \\
F \arrow[u] \arrow[r, "x"'] & \Omega \arrow[u, dashed, "z"']
\end{tikzcd}$$

Note that we have TWO k-embedding $K \to \widetilde{\Omega}$: one is $y_2\colon K \to \widetilde{\Omega}$ in the diagram above; the other is obtained composing z with the given inclusion $K \subset \Omega$:

$$y_1\colon K \subset \Omega \overset{z}{\to} \widetilde{\Omega}$$

It follows from the normality of $k \subset K$ that $y_2(K) \subset y_1(K) \subset z(\Omega)$. In other words, y_2 landed K in Ω, that is, it gave the sought-for extension $y_2 = \widetilde{x}$. □

4 Philosophical considerations

In teaching the course these were my aims:

(i) Work with finite extensions only; *avoid* constructing an algebraic closure. (Even if having one helps a great deal.) There should be no need of discussing infinite algebraic extensions if one is only interested in finite ones.

(ii) Discuss characteristic p and the phenomenon of inseparability. Develop the theory of Frobenius lifts and use these to give a transparent proof of the irreducibility of cyclotomic polynomials over $\mathbb{Q}$ (a shockingly deep theorem of Dedekind).

(iii) Avoid copying Emil Artin like everybody else does. Aim to follow Grothendieck in spirit: uncompromisingly express all important definitions and statements in pure categorical terms; have a clean set of axioms.

(iv) Most books spend a lot of time developing many things; the Fundamental Theorem comes at the very end when one has seen so much detail that one can not see what really makes it work. I wanted to do the opposite: prove the Fundamental Theorem as soon as possible and develop the theory later.

There are **three levels of abstraction**:

(i) At the beginning one is interested in polynomials and their roots and in proving that there is no general formula in radicals for the roots of polynomials of degree ≥ 5;

(ii) One then discovers that it is helpful to keep roots in the fields that they inhabit, and that one is interested only in those permutations of roots that are automorphisms of these fields;

(iii) The third level of abstraction is arrows in a category, and the discipline of phrasing everything in terms of these. My innovation in this course is to access this level and try to convince you of the benefits.

5 Proofs of the Axioms

5.1 Proofs of Axioms 1 and 4

Lemma 18 (Axiom 1)**.** *$\mathrm{Emb}_k(K, L)$ has at most $[K : k]$ elements.*

Proof. We know that [**iii, iv**] that in the case of a primitive extension $k \subset k(a)$ $\mathrm{Emb}_k(k(a), L)$ has at most $\deg f_a = [k(a) : k]$ elements, hence the statement is true in this case. We will reduce the general case to the primitive case by tower law and induction on the degree of the extension.[13] Pick $a \in K \setminus k$ (if there is no such a then we have nothing to do). Consider the tower $k \subset k(a) \subset K$. We have an obvious restriction map:

$$\rho \colon \mathrm{Emb}_k(K, L) \to \mathrm{Emb}_k\,(k(a), L)$$

and

$$\text{for } x \in \mathrm{Emb}_k\,(k(a), L), \quad \rho^{-1}(x) = \mathrm{Emb}_{k(a)}(K, L)$$

hence

$$|\,\mathrm{Emb}_k\,(K, L)\,| = \sum_{x \in \mathrm{Emb}_k(k(a),L)} |\rho^{-1}(x)| \leq [k(a) : k][K : k(a)] = [K : k]$$

by the primitive case, induction, and the tower law.[14] □

Proof of Axiom 4. We want to create a field Ω completing to a commutative diagram:

$$\begin{tikzcd}
 & L \arrow[dr, dashed] & \\
K \arrow[ur] \arrow[dr] & & \Omega \\
 & M \arrow[ur, dashed] &
\end{tikzcd}$$

[13] This proof has a typical structure: to show that something holds for an arbitrary extension $k \subset K$, we show that it hods for a primitive extension, and then reduce to the primitive extension case by tower law and induction on degree. This scheme is not super-elementary but it is never very difficult to implement.

[14] I iron out a wrinkle in the proof. Fix a k-embedding $x \colon k(a) \to L$:

$$\begin{tikzcd}
K \arrow[dr, dashed, "\widetilde{x}"] & \\
k(a) \arrow[u] \arrow[r, "x"] & L \\
k \arrow[u] &
\end{tikzcd}$$

$\rho^{-1}(x)$ is the set of k-embeddings $\widetilde{x} \colon K \to L$ such that $\widetilde{x}_{|k(a)} = x$. In the proof, I denoted this set by $\mathrm{Emb}_{k(a)}(K, L)$ but note that this set **depends** on the given embedding $x \colon k(a) \to L$. Let us be precise and denote this set by $\mathrm{Emb}_x(K, L)$ to emphasize this dependence on $x \colon k(a) \to L$. Note, however, that the $[K : k(a)] < [K : k]$, hence by induction we may still assume that:

$$|\,\mathrm{Emb}_x(K, L)| \leq [K : k(a)]$$

is bounded independent of x, and this is all we needed in the proof.

The proof is by induction on $[L : K]$. The base of the induction: If $[L : K] = 1$, then $K = L$ and we take $\Omega = M$.

If $[L : K] > 0$, pick $a \in L \setminus K$ and let $f(X) \in K[X]$ be the minimal polynomial [**i**] of a over K. It is an elementary fact [**ii**] that there is a (possibly trivial) extension $E = M(b)$ in which $f(X)$ has a root $b \in E$; and we know [**iii**] that there is a (unique) K-embedding $x \colon K(a) \to E$ such that $x(a) = b$:

$$\begin{tikzcd}
 & & L \\
 & K(a) \arrow[ur] \arrow[dr, dashed, "x"] & \\
K \arrow[ur] \arrow[dr] & & E \\
 & M \arrow[ur] &
\end{tikzcd}$$

Since by the tower law $[L : K(a)] < [L : K]$, we may assume by induction that there exists a finite field extension $K(a) \subset \Omega$:

$$\begin{tikzcd}
 & L \arrow[dr, dashed] & \\
K(a) \arrow[ur] \arrow[dr, "x"'] & & \Omega \\
 & E \arrow[ur, dashed] &
\end{tikzcd}$$

and by composing the relevant arrows $K \subset \Omega$ proves the statement. □

5.2 Proof of Axiom 5

Proposition 19 (Axiom 5). *Let L be a field, $G \subset \operatorname{Aut} L$ a finite subgroup, and write $K = L^G$ the subfield fixed by G. Then*

(i) $[L : K] = |G|$;

(ii) The manifest inclusion $G \subset \operatorname{Emb}_K(L, L)$ is an isomorphism.

Proof. We already know from Lemma 18 that

$$|\operatorname{Emb}_K(L, L)| \leq [L : K]$$

and obviously $|G| \leq |\operatorname{Emb}_K(L, L)|$ so (i) and (ii) follow from: $[L : K] \leq |G|$, which is proved in the next lemma. □

Lemma 20. *Let L be a field, $G \subset \operatorname{Aut} L$ a finite subgroup, and write $K = L^G$ the subfield fixed by G. Then $[L : K] \leq |G|$.*

Proof. Suppose that $G = \{\sigma_1, \dots, \sigma_n\}$, we want to show that all $(n+1)$-tuples $a_1, \dots, a_{n+1} \in L$ are linearly dependent over K.

Indeed, to start with, the $n+1$ vectors in L^n:

$$\mathbf{a}_1 = \begin{pmatrix} \sigma_1(a_1) \\ \vdots \\ \sigma_n(a_1) \end{pmatrix}, \dots, \mathbf{a}_{n+1} = \begin{pmatrix} \sigma_1(a_{n+1}) \\ \vdots \\ \sigma_n(a_{n+1}) \end{pmatrix}$$

are linearly dependent over L. Let $k \leq n+1$ be the smallest number of summands in a nontrivial linear dependence between the $\mathbf{a}_i$; by rearranging the indices we may assume that such a dependence holds between $\mathbf{a}_1, \dots, \mathbf{a}_k$:

$$x_1\mathbf{a}_1 + \cdots + x_k\mathbf{a}_k = 0 \tag{1}$$

Because this is a nontrivial linear dependence with the smallest number of summands, all $x_i \neq 0$, and by rescaling we may also assume that $x_1 = 1$.

We can re-word the linear dependence by stating that $x_1, \dots, x_k$ is a solution of the linear system of equations:

$$\forall\, j \in [n], \quad \sum_{i=1}^{k} x_i \sigma_j(a_i) = 0 \tag{2}$$

Applying $\sigma \in G$ to this reshuffles the j and from this we conclude that $\sigma(x_1), \dots, \sigma(x_n)$ is another solution of the system of Equations 2. So it is the old solution (otherwise by subtracting it from the old solution—since $x_1 = 1$ and so also $\sigma(x_1) = 1$—we would obtain a nontrivial linear dependence with a smaller number of summands), and then all $x_i \in K = L^G$.

