GALOIS THEORY

Alessio Corti*

v0.92, 10th January 2020

Contents

1 Elementary topics 2
2 Axiomatics 4
3 Fundamental Theorem 5
4 Philosophical considerations 8
5 Proofs of the Axioms 9
6 Biquadratic extensions 11
7 Normal extensions 17
8 The separable degree 18
9 Separable extensions 19
10 Finite fields 20
11 Frobenius lifts 21
12 Cyclotomic polynomials over Q 23
13 Texts 25
14 Worksheets 25
15 Solutions 28

*This is a preliminary version. Updates will keep appearing here. The text is a concise version of Galois theory as presented in my MP11 lecture course at Imperial College London (Easter terms 2018, 2019 & 2020). I thank the students who attended those courses, and my class assistant Giulia Gugiatti for correcting many mistakes.
1 Elementary topics

1.1 The category of fields and finite extensions

There is a category of fields where: objects are fields, morphisms are finite extensions.

In fact, we almost always work with a variant of this, namely we fix a field $k$ and we work in the category whose objects are finite extensions of $k$, and for two objects $k \subset K$ and $k \subset L$, morphisms are understood as morphisms that restrict to the identity on $k$.

Remark 1. Every morphism of fields is injective.

For two fields $K$, $L$, we denote by $\text{Emb}(K, L)$ the set of field homomorphisms (Embeddings) from $K$ to $L$, and by

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

the set of field homomorphisms $f : K \to L$ that are the identity on $k$, and we call the elements of this set $k$-embeddings of $K$ in $L$.

1.2 Degree and the tower law

An important observation The earlier you understand this, the better: The field structure is complicated and strangely baroque: there are two operations and they satisfy this weird distributive property. Vector spaces, groups and their representations are simpler structures and hence they are much 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.

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

Definition 2. The degree of a finite extension $K \subset L$ is the quantity:

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

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

Remark 3. (a) If $[L : K] = 1$ then $K = L$;

(b) For all $k \subset K$, every element of $\text{Emb}_k(K, K)$ is surjective, hence an isomorphism. Thus $G = \text{Emb}_k(K, K)$ is a group, and the $k$-vector space $K$ is a $k$-linear representation of $G$.

Theorem 4 (Tower law). For a tower $k \subset K \subset L$

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

\[1\text{This follows immediately from the rank-nullity formula.}\]
1.3 Elementary topics

Elsewhere in the text I use the following 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]

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

$$[\varphi_a]: K[X]/(f_a) \xrightarrow{\cong} k(a)$$

Because $[\varphi_a]$ is (by construction) injective, and because $L$ is a field, hence as a ring it is an integral domain, it follows that $k[X]/(f_a)$ is also an integral domain, and hence $(f_a)$ is a prime ideal, and hence $f_a$ is **irreducible**;

(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) For all $K \subset L$, there is a canonical bijection from the set of roots of $f_a$ in $L$ to $\text{Emb}_K(K(a), L)$ that maps a root $b$ to the unique $K$-embedding $\varphi: K(a) \to L$ such that $\varphi(a) = b$;

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

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

(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) $L = K(a_1, \ldots, a_n)$ 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) Any two splitting fields of $f \in K[X]$ are $K$-isomorphic; the isomorphism is not canonical, but it sends a root of $f$ to a root of $f$.

More generally, let $f \in K[x]$ be a polynomial, $K \subset L$ a splitting field of $f$, and $K \subset E$ any field extension. If $a_1, \ldots, a_m \in E$ are roots of $f$, then there is a $K$-embedding $K(a_1, \ldots, a_m) \subset L$;

(viii) If $K \subset L$ is a splitting field of a polynomial $f \in K[X]$ then the group $G = \text{Emb}_K(L, L)$ 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;

---

2In the course, I introduce and explain all of these points in detail when they are needed.
(ix) Let $K \subset L$ be an extension of fields; note that this induces an inclusion of polynomial rings $K[X] \subset L[X]$. The following are equivalent for two polynomials $f, g \in K[X]$: 