But then the equation corresponding to $\sigma_j = e$ states:

$$\sum_{i=1}^{k} x_i a_i = 0$$

and this is the sought-for linear dependence over K. □

Remark 21. The following considerations may help to put what happens in Lemma 20 in context. If V is a K-vector space we can extend scalars to L: $V_L = L \otimes_K V$, and make a vector space V_L over L. When $K \subset L$ is the extension $\mathbb{R} \subset \mathbb{C}$ you are familiar with this construction under the name of *complexification* of a real vector space. Given an L-vector space V_L, we say that V_L *descends* to K when there is a K-vector space V such that $V_L = L \otimes_K V$ as above. So how can we tell if V_L descends to K? A *descent datum* is a G-action on V_L such that: For all $g \in G$, for all $\lambda, \mu \in L$, for all $v, w \in V_L$: $g(\lambda v + \mu w) = g(\lambda)g(v) + g(\mu)g(w)$. It is a general fact of linear algebra (which you can show by adapting the ideas of the proof of Lemma 20) that the category of K-vector spaces is equivalent to the category of L-vector spaces equipped with descent datum. Now the set of solutions of Equation 2 is a (nontrivial) L-vector subspace of L^{n+1} with descent datum inherited from the standard descent datum of L^{n+1}. This vector subspace descends to a nontrivial K-vector subspace $V \subset K^{n+1}$ and a nonzero element of V is the same as a solution $x_1, \dots, x_{n+1} \in K^{n+1}$ of Equation 2.

6 Discriminants and Galois groups

In this section, among other things, we answer the following question. Let K be a field of characteristic $\neq 2$. Consider a separable irreducible cubic monic polynomial with coefficients in K:

$$f(X) = X^3 + AX^2 + BX + C \in K[X] \tag{3}$$

What is the Galois group of the splitting field $K \subset L$ of f?

If $\operatorname{ch} K \neq 3$, the simple transformation $X \mapsto X - \frac{A}{3}$ changes f into a polynomial of the form

$$g(X) = X^3 + 3pX + 2q \in K[X] \tag{4}$$

Key formulas simplify for a polynomial of this form and because of this we often implicitly perform the transformation.

The Galois group is a transitive subgroup of $\mathfrak{S}_3$ — the group of permutations of the roots — and hence it is either all of $\mathfrak{S}_3$ or the cyclic subgroup of order 3 generated by a 3-cycle. The task is simple: find an **invariant** expression in the coefficients of f to distinguish these two possibilities. This invariant is the discriminant, which we introduce next.

6.1 Discriminants

Definition 22. Let the symmetric group $\mathfrak{S}_n$ act on the ring $R[X_1, \dots, X_n]$ of polynomials in n variables with coefficients in a ring R by permuting the variables.

A $\mathfrak{S}_n$-invariant polynomial is called a *symmetric polynomial.*

Example 23. For $k = 1, \dots, n$ we define the k-th elementary symmetric polynomial $\sigma_k(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ by the formula:

$$(X - X_1)(X - X_2) \cdots (X - X_n) = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \cdot + (-1)^n \sigma_n$$

Alternatively

$$\sigma_k(X_1, \dots, X_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} X_{i_1} X_{i_2} \dots X_{i_k}$$

Theorem 24. *Every symmetric polynomial is a polynomial in the elementary symmetric polynomials. More precisely:*

$$\mathbb{Z}[X_1, \dots, X_n]^{\mathfrak{S}_n} = \mathbb{Z}[\sigma_1, \dots, \sigma_n]$$

The proof is not difficult but at this point it would be a distraction.

Definition 25. Let K be a field and $f \in K$ a monic polynomial. In a splitting field we may write

$$f(X) = (X - a_1)(X - a_2) \cdots (X - a_n)$$

The *discriminant* of f is the quantity

$$\Delta_f = \prod_{i<j} (a_i - a_j)^2$$

It is obvious that the discriminant is a symmetric polynomial in the roots and hence that the discriminant is a universal polynomial expression in the coefficients of the polynomial and hence, in particular, that $\Delta_f \in K$. It is not too difficult to find and prove this formula (but not so easy either) but at this point it would be a distraction. I only mention two special cases.

Lemma 26. *(1) The discriminant of the quadratic polynomial:*

$$f(X) = X^2 - \sigma_1 X + \sigma_2 \quad \textit{is} \quad \Delta_f = \sigma_1^2 - 4\sigma_2$$

(2) The discriminant of the cubic polynomial

$$f(X) = X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3 \quad \textit{is} \quad \Delta_f = \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + 18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2$$

(3) In particular, the discriminant of the cubic polynomial[15]

$$X^3 + 3pX + 2q \quad \textit{is} \quad \Delta_f = -4 \times 27(p^3 + q^2)$$

6.2 Galois groups

Theorem 27. *Let K be a field of characteristic $\neq 2$, $f(X) \in K[X]$ a monic separable polynomial, $K \subset L$ a splitting field of f, and $G = \operatorname{Emb}_K(L, L)$ the Galois group. Then $G \subset \mathfrak{A}_n$ if and only if $\Delta(f)$ is a square in K.*

The theorem answers the question raised at the beginning of the section.

Example 28. The polynomial $f = X^3 - X - 1 \in \mathbb{Q}[X]$ has no rational roots hence it is irreducible, and $\Delta_f = -4 \times 27\left(-\frac{1}{27} + \frac{1}{4}\right) = -23$ is not a square in $\mathbb{Q}$, hence the Galois group is $\mathfrak{S}_3$.

The polynomial $f(X) = X^3 - 3X - 1 \in \mathbb{Q}[X]$ has no rational roots hence it is irreducible, and $\Delta_f = -4 \times 27\left(-1 + \frac{1}{4}\right) = 81$ is a square in $\mathbb{Q}$, hence the Galois group is $\mathfrak{A}_3$.

7 Biquadratic extensions (characteristic $\neq 2$)

This is a *pièce de résistance* that every beginner in Galois theory needs to master completely.

7.1 The key statement

In this section we fix a field K of characteristic $\neq 2$. For $a, b \in K^\times$ we study the field extension

$$L = K\left(\sqrt{a \pm \sqrt{b}}\right)$$

Below **we always assume that** b **is not a square in** K — otherwise, L is not very interesting. (The case $a = 0$, on the other hand, is perfectly interesting.)

[15] The sign in this formula is **absolutely** important.

Remark 29. (i) L is the splitting field of the polynomial:

$$f(X) = X^4 - 2aX^2 + c \in K[X] \quad \text{where} \quad c = a^2 - b \tag{5}$$

(ii) If $\operatorname{char} K \neq 2$, then $f(X)$ is separable. Indeed, under these assumptions, $Df = 4X^3 - 4aX = 4X(X^2 - a)$ manifestly has no roots in common with $f(X)$.

(iii) It is not super-obvious, but important, that L is also the splitting field of the *companion polynomial*:

$$g(Y) = Y^4 - 4aY^2 + 4b \in K[Y] \tag{6}$$

You can either prove this now, or leave it as a mystery to unveil later. In case you wonder, there are certain annoying factors of 2 in this story and I don't think you can get rid of them.

Theorem 30. *Let K be a field of characteristic $\neq 2$; let $a, b \in K^\times$ with b not a square in K. Consider the normal and separable extension*

$$K \subset L = K\left(\sqrt{a \pm \sqrt{b}}\right) \quad \textit{and set} \quad c = a^2 - b$$

Denote by G the Galois group of the extension. Then

(I) If bc, c are not squares in K, then $[L : K] = 8$ and $G = D_8$.

(II) If bc is a square in K (and then c is not a square in K, for if both bc and c are squares, then b is also square, which it isn't), then $[L : K] = 4$ and $G = C_4$.

(III) If c is a square in K (and then bc is not a square in K), then ***either***

(IIIa) Neither $2(a + \sqrt{c})$ nor $2(a - \sqrt{c})$ are squares in K. In this case $[L : K] = 4$ and $G = C_2 \times C_2$; ***or***

(IIIb) One of $2(a + \sqrt{c})$, $2(a - \sqrt{c})$ is a square in K (but not both). In this case $L = K(\sqrt{b})$, and $G = C_2$.

It will be clear that $f(X)$ is irreducible in cases (I), (II), (IIIa), and it splits into two quadratic polynomials in case (IIIb). See Lemma 33 for a discussion of this point.

In all cases the action of G on the roots of $f(X)$ is spelled out in Theorem 32. The discussion in Secs. 7.5, 7.6, 7.7 identifies all the intermediate fields and illustrates the Galois correspondence.

7.2 Initial set-up

I summarise all of the key algebra. Invest the time to familiarise yourself with it now.

In the discussion below we make the following choices:

(1) Choose $\beta \in L$ such that $\beta^2 = b$ (there are two choices, make one);

(2) Next, choose $\alpha, \alpha' \in L$ such that $\alpha^2 = a + \beta$ and ${\alpha'}^2 = a - \beta$. It is clear that $L = K(\alpha, \alpha')$. The roots of $f(X)$ are $\pm\alpha, \pm\alpha' \in L$.

The following quantities will be used throughout:

(3) $\gamma = \alpha\alpha'$. Note that $\gamma^2 = (a+\beta)(a-\beta) = a^2 - b = c$;

(4) $\delta = \alpha + \alpha'$ and $\delta' = \alpha - \alpha'$. Note that

$$\delta^2 = \alpha^2 + \alpha'^2 + 2\gamma = 2(a+\gamma)$$

and

$$\delta'^2 = \alpha^2 + \alpha'^2 - 2\gamma = 2(a-\gamma)$$

Finally note:

(5) $\delta\delta' = 2\beta$.

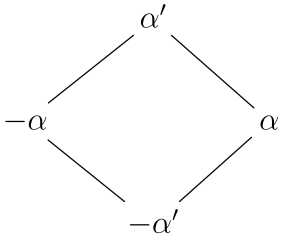
Indeed $\delta\delta' = (\alpha+\alpha')(\alpha-\alpha') = \alpha^2 - \alpha'^2 {=} a + \beta - (a-\beta) = 2\beta$.

Exercise 31. 1. Write formulas for γ, α, α' in terms of δ, δ';

2. Convince yourself that $K \subset L$ is the splitting field of the companion polynomial $g(Y)$.

7.3 The action of G on the roots of $f(X) = X^4 - 2aX^2 + c$

Theorem 32. *With the assumptions and notation of Theorem 30 and Sec. 7.2, the Galois group acts on the roots of $f(X)$ as a subgroup of the group of symmetries of the square:*



More precisely:

(I) If bc, c are not square in K, then $G = D_8$ is the whole group of symmetries of the square;

(II) If bc is a square in K, then $G = C_4$ is the group of rotations of the square;

(IIIa) If c is a square in K and neither $2(a+\sqrt{c})$ nor $2(a-\sqrt{c})$ is a square in K, then $G = C_2 \times C_2$ is generated by the two reflections along the lines of angle $\pm\frac{\pi}{4}$ in the picture;

(IIIb.1) If c is a square in K and $2(a+\sqrt{c})$ is a square in K, then $G = C_2$ acts as reflection along the line of angle $\frac{\pi}{4}$ in the picture;

(IIIb.2) If c is a square in K and $2(a-\sqrt{c})$ is a square in K, then $G = C_2$ acts as reflection along the line of angle $-\frac{\pi}{4}$ in the picture.

7.4 Irreduciblilty of $f(X) = X^4 - 2aX^2 + c$

We haven't yet understood if or when the polynomial $f(X) \in K[X]$ is irreducible.

Lemma 33. *Let K be a field of characteristic $\neq 2$. Consider $f(X) = X^4 - 2aX^2 + c \in K[X]$ where $c = a^2 - b$ and b not a square in K. Then $f(X)$ is reducible if and only if c is a square in K and either $2(a + \sqrt{c})$ or $2(a - \sqrt{c})$ is a square in K (but not both).*

Proof. We have
$$f(X) = (X - \alpha)(X + \alpha)(X - \alpha')(X + \alpha')$$
where none of the roots is in K (otherwise, for example, b is a square in K). If $f(X)$ is reducible, then either $(X - \alpha)(X - \alpha') \in K[X]$ or $(X - \alpha)(X + \alpha') \in K[X]$.

Case 1 $(X - \alpha)(X - \alpha') \in K[X]$:

$$(X - \alpha)(X - \alpha') = X^2 - \delta X + \gamma \quad \text{and} \quad f(X) = (X^2 - \delta X + \gamma)(X^2 + \delta X + \gamma)$$

since $\gamma^2 = c$, we get that c is a square in K and also $\delta^2 = 2(a + \gamma)$ is a square in K.

Case 2 $(X - \alpha)(X + \alpha') \in K[X]$:

$$(X - \alpha)(X + \alpha') = X^2 - \delta' X - \gamma \quad \text{and} f(X) = (X^2 - \delta' X - \gamma)(X^2 + \delta' X - \gamma)$$

and in this case c is a square in K and also $\delta'^2 = 2(a - \gamma)$ is a square in K.

Note that $2(a \pm \gamma)$ are not both squares in K, for otherwise the product

$$(a + \gamma)(a - \gamma) = a^2 - c = b$$

is also a square in K. □

It really can happen that f is reducible:

Example 34. Consider $f(X) = X^4 - 6X + 1 \in \mathbb{Q}[X]$, so $a = 3$, $b = 8$ (not a square in $\mathbb{Q}$) and $c = a^2 - b = 1$. Now $f(X)$ has innocent-looking roots $\pm\sqrt{3 \pm 2\sqrt{2}}$ but

$$f(X) = (X^2 - 2X - 1)(X^2 + 2X - 1)$$

So in fact the splitting field is $L = \mathbb{Q}(\sqrt{2})$ and the four roots are

$$1+\sqrt{2} = \sqrt{3 + 2\sqrt{2}},\ -1+\sqrt{2} = \sqrt{3 - 2\sqrt{2}},\ 1-\sqrt{2} = -\sqrt{3 - 2\sqrt{2}},\ -1-\sqrt{2} = -\sqrt{3 + 2\sqrt{2}}$$

Remark 35. Recall that the companion polynomial of $f(X) = X^4 - 2aX^2 + c$ is the polynomial

$$g(Y) = Y^4 - 4aY^2 + 4b \in K[Y]$$

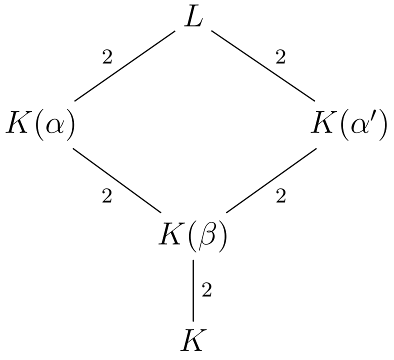
with roots $\pm\sqrt{2(a \pm \sqrt{c})}$. The previous discussion shows that f splits in $K[X]$ if and only if the companion polynomial has a root in K.

7.5 The generic case: bc, c not squares in K

We will need the following:

Lemma 36. *Let F be a field and $A, B \in F$. If A is a square in $F(\sqrt{B})$ then either A or AB is a square in F.* $\square$

Step 1 We show: $[L : K] = 8$ *in this case.*



Write $K_1 = K(\beta)$; by assumption $[K_1 : K] = 2$. I claim that $a + \beta$ is not a square in K_1. If it were, there would be $x, y \in K$ such that

$$a + \beta = (x + y\beta)^2 = (x^2 + by^2) + 2xy\beta, \quad \text{and then} \quad a - \beta = (x - y\beta)^2$$

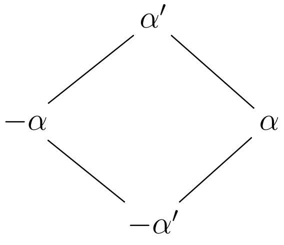
would also be a square in K_1, and then

$$c = a^2 - b = (a + \beta)(a - \beta) = (x + y\beta)^2(x - y\beta)^2 = (x^2 - y^2b)^2$$

would be a square in K, which it isn't. A similar argument shows that $a - \beta$ is not a square in K_1. We conclude that $[K_1(\alpha) : K_1] = [K_1(\alpha') : K_1] = 2$.

To finish Step 1 we just need to argue that $K_1(\alpha) \neq K_1(\alpha')$, that is, for example, $a - \beta$ is not a square in $K_1(\alpha)$. Apply Lemma 36 with $F = K_1$, $A = a - \beta$, $B = a + \beta$. If $a - \beta$ were a square in $K_1(\alpha)$, then either $a - \beta$ is a square in K_1, which it is not, or $(a - \beta)(a + \beta) = a^2 - b = c$ is a square in K_1. We need to exclude this last possibility. We apply again Lemma 36, this time with $F = K$, $A = c$, $B = b$. If c were a square in K_1, then either c is a square in K, or bc is a square in K, but we are assuming that neither is.