(a) The polynomials $f, g$ are coprime as elements of $K[X]$;
(b) The polynomials $f, g$ are coprime as elements of $L[X]$;
(c) For all finite extensions $K \subset E$, the polynomials $f, g$ have no common root in $E$;
(d) If $K \subset E$ is a field extension in which both $f$ and $g$ split completely, then $f$ and $g$ have no common root in $E$;

(x) By definition a polynomial $f \in K[X]$ is \textit{separable} if it has $n = \deg f$ distinct roots (in $a$ — and hence by [vii] in all — splitting field $K \subset L$). The \textit{Jacobian criterion}: a polynomial $f$ is separable if and only if $f$ and $Df$ (the \textit{derivative} 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 \textit{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 Section 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 $k \subset L$, $\text{Emb}_k(K, L)$ is finite.

**Axiom 2** Every morphism is injective. Also: every $k$-morphism from $K$ to $K$ is an isomorphism, that is, $\text{Emb}_k(K, K)$ is a group. For all fields $\Omega$ the (right) action of $\text{Emb}_k(K, K)$ on $\text{Emb}_k(K, \Omega)$ is free.\footnote{$f: K \to \Omega$ is injective if for all pairs of morphisms $g_1, g_2: L \to K$, $f \circ g_1 = f \circ g_2$ implies $g_1 = g_2$. Now $f \in \text{Emb}_k(K, \Omega)$ is fixed by some $g \in \text{Emb}_k(K, K)$ if and only if $f \circ g = f \circ \text{id}_K$ and then, because $f$ is injective, $g = \text{id}_K$.}

**Axiom 3** Fibered products exist. (These are just “intersections” in a bigger field.) Also, “framed” pushouts exist. (If $x_1: K \hookrightarrow L_1$, $x_2: K \hookrightarrow L_2$ are contained in a bigger field $\Omega$, 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 $\Omega$ generated by $L_1$ and $L_2$ applying all field operations; alternatively it is the smallest subfield of $\Omega$ 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:

$$
\begin{array}{ccc}
L & \downarrow & \Omega \\
\downarrow & & \downarrow \\
K & \rightarrow & M
\end{array}
$$

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

3 Fundamental Theorem

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

Definition 5. $k \subset K$ is normal if: For all $\Omega$ any two $k$-embeddings $x_1, x_2: K \rightarrow \Omega$ differ by a $k$-automorphism of $K$. More formally, for all $x \in \text{Emb}_k(K, \Omega)$, the naturally induced $x_\ast: \text{Emb}_k(K, K) \rightarrow \text{Emb}_k(K, \Omega)$ defined as: $x_\ast: \sigma \mapsto x \circ \sigma$

is bijective.

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

Informally: no matter where I go I can not “displace” $K$ away from itself.

Lemma 6. Splitting fields \[ \text{vi} \] are normal.

Proof. Let $k \subset K$ be a splitting field of the polynomial $f \in k[X]$, $K \subset \Omega$ and $x: K \rightarrow \Omega$ 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 $x(K) \subset K$.

4This field has no universal property and it is not unique. Indeed the intersection and product of $L$ and $M$ in $\Omega$ 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.

5This 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 $F$ is the fibre functor: for fields $F(K) = \text{Emb}_k(K, \Omega)$ where $\Omega$ 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!

6The function $(x, \sigma) \mapsto x \circ \sigma$ is in fact a right group action $X \times G \rightarrow G$, where $X = \text{Emb}_k(K, \Omega)$ and $G = \text{Emb}_k(K, K)$. Axiom 2 states that this action is free. An extension $k \subset K$ is normal if and only if, for all $\Omega$, $X = \text{Emb}_k(K, \Omega)$ is a $G$-torsor.
The following statement is immediate from the definition:

**Lemma 7.** Suppose given \( k \subset K \subset L \): If \( k \subset L \) is normal, then \( K \subset L \) is normal. \( \square \)

(There are counterexamples to all other obvious wishful statements.)

**Definition 8.** \( k \subset K \) is separable if: For every tower of subfields

\[
    k \subset K_1 \subset K_2 \subset K
\]

there exist: a field \( \Omega \), and at least two distinct \( K_1 \)-embeddings \( x, y : K_2 \to \Omega \).