Step 2 *Action of the Galois group on roots.* We will show: *the Galois group acts as the group D_8 of symmetries of the square:*

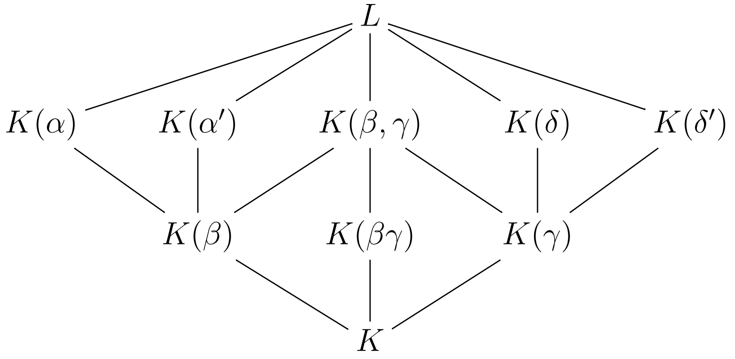


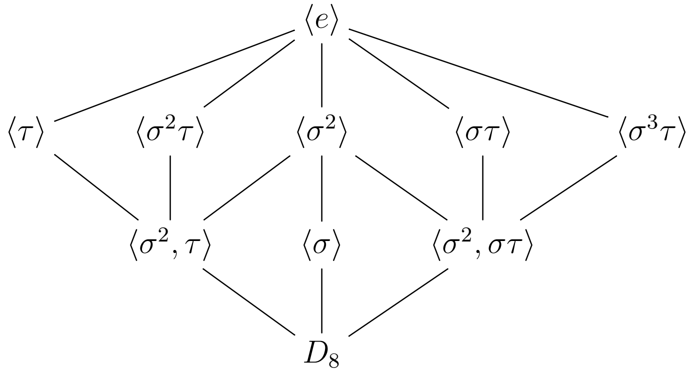
Indeed let $g \in G$ be any element. Clearly $g(\beta) = \pm\beta$. If $g(\beta) = \beta$, then $g(\alpha) = \pm\alpha$ and $g(\alpha') = \pm\alpha'$. On the other hand if $g(\beta) = -\beta$, then $g(\alpha) = \pm\alpha'$ and $g(\alpha') = \pm\alpha$. There is a total of 8 possibilities and they all are in D_8. Hence G acts on the roots as a subgroup of D_8. On the other hand [**viii**] G is a subgroup of the permutation group $\mathfrak{S}_4$ on the roots of f, and by Proposition 19 it has order $8 = [L : K]$, hence $G = D_8$.

STEP 3 *Picture of the Galois correspondence.*

I work with the following generators of D_8: τ is the reflection in the horizontal line, and σ the counterclockwise $\pi/2$-rotation.

The next picture shows the lattice of fields lying between K and L and the picture below it the corresponding lattice of subgroups of D_8:




$\langle e\rangle$
$\langle\tau\rangle$
$\langle\sigma^2\tau\rangle$
$\langle\sigma^2\rangle$
$\langle\sigma\tau\rangle$
$\langle\sigma^3\tau\rangle$
$\langle\sigma^2,\tau\rangle$
$\langle\sigma\rangle$
$\langle\sigma^2,\sigma\tau\rangle$
D_8

To establish the whole picture is more-or-less straightforward but still not without its twists and turns.

For example, $\sigma^2\tau(\alpha') = \alpha'$ (and $\sigma^2\tau(\alpha) = -\alpha$) thus the corresponding fixed field is $K(\alpha')$.

Similarly, $\sigma\tau(\alpha) = \alpha'$, $\sigma\tau(\alpha') = \alpha$, hence $K(\delta) \subset \langle\sigma\tau\rangle^\star$. To show that actually $K(\delta) = \langle\sigma\tau\rangle^\star$ we argue that $[K(\delta) : K] = 4$. Recall that δ is a root of the companion polynomial

$$g(Y) = Y^4 - 4aY^2 + 4b \in K[Y]$$

and, by the theory developed above — now brought to bear upon $g(Y)$, so now "b" is $4(a^2 - b)$, "bc" is $16bc$, and "c" is $4b$, and none of these three quantities is a square in K — the polynomial $g(Y)$ is irreducible and hence $[K(\delta) : K] = 4$. Etcetera...

7.6 bc square in K

We already know that in this case $f(X)$ is irreducible, so then $[L : K] = [K(\alpha) : K] = \deg f(X) = 4$. Similarly the companion polynomial $g(Y)$ is also irreducible. The situation with fields is as in the following diagram:

$$\begin{tikzcd}
L = K(\alpha) = K(\alpha') = K(\delta) = K(\delta') \arrow[d, dash, "2"] \\
K(\beta) = K(\gamma) \arrow[d, dash, "2"] \\
K = K(\beta\gamma)
\end{tikzcd}$$

where all arrows are degree-2 extensions. Indeed, first of all, $(\beta\gamma)^2 = bc$ so $\beta\gamma \in K$ and hence $K(\beta) = K(\gamma)$. I claim that $L = K(\alpha)$: clearly $\beta \in K(\alpha)$ so also $\gamma \in K(\alpha)$ and then so

$$\alpha' = \gamma/\alpha \in K(\alpha)$$

This shows that $L = K(\alpha)$. A similar argument shows that $L = K(\alpha')$. To show, for example, that $K(\alpha) = K(\delta)$, first observe that $\delta = \alpha + \alpha' \in K(\alpha)$, and then note that $[K(\delta) : K] = 4$ because the companion polynomial is irreducible. Similarly $K(\alpha) = K(\delta')$.

I claim that the Galois group G is a cyclic group of order 4 acting on the set of roots pictured above as rotations. Indeed consider an element $g \in G$. Then $g(\beta) = \pm\beta$ and we study the two possibilities in detail:

(1) Suppose that $g(\beta) = \beta$. Now $\beta\gamma \in K$ so we must also have $g(\gamma) = \gamma$. If $g(\alpha) = \alpha$ then also $g(\alpha') = \alpha'$ (recall that $\gamma = \alpha\alpha'$), i.e., g is the identity. Similarly, if $g(\alpha) = -\alpha$, then also $g(\alpha') = -\alpha'$: g is a π-rotation.

(2) Now suppose that $g(\beta) = -\beta$ and hence also $g(\gamma) = -\gamma$. If $g(\alpha) = \alpha'$ then

$$\alpha' = \frac{\gamma}{\alpha} \quad \text{so} \quad g(\alpha') = \frac{g(\gamma)}{g(\alpha)} = \frac{-\gamma}{\alpha'} = -\alpha$$

hence g is a rotation in this case. A similar argument shows that if $g(\alpha) = -\alpha'$, then in that case also g is a rotation.

7.7 c square in K

We are saying here that $\gamma \in K$. It is best to work with the companion polynomial:

$$Y^4 - 4aY^2 + 4b = (Y^2 - 2a - 2\gamma)(Y^2 - 2a + 2\gamma)$$

In case (IIIa) the two quadratic factors of the companion polynomial are both irreducible over K. The situation with fields is as in the following diagram:

$$\begin{tikzcd}
 & L \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
K(\beta) \arrow[dr, dash, "2"'] & K(\delta) \arrow[d, dash, "2"] & K(\delta') \arrow[dl, dash, "2"] \\
 & K &
\end{tikzcd}$$

where all arrows are degree-2 extensions. Indeed, for example, $2(a-\gamma)$ is not a square in $K(\delta)$: if it were then — by Lemma 36 — either it is already a square in K, and we are assuming that it isn't, or the product $(a+\gamma)(a-\gamma) = a^2 - c = b$ is a square in K, which it isn't.

It is easy to nail down the action of generators of G on the roots of $f(X)$. For instance $[L : K(\delta)] = 2$, hence there is an involution involution τ_1 that fixes $\delta = \alpha + \alpha'$ and necessarily $\tau_1(\alpha) = \alpha'$. Similarly there is an involution τ_2 that fixes δ' and necessarily $\tau_2(\alpha) = -\alpha'$.

Finally, suppose that we are in case (IIIb.1): $2(a+\gamma)$ is a square in K, that is $\delta \in K$. In this case G is generated by τ_1. Similarly, in case (IIIb.2) $2(a-\gamma)$ is a square, $\delta' \in K$ and G is generated by τ_2.

7.8 Examples of biquadratic extensions

Example 37. If K is the splitting field of $X^4 - 2$ over $\mathbb{Q}$, then $G = D_8$.

Example 38. If K is the splitting field of $X^4 - 4X^2 + 2$ over $\mathbb{Q}$, then $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ and $G = C_4$.

Example 39. If K is the splitting field of $\Phi_{12}(X) = X^4 - X^2 + 1$ (the cyclotomic polynomial) over $\mathbb{Q}$, then $G = C_2 \times C_2$.

Example 40. If K is the splitting field of the polynomial $X^4 - 10X^2 + 1$ over $\mathbb{Q}$, then $G = C_2 \times C_2$. In fact $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, which – inter alia – explains the identity:

$$\sqrt{5 + 2\sqrt{6}} = \sqrt{2} + \sqrt{3}$$

8 Normal extensions

We can not go very far without some practical understanding of normal and separable extensions. Here I just sketch the bare bones.

Theorem 41 (Characterisation of normal extensions)**.** *For a finite extension of fields $k \subset K$ TFAE:*

(I) for all $f \in k[X]$ irreducible, either f has no root in K or f splits completely in $K[X]$;

*(II) there exists $f \in k[X]$ (not necessarily irreducible) such that K is the splitting field [**vi**] of f;*

(III) $k \subset K$ is normal.

Proof. I show (I)⇒(II)⇒(III)⇒(I), in that order.

(I)⇒(II) If $K = k(a_1, \ldots, a_n)$, let $f_i \in k[X]$ be the minimal polynomial [**i**] of a_i. It is clear that $k \subset K$ is the splitting field [**vi**] of $f = \prod f_i$.

(II)⇒(III) Suppose that $K = k(a_1, \ldots, a_n)$ is the splitting field [**vi**] of $f \in k[X]$ where in fact

$$f = \prod (X - a_i) \in K[X]$$

(here $f \in k[X]$ is not necessarily irreducible and the a_i are not necessarily pairwise distinct). Suppose that $K \subset \Omega$ and let $x\colon K \to \Omega$ be a k-embedding. It is an elementary fact [**vii**] that for all i $x(a_i)$ is a root of f, that is, $x(K) \subset K$.

(III)⇒(I) Now assume that $k \subset K$ is normal. Let $f \in k[X]$ be an irreducible polynomial with a root $a \in K$: we will show that f splits completely in K. To this end, let $K \subset \Omega$ be the splitting field [**vi**] of f—seen as an element of $K[X]$—and let $b \in \Omega$ be a root of f: we want to show that $b \in K$. With $F = k(a)$ consider the tower:

$$k \subset F \subset K \subset \Omega$$

It is an elementary fact [**iii**] that there is a unique k-embedding $x\colon F \to \Omega$ such that $x(a) = b$. By Lemma 16(A), $x(F) \subset K$, that is, $b \in K$ as was to be shown. □

Lemma 42. *For all $k \subset K$ there is $K \subset L$ such that $k \subset L$ is normal.*

Proof. The easiest way to prove this is to use the part of Theorem 41 stating that splitting fields [**vi**] are normal: there are elements $a_1, \dots, a_n \in K$ such that $K = k(a_1, \dots, a_n)$, let $f_i \in k[X]$ be the minimal polynomial [**i**] of a_i, take $K \subset L$ the splitting field [**vi**] of $f = \prod f_i$, then $k \subset L$ is also the splitting field [**vi**] of f over k and hence $k \subset L$ is normal. □

9 The separable degree

Definition 43. For $k \subset K$, the *separable degree* $[K : k]_s$ is the number of elements of the (finite) set $\mathrm{Emb}_k(K, \Omega)$ where $k \subset \Omega$ is a normal field extension that also contains K.[16]

Remark 44. (i) By Lemma 18 $[K : k]_s \leq [K : k]$;

(ii) By Lemma 42 the separable degree is defined, but we don't yet know that it is *well* defined, that is, at the moment $[K : k]_s$ a priori depends on Ω.

Lemma 45. *$[K : k]_s$ does not depend on Ω.*

Proof. Suppose that $K \subset \Omega_1$ and $K \subset \Omega_2$ are two field extensions and $k \subset \Omega_1$ and $k \subset \Omega_2$ are normal. Let Ω be an over-field of Ω_1, Ω_2 whose existence is guaranteed by Axiom 4; by Lemma 16(A) we have

$$\mathrm{Emb}_k(K, \Omega_1) = \mathrm{Emb}_k(K, \Omega) = \mathrm{Emb}_k(K, \Omega_2)$$

□

Remark 46. We can rephrase the definition of separable extensions as follows: $k \subset K$ is separable if and only if for all towers of subfields: $k \subset K_1 \subset K_2 \subset K$, if $[K_2 : K_1]_s = 1$, then $K_2 = K_1$.

Theorem 47 (Tower law for the separable degree)**.** *For a tower $k \subset K \subset L$*

$$[L : k]_s = [L : K]_s [K : k]_s$$

[16] As a geometer, the degree of a covering is the number of geometric points in the fibre of a geometric point! The dimension of a vector space is a much more mysterious invariant.

Proof. Consider a tower $k \subset K \subset L$ and use Lemma 42 to make an extension $L \subset \Omega$ such that $k \subset \Omega$ is normal. The key point is:

Claim the natural restriction:

$$\rho \colon \operatorname{Emb}_k(L, \Omega) \to \operatorname{Emb}_k(K, \Omega)$$

is surjective, that is every k-embedding $\sigma \colon K \to \Omega$ can be extended to a k-embedding $\widetilde{\sigma} \colon L \to \Omega$.

Indeed by Lemma 16(B) σ extends to all of Ω hence a fortiori to L.

Now for all $y \in \operatorname{Emb}_k(K, \Omega)$, $\rho^{-1}(y)$ is the set of K-embeddings $x \colon L \to \Omega$, and $K \subset \Omega$ is normal, hence $\rho^{-1}(y)$ consists of $[L : K]_s$ elements.[17] The formula follows from counting elements of $\operatorname{Emb}_k(L, \Omega)$:

$$[L : k]_s = |\operatorname{Emb}_k(L, \Omega)| = \sum_{y \in \operatorname{Emb}_k(K, \Omega)} |\rho^{-1}(y)| = |\operatorname{Emb}_k(K, \Omega)| [L : K]_s = [K : k]_s [L : K]_s$$

□

10 Separable extensions

Recall [**x**] that a polynomial is separable if it has distinct roots, and an element is separable over k [**xii**] if its minimal polynomial over k is separable.

Theorem 48 (Characterisation of separable extensions). *(I) $k \subset K$ is separable if and only if $[K : k]_s = [K : k]$;*

(II) For all tower $k \subset K \subset L$, if $k \subset K$ and $K \subset L$ are separable, then $k \subset L$ is separable;

(III) $k \subset K$ is separable if and only if every $a \in K$ is separable over k.

[17] I iron out a wrinkle in the proof, the same wrinkle in fact that occurred in the proof of Lemma 18, only now it is less of a wrinkle. I warn you that reading this footnote can lead to more trouble for you than it is worth: read on at your own risk and peril! We have a fixed tower $k \subset K \subset L$:

$$\begin{tikzcd}
L \arrow[dr, dashed, "\widetilde{y}"] & \\
K \arrow[u] \arrow[r, "y"] & \Omega \\
k \arrow[u] &
\end{tikzcd}$$

$\rho^{-1}(y)$ is the set of k-embeddings $\widetilde{y} \colon L \to \Omega$ such that $\widetilde{y}_{|K} = y$. In the proof, I denoted this set by $\operatorname{Emb}_K(L, \Omega)$ but note that this set **depends** on the given embedding $y \colon K \to \Omega$. Let us be precise and denote this set by $\operatorname{Emb}_y(L, \Omega)$ to emphasize this dependence on $y \colon K \to \Omega$. The number of elements $|\operatorname{Emb}_y(L, \Omega)|$ does not depend on $y \colon L \to \Omega$: indeed this number is $[L : K]_s$ and we showed in Lemma 45 that it is independent of choices.

Given $y_1, y_2 \colon K \to \Omega$, you may want to construct as an exercise a bijective correspondence $\operatorname{Emb}_{y_1}(L, \Omega) \to \operatorname{Emb}_{y_2}(L, \Omega)$, showing in particular that these sets have the same number of elements.

Corollary 49. *(i) If a is separable over k, then $k \subset k(a)$ is separable.*

(ii) If $k \subset K$ is a splitting field of a separable polynomial, then $k \subset K$ is separable.

Proof. To prove statement (i) just observe that, by [**iii**], $[k(a) : k]_s = [k(a) : k]$; the statement then follows from Part (I) of the theorem. (In fact we only need the easy direction $[K : k]_s = [K : k]$ implies $k \subset K$ separable. This is a simple consequence of the tower law for the separable degree.)

Let us prove statement (ii). We can realise $k \subset K$ as a tower of extensions:

$$k \subset k(a_1) \subset k(a_1, a_2) \subset \cdots \subset k(a_1, a_2, \dots, a_n) = K$$

where all a_i are roots of f. By [**v**] for all i the minimal polynomial of a_i over $k(a_1, \dots, a_{i-1})$ is a factor of f, and hence it is a separable polynomial. By [**iii**] for all i

$$[k(a_1, \dots, a_i) : k(a_1, \dots, a_{i-1})]_s = [k(a_1, \dots, a_i) : k(a_1, \dots, a_{i-1})]$$

and then $[K : k]_s = [K : k]$ by repeated application of two tower laws. □

Proof of Theorem 48. The proof is in six steps:

STEP 1 *If $[K : k]_s = [K : k]$, then $k \subset K$ is separable.*

Indeed applying two tower laws to the tower

$$k \subset K_1 \subset K_2 \subset K$$

(and remembering that $[:]_s \leq [:]$) we get: if $[K_2 : K_1]_s = 1$ then $[K_2 : K_1] = 1$ and then $K_1 = K_2$.

STEP 2 *If $K \subset K(a)$ is separable, then the element a is separable over K.*

Indeed, let $f \in K[X]$ be the minimal polynomial [**i**] of a over K and suppose for a contradiction that f is not a separable polynomial. It is then an elementary fact [**xi**] that there exists $h \in K[X]$ irreducible such that $f(X) = h(X^p)$. Now $b = a^p \in K(a)$ is a root of h: $h(b) = h(a^p) = f(a) = 0$. We can form the tower

$$K \subset K_1 = K(b) \subset K_2 = K(a)$$

By the tower law

$$p \deg h = \deg f = [K_2 : K] = [K_2 : K_1][K_1 : K] = [K_2 : K_1] \deg h$$

hence $[K_2 : K_1] = p$. It follows that $X^p - b \in K_1[X]$ is the minimal polynomial [**i**] of a over K_1: indeed a is a root of this polynomial and the extension has degree p. BUT

$$X^p - b = (X - a)^p$$

hence by [**iii**] $[K_2 : K_1]_s = 1$ and this fact contradicts the separability of $k \subset k(a)$ because manifestly $K_1 \neq K_2$ (for instance because $[K_2 : K_1] = p$).

STEP 3 *If $K \subset K(a)$ is separable, then $[K(a) : K]_s = [K(a) : K]$.*

Indeed, we know from Step 2 that a is separable over K. In other words, the minimal polynomial [**i**] f of a has distinct roots and hence [**iii**, **v**]

$$[K(a):K] = \deg f = |\{\text{roots of } f\}| = [K(a):K]_s$$

STEP 4 *If $k \subset K$ is separable, then $[K:k]_s = [K:k]$. Together with Step 1, this concludes the proof of Part (I) of the theorem.*

Pick $a \in K \setminus k$ and consider the tower

$$k \subset k(a) \subset K$$

we know (trivially from the definition of separable extension of fields) that $k \subset k(a)$ and $k(a) \subset K$ are both separable. We have just shown that $[k(a):k]_s = [k(a):k]$; on the other hand definitely $[K:k(a)] < [K:k]$ hence we may assume inductively that $[K:k(a)]_s = [K:k(a)]$, hence by two tower laws $[K:k]_s = [K:k]$.

STEP 5 *(II) holds.*

Indeed (II) follows easily from (I) and two tower laws.

STEP 6 *(III) holds.*

This is easy to put together given all the above. (Don't read my proof, just do it in your head.)

Indeed, if $k \subset K$ is separable, let $a \in K$. Clearly $k \subset k(a)$ is separable, and hence by Step 2 a is separable over k.

Conversely, let $k \subset K$ be an extension and suppose that every $a \in K$ is separable over k. Pick $a \in K \setminus k$; because a is separable over k we have that $[k(a):k]_s = [k(a):k]$ and hence by Step 1 $k \subset k(a)$ is separable. By (II), to show that $k \subset K$ is separable, it suffices to show that $k(a) \subset K$ is separable. By assumption every element $b \in K$ is separable over k, and hence a fortiori it is also separable over $k(a)$. Since $[K:k(a)] < [K:k]$, we may assume by induction on degree that $k(a) \subset K$ is separable. □

11 Finite fields

If F is a finite field, then for some prime $p > 0$ $\operatorname{ch} F = p$ and $\mathbb{F}_p \subset F$. Since F is finite, the extension $\mathbb{F}_p \subset F$ is finite and hence if $m = \dim_{\mathbb{F}_p} F = [F:\mathbb{F}_p]$, then $|F| = q = p^m$.

Theorem 50. *Fix a prime $p > 0$. For all integer $m > 0$ there exists a field $\mathbb{F}_q$ with $q = p^m$ elements, unique up to isomorphism. The field $\mathbb{F}_q$ is the splitting field of the (separable) polynomial $X^q - X \in \mathbb{F}_p[X]$. The Galois group of the extension $\mathbb{F}_p \subset \mathbb{F}_q$ is a cyclic group of order m generated by the* Frobenius automorphism*:*

$$\mathrm{Fr}_p \colon a \mapsto a^p$$

Proof. Suppose such a field F exists. The multiplicative group $F^\times$ has $q-1$ elements, hence they all satisfy the equation $X^q = X$ and hence $\mathbb{F}_p \subset F$ is the splitting field of the polynomial $X^q - X$ and in particular this shows uniqueness up to isomorphism [**vii**].

On the other hand let F be a splitting field of the polynomial $X^q - X$. By the Jacobian criterion [**x**] this polynomial is separable and hence it has q distinct roots in F. Now comes the key observation. Write

$$\mu_{q-1}(F) = \{z \in F \mid z^{q-1} = 1\}$$

Because $(a+b)^q = a^q + b^q$ in F, and because $\mu_{q-1}(F)$ is a group under multiplication, it follows that the set of roots of $X^q - X$ is a field, and hence by property (b) of the characterisation of splitting fields [**vi**] it must be all of F, and this shows that F has q elements.

Finally it is clear that the Frobenius automorphism Fr_p has order m and hence it is all of the Galois group. □

Corollary 51. *Every extension of finite fields is normal separable with Galois group a cyclic group.*

More precisely every extension is of the form $\mathbb{F}_q \subset \mathbb{F}_{q^r}$ — where $q = p^m$ for some prime p and $m = [\mathbb{F}_q : \mathbb{F}_p]$— where r is the degree of the extension. The Galois group is generated by $\mathrm{Fr}_q = (\mathrm{Fr}_p)^m$.

Proof. A straightforward consequence of the theorem. Let $K \subset L$ be an extension of finite fields of characteristic p. By what we said $K = \mathbb{F}_q$ where $q = p^m$ and then if $[L : K] = r$ it must be that $L = \mathbb{F}_{q^r} = \mathbb{F}_{p^{rm}}$.

Consider the tower $\mathbb{F}_p \subset K \subset L$: $K \subset L$ is normal and separable because $\mathbb{F}_p \subset L$ is normal and separable. All other statements follow easily from the Galois correspondence. □

12 Frobenius lifts

Definition 52. A *monoid* is a commutative semigroup with identity. (For example, $\mathbb{N}$ is a monoid.)

Let P be a monoid and K be a field. A function $\chi\colon P \to K$ is a *(multiplicative) character* if: $\chi(0) = 1$ and for all $p_1, p_2 \in P$, $\chi(p_1 + p_2) = \chi(p_1)\chi(p_2)$.[18]

Theorem 53 (Linear independence of characters, a.k.a. Dedekind independence Theorem)**.** *Let K be a field, P a monoid. Any set*

$$\{\chi_1, \dots, \chi_n\colon P \to K\}$$

of pairwise distinct nontrivial characters is a linearly independent subset of the K-vector space of (set-theoretic) functions $f\colon P \to K$.

Proof. Work by induction on n. Assume for a contradiction a linear relation:

$$\sum \lambda_i \chi_i = 0$$

By induction, we may assume that all $\lambda_i \neq 0$. Find $p \in P$ such that $\chi_1(p) \neq \chi_2(p)$ and then write a new relation:

$$\sum \lambda_i \chi_i(p) \chi_i = 0$$

[18] For us, it will always be the case that $\chi(P) \subset K^\times$, but I am not requiring this in the definition.

By induction, the new relation relation must be a multiple of the old relation. The two relations are

$$(\lambda_1, \lambda_2, \dots, \lambda_n) \quad \text{and} \quad (\lambda_1\chi_1(p), \lambda_2\chi_2(p), \dots, \lambda_n\chi_n(p))$$

Note that the new relation is not the zero relation, because if it were, then we would have for all i $\chi_i(p) = 0$, contradicting $\chi_1(p) \neq \chi_2(p)$. Hence for all i $\chi_i(p) = \chi_1(p)$, which contradicts $\chi_2(p) \neq \chi_1(p)$. □

To illustrate the statement, we show as a consequence that if L is a field, G a finite group of automorphisms of L, and $K \subset L^G$, then $|G| \leq [L : K]$. This is a special case of Lemma 18, which we proved earlier by a different method. The proof here follows from considering two different interpretations of the elements $\sigma_1, \dots, \sigma_n$ of G:

(I) In the first interpretation, an element $\sigma \in G$ is a character

$$\sigma\colon P = L^\times \to L$$

therefore $\sigma_1, \dots, \sigma_n$ are linearly independent in the L-vector space $\mathrm{Fun}(L^\times, L)$ of set-theoretic functions $f\colon L^\times \to L$. Note that it is the *target* L that makes any space of functions $\mathrm{Fun}(S, L)$ an L-vector space (S any set);

(II) On the other hand, each $\sigma\colon L \to L$ is a K-linear function. Identify the *source* L with K^m (for example by choosing a basis) then an element $\sigma \in G$ is a K-linear map

$$\sigma\colon K^m \to L$$

and hence, by extending scalars at the source, σ extends to a L-linear map $\widetilde{\sigma}\colon L^m \to L$, in other words an element of the vector space

$$(L^m)^\vee = \mathrm{Hom}_L(L^m, L)$$

Now the $\widetilde{\sigma}_i$ are linearly independent as elements of $(L^m)^\vee$, because a linear dependence between the $\widetilde{\sigma}_i$ implies by restricting scalars a linear dependence between the σ_i. It follows that $n \leq m$.

Theorem 54. *Let $f(X) \in \mathbb{Z}[X]$ be degree n monic; $\mathbb{Q} \subset K$ a splitting field; p a prime such that the reduction $f_p \in \mathbb{F}_p[X]$ of f mod p has n distinct roots; $\mathbb{F}_p \subset F$ a splitting field of f_p. Let $\lambda_1, \dots, \lambda_n \in K$ be the roots of f and let*

$$R = \mathbb{Z}[\lambda_1, \dots \lambda_n] \subset K$$

We have:

(i) There is a ring homomorphism $\psi\colon R \to F$;

(ii) Any such ψ gives a bijection from the set Z of roots of f in K to the set Z_p of roots of f_p in F;

(iii) A function $\psi'\colon R \to F$ is a ring homomorphism if and only if there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\psi' = \psi\sigma$;

(iv) In particular there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\mathrm{Fr}_p \psi = \psi\sigma$, where $\mathrm{Fr}_p \in \mathrm{Gal}(F/\mathbb{F}_p)$ is the Frobenius automorphism.

Definition 55. The element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\mathrm{Fr}_p \psi = \psi\sigma$ in the above theorem (iii) is called a *Frobenius lift.*

Remark 56. If $f(X)$ is separable, then a prime p satisfying the assumption of the theorem always exists. Indeed by the Jacobian criterion $f(X), Df(X) \in \mathbb{Q}[X]$ are coprime, hence there are polynomials $\phi(X), \psi(X) \in \mathbb{Z}[X]$ such that

$$\phi(X)f(X) + \psi(X)Df(X) = h \neq 0 \in \mathbb{Z} \tag{7}$$

If p is not a factor of h then, reducing Equation 7 modulo p, we get that $f_p(X), Df_p(X) \in \mathbb{F}_p[X]$ are coprime and hence, by the Jacobian criterion, f_p is separable.

Proof. Step 1 *(i) holds.*

Let $R \supset \mathfrak{m} \supset (p)$ be a maximal ideal; then $R/\mathfrak{m} \supset \mathbb{F}_p$ is a field generated by the roots of f_p; hence it is isomorphic to F.

Step 2 *(ii) holds.*

This is basically obvious. Applying ψ to the identity $f(X) = \prod(X - \lambda_i)$ we get $f_p(X) = \prod(X - \psi(\lambda_i))$, hence the $\psi(\lambda_i)$ are the roots of f_p. No two are the same, since we are assuming that f_p is a separable polynomial.

Step 3 *R is a finitely generated free $\mathbb{Z}$-module.*

Let $\lambda_1, \dots, \lambda_n \in K$ be the roots of f. It is more-or-less obvious that R is generated as a $\mathbb{Z}$-module by the set of $\lambda_1^{k_1} \dots \lambda_n^{k_n}$ where all $0 \leq k_i \leq n-1$. (Use the equation.)

Step 4 *Let $u_1, \dots, u_d$ be a basis of R as a $\mathbb{Z}$-module. This is also a basis of K as a $\mathbb{Q}$-vector space and hence $d = [K : \mathbb{Q}]$.*

Indeed, it is clear that the $u_1, \dots, u_d$ are $\mathbb{Q}$-linearly independent (clear denominators). Next $\mathbb{Q}R \subset K$ is a subring of K containing $\mathbb{Q}$, hence it is a field.[19] Because it contains all the roots of f, $\mathbb{Q}R = K$ and this implies that the $u_1, \dots, u_d$ generate K as a $\mathbb{Q}$-vector space.

Step 5 *(iii) holds.*

It is clear that G acts on R as a group of ring automorphisms. It follows that for all $\sigma \in G$, $\psi\sigma \colon R \to F$ is a ring homomorphism. Now fix $\psi \colon R \to F$ and consider $\psi_1 = \psi\sigma_1, \dots, \psi_d = \psi\sigma_d \colon R \to F$: by (ii) and because $G \subset \mathfrak{S}_n$ (the group of all permutations of the roots of f) these are all distinct (because they are distinct on the set of roots).

[19] In general if $E \subset L$ is an algebraic extension and $E \subset R \subset L$ is a ring, then R is a field. Indeed if $a \in R$, then a is the root of a polynomial

$$f(X) = a_0X^N + a_1X^{N-1} + \dots + 1$$

with coefficients in E and hence in R. Thus

$$1/a = -a_0a^{N-1} - a_1a^{N-2} - \dots - a_{N-1} \in R$$

Suppose now that $\psi_{d+1}\colon R \to F$ is one other homomorphism. Fix a basis $u_1, \dots, u_d$ of R as a $\mathbb{Z}$-module (we showed in Step 2 that $|G| = [K : \mathbb{Q}] = \mathrm{rk}_{\mathbb{Z}} R!$). By linear algebra we can solve for $\lambda_i \in F$:

$$\forall j, \quad \sum_{i=1}^{d+1} \lambda_i \psi_i(u_j) = 0$$

and this in fact implies $\sum \lambda_i \psi_i = 0$, contradicting Dedekind independence (with monoid $P = R \setminus \{0\}$ and field F). □

Corollary 57. *Let $f(X) \in \mathbb{Z}[X]$ be degree n monic; $\mathbb{Q} \subset K$ a splitting field; p a prime such that the reduction f_p of $f \mod p$ has n distinct roots and factors as a product of irreducible factors of degree $n_1, \dots, n_k$. Then the Galois group G of $\mathbb{Q} \subset K$ contains a permutation of the roots of f whose cycle decomposition is $(n_1)(n_2) \cdots (n_k)$.*

Proof. Any Frobenius lift will do. □

The corollary can be used to produce examples of extensions of $\mathbb{Q}$ that have Galois group the full symmetric group. To illustrate the point I show just two example. The technique is based on pure group theory statements of the following type:

Lemma 58. *Let $G \subset \mathfrak{S}_n$ be a transitive subgroup. If G contains a transposition and an $(n-1)$-cycle, then $G = \mathfrak{S}_n$.*

Proof. The $(n-1)$-cycle $c \in G$ must fix an element of $[n]$[20] which we may well assume to be 1, and then after relabelling the elements of $[n]$ we may assume that $c = (23 \dots n)$. Let t be the transposition; then either t involves 1 — and then by further relabelling elements we may assume $c = (23 \cdots n)$, $t = (12)$, and it is easy to conclude from here — or $t = (ab)$ where $1 < a < b$: this is what we assume from now on.

Because G is transitive, it must contain an element s such that $s(a) = 1$, but then $sts^{-1} = (1, s(b))$ and we are back in the previous case. □

Lemma 59. *Let p be prime and $G \subset \mathfrak{S}_p$ a subgroup. If G contains a transposition and a p-cycle, then $G = \mathfrak{S}_p$.*

Proof. It is well known and not difficult to see that for all n $\mathfrak{S}_n$ is generated by the elements $(1, 2)$ and $(1, 2, \dots, n)$. If $n = p$ is prime and $t, c \in \mathfrak{S}_n$ are an arbitrary transposition and n-cycle, then we may relabel the elements of $[n]$ such that $t = (1, 2)$ and $c = (1, 2, \dots, n)$. □

Example 60. The Galois group G of the splitting field $\mathbb{Q} \subset K$ of the polynomial

$$f(X) = X^5 - X - 1$$

is the symmetric group $\mathfrak{S}_5$.

Indeed, modulo $p = 2$ we get

$$f(X) \equiv x^5 + x + 1 = (x^2 + x + 1)(X^3 + x^2 + 1) \in \mathbb{F}_2[X]$$

[20] Notation: $[n] = \{1, 2, \dots, n\}$ is the set with n elements.

hence by Corollary 57 G contains a permutation with cycle decomposition (2)(3).

Modulo $p = 3$, the polynomial is irreducible, because it does not have a root and it is not divisible by any of the three irreducible degree 2 monic polynomials in $\mathbb{F}_3[X]$ (direct inspection). It follows that $f(X) \in \mathbb{Q}[X]$ is itself irreducible and, by Corollary 57, that G contains a 5-cycle.

It is easy to see, for example using Lemma 59, that $G = \mathfrak{S}_5$.

Example 61. The Galois group G of the splitting field $\mathbb{Q} \subset K$ of the polynomial

$$f(X) = X^6 - 12X^4 + 15X^3 - 6X^2 + 15X + 12$$

is the symmetric group $\mathfrak{S}_6$.

We look at the polynomial modulo small primes. Modulo $p = 2$ we get:

$$f(X) \equiv X(X^5 + X^2 + 1) \mod 2$$

where the second polynomial $r(X) = X^5+X^2+1 \in \mathbb{F}_2[X]$ is irreducible because if it weren't it would split an irreducible degree two polynomial and the only such polynomial is X^2+X+1, which does not divide into $r(X)$ (direct inspection). By Corollary 57, G contains a 5-cycle.

Eisenstein at $p = 3$ shows that $f(X)$ is irreducible in $\mathbb{Q}[X]$ and in turn this implies that G is transitive.

Next

$$f(X) \equiv (X + 1)(X + 2)(X + 3)(X + 4)(X^2 + 3) \mod 5$$

thus by Corollary 57 G contains a transposition.

By Lemma 58 $G = \mathfrak{S}_6$.

13 Cyclotomic polynomials over $\mathbb{Q}$

Definition 62. For $n > 0$ integer, the n-th *cyclotomic polynomial* is the polynomial:

$$\Phi_n(X) = \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times} \left(X - e^{\frac{2\pi k\,\mathrm{i}}{n}}\right)$$

Lemma 63. *For all $n > 0$ integer,*

$$\Phi_n(X) \in \mathbb{Z}[X]$$

Proof. Denote by $\mu_n \subset \mathbb{C}^\times$ the group of roots of unity and by $\mathbb{Q} \subset \mathbb{Q}(\mu_n)$ the splitting field of the polynomial $X^n - 1 \in \mathbb{Q}[X]$; a priori $\Phi_n(X) \in \mathbb{Q}(\mu_n)[X]$.

It is easy to argue that $\Phi_n(X) \in \mathbb{Q}[X]$. Indeed, the Galois group G of the extension is a subgroup of $\operatorname{Aut} \mu_n = (\mathbb{Z}/n\mathbb{Z})^\times$ and hence the polynomial $\Phi_n(X)$ is Galois-invariant and hence in $\mathbb{Q}[X]$.

It is a little bit more subtle to show that $\Phi_n(X)$ has integer coefficients. Fix $n > 0$. It is clear from the definition that

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

If we assume by induction that for all $d|n$, $d \neq n$, $\Phi_d(X) \in \mathbb{Z}[X]$ then it follows from the Gauss Lemma that $\Phi_n(X) \in \mathbb{Z}[X]$. □

I conclude the course with the proof of the following very deep theorem of Dedekind. I am shocked and surprised by how deep this theorem is. There really seems to be no elementary proof of the irreducibility of $\Phi_n(X) \in \mathbb{Z}[X]$ for general n (if n is prime, or the power of a prime, there is an elementary proof of irreducibility using the Eisenstein criterion).

Theorem 64. *Fix an integer $n > 0$, denote by μ_n the group of n-th roots of unity, by $\mathbb{Q} \subset \mathbb{Q}(\mu_n)$ the splitting field of the polynomial $X^n - 1$, and by G_n the Galois group of the extension $\mathbb{Q} \subset \mathbb{Q}(\mu_n)$.*[21] *The following equivalent facts hold:*

(1) The cyclotomic polynomial $\Phi_n(X)$ is irreducible;

(2) $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n)$ where

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{k \mid 0 \leq k < n \text{ and } \operatorname{hcf}(k, n) = 1\}|$$

is Euler's function;

(3) The canonical injective group homomorphism $\rho\colon G_n \to \operatorname{Aut} \mu_n = (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

Proof. It is easy to see that the three statements are equivalent. I prove statement (3).

To show that the inclusion

$$\rho\colon G_n \to (\mathbb{Z}/n\mathbb{Z})^\times$$

is surjective, we need to construct enough elements of G_n that they generate all of $(\mathbb{Z}/n\mathbb{Z})^\times$, and this we do by Frobenius lifts. The idea is clear enough and the implementation, as we shall see momentarily, straightforward.

Below for a ring A we write:

$$\mu_n(A) = \{z \in A \mid z^n = 1\}$$

Note that this assignment is *functorial*: if $\psi\colon A \to B$ is a ring homomorphism, then it induces a *group homomorphism* $\psi\colon \mu_n(A) \to \mu_n(B)$.

If p is a prime not dividing n, then — by the Jacobian criterion — $X^n - 1 \in \mathbb{F}_p[X]$ is separable, and hence Theorem 54 applies. We work with the notation of Theorem 54; in particular,

$$R = \mathbb{Z}[\zeta_n] \quad \text{where} \quad \zeta_n = e^{\frac{2\pi\,\mathrm{i}}{n}}$$

$\mathbb{F}_p \subset F$ is the splitting field of $X^n - 1 \in \mathbb{F}_p[X]$, and $\psi\colon R \to F$ the ring homomorphism whose existence is proved in Theorem 54. According to that theorem ψ gives a set-theoretic bijection from the set of roots of $X^n - 1$ in $\mathbb{Q}(\mu_n)$ to the set of roots of $X^n - 1$ in F; these sets are the groups $\mu_n = \mu_n(R)$ (recall that R is the $\mathbb{Z}$-subalgebra of K generated by the roots of $X^n - 1$ in K) and $\mu_n(F)$ and by what we said above about functoriality of μ_n

$$\psi\colon \mu_n(R) \to \mu_n(F)$$

is a *group homomorphism*. But we just said that it is also a set-theoretic bijection, therefore it is a group isomorphism. Because $\mu_n(R)$ is a cyclic group of order n (generated, for instance,

[21] I should say "a" splitting field but I have in mind the model $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n) \subset \mathbb{C}$ where $\zeta_n = e^{\frac{2\pi\,\mathrm{i}}{n}}$.

by $\zeta_n = e^{\frac{2\pi \mathrm{i}}{n}}$), this implies that $\mu_n(F)$ is also cyclic of order n.[22] For both groups, the group of automorphisms is *canonically* $(\mathbb{Z}/n\mathbb{Z})^\times$.[23]

Consider the Frobenius automorphism $\mathrm{Fr}_p \colon F \to F$. Fr_p acts on $\mu_n(F)$ as the group automorphism

$$\mathrm{Fr}_p \colon z \mapsto z^p$$

By Theorem 54 there exists $\sigma \in G_n$ such that $\mathrm{Fr}_p \, \psi = \psi\sigma$, and σ acts on $\mu_n = \mu_n(R)$ also as $z \mapsto z^p$.

To summarise we have shown: for every prime p not dividing n, there is an element of G_n that acts on μ_n as $z \mapsto z^p$.

All we need is to show that $(\mathbb{Z}/n\mathbb{Z})^\times$ is generated as a group by the classes of primes p such that $\mathrm{hcf}(p, n) = 1$, and this is completely obvious: take any $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ and decompose it into primes: by the argument with Frobenius lifts all those primes are in $G_n \subset (\mathbb{Z}/n\mathbb{Z})^\times$, hence also $k \in G_n$, hence $G_n = (\mathbb{Z}/n\mathbb{Z})^\times$. □

14 Texts

All undergraduate texts on Galois Theory go back to Emil Artin's treatment [Art44]. Because of this fact, almost any book will do, in that it is probably not much better than a more or less good copy of Artin. In my day I studied [Her75] and I still like it very much. I also recommend the notes by my friend and long-time collaborator Miles Reid [Rei], which you can find at `https://homepages.warwick.ac.uk/~masda/MA3D5/`. I am a big fan of the *expository papers* by Keith Conrad, see `https://kconrad.math.uconn.edu/blurbs/`, where you will find several articles on Galois theory.

A big step forward was taken by Grothendieck [GR, Exposé V] with his theory of the étale fundamental group (the axioms of a *Galois category* are listed at the beginning of § 4). Perhaps surprisingly, his treatment did not yet, as far as I know, "trickle down" to undergraduate texts on the subject.

My treatment in this course is close in spirit to Grothendieck's: I take an uncompromisingly "categorical" point of view where I express key definitions and statements in terms of field inclusions; never in terms of elements.

References

[Art44] Emil Artin. *Galois Theory.* Notre Dame Mathematical Lectures, no. 2. University of Notre Dame, Notre Dame, Ind., second edition, 1944.

[GR] Alexander Grothendieck and Michele Raynaud. Revêtements étales et groupe fondamental (SGA 1). `arXiv:math/0206203`.

[22] We knew this already — every finite group of the multiplicative group of a field is cyclic — but this is a new proof.

[23] I don't want to make too much of a big deal, but the point is this. Let C_n be a cyclic group of order n. I have not chosen a generator. An element $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ acts on C_n as $g \mapsto g^k$. This gives $(\mathbb{Z}/n\mathbb{Z})^\times = \operatorname{Aut} C_n$.

[Her75] Israel Nathan Herstein. *Topics in Algebra.* Xerox College Publishing, Lexington, Mass.-Toronto, Ont., second edition, 1975.

[Rei] Miles Reid. MA3D5 Galois Theory. Available from `https://homepages.warwick.ac.uk/~masda/MA3D5/`.