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

**Lemma 9.** 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 37, 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 31 we define the separable degree \([K : k]_s\) of an extension \( k \subset K \) to be the number of elements of the set \( \text{Emb}_k(K, \Omega) \) of \( k \)-embeddings of \( K \) into a field \( \Omega \) such that \( k \subset \Omega \) is a normal extension that also contains \( K \). In Section 8 it is shown that the separable degree is well-defined and that it satisfies the tower law. Note that by [iv] \([K : k]_s \leq [K : k]\).

It is more-or-less obvious (and proved as Step 1 in the proof of Theorem 36) that if \([K : k]_s = [K : k]\) then \( k \subset K \) is separable.

Now if \( a \) is separable over \( k \), then by [iii] \([k(a) : k]_s = [k(a) : k]\). \( \square \)

The following is immediate from the definition:

**Lemma 10.** For \( k \subset K \subset L \), if \( k \subset L \) is separable, then \( K \subset L \) and \( k \subset K \) are separable. \( \square \)

(The converse is also true, see Theorem 36(II).)

**Theorem 11** (Fundamental Theorem of Galois Theory). If \( k \subset K \) is normal and separable then the correspondence between subfields and subgroups holds.

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

For \( H \leq G \) :

\[
    H \mapsto H^* = \{ a \in K \mid \forall g \in H, g(a) = a \}
\]

and

For \( k \subset L \subset K \):

\[
    L \mapsto L^t = \{ g \in G \mid \forall a \in L, g(a) = a \}
\]

and the task is naturally split into two halves:

---

7This 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.

8In 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 \( \text{Mor}(H_1, H_2) \) 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 \( G/H \).
**First Half** For all \( H, (H^*)^\dagger = H \). This is just Axiom 5;

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

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

Let \( k \subset F = G^* \); I show that for all \( K \subset \Omega \), the set \( \text{Emb}_k(F,\Omega) \) consists of the obvious inclusion \( F \subset K \subset \Omega \) and hence it must be that \( k = F \).

Indeed consider the tower \( k \subset F \subset K \subset \Omega \). For clarity denote by \( \iota_{F,\Omega}: F \to \Omega \) the inclusion in this tower and similarly all other inclusions in the tower. Consider \( y \in \text{Emb}_k(F,\Omega) \).

By Lemma 12(B) below, there is \( x \in \text{Emb}_k(K,\Omega) \) such that \( y = x|F \). Because \( k \subset K \) is normal, there exists \( \sigma \in \text{Emb}_k(K,K) \) such that \( y = \iota_{K,\Omega} \circ \sigma \). By construction of \( F \sigma|F \) is the identity, and therefore \( x = y|F = \iota_{F,\Omega} \).

**Lemma 12.** Suppose that \( k \subset K \) is normal. Then for all given towers:

\[
k \subset F \subset K \subset \Omega
\]

we have:

(A) the natural \( \text{Emb}_k(F,K) \to \text{Emb}_k(F,\Omega) \) (compose with the given inclusion \( K \subset \Omega \)) is surjective;

(B) the natural \( \text{Emb}_k(K,\Omega) \to \text{Emb}_k(F,\Omega) \) (restrict to the given subfield \( F \subset K \)) is surjective.

**Remark 13.** (i) (A) states that every \( k \)-embedding \( x: F \to \Omega \) in fact lands \( F \) in \( K \): \( x(F) \subset K \). When \( F = K \), this is just the definition of \( k \subset K \) normal.

(ii) (B) states that every \( k \)-embedding \( x: F \to \Omega \) extends to a \( k \)-embedding \( \tilde{x}: K \to \Omega \) (which, in fact, lands \( K \) in itself, but this fact is here besides the point):

```
     K
    / \  \
   /   \ 
  /     \ 
 F     \Omega
 /  \     \
/    \  \\
\   k
```

The case \( K = \Omega \) is especially significant: If \( k \subset K \) is normal then every embedding \( x: F \to K \) extends to an automorphism \( \sigma: K \to K \): this fact was crucial in the proof of the fundamental Theorem.

(iii) It is manifestly the case that, assuming as we are that \( k \subset K \) normal, (B)\( \Rightarrow \) (A): Indeed, given \( x: F \to \Omega \), extend it to \( \tilde{x}: K \to \Omega \), and then observe that by normality \( \tilde{x}(K) \subset K \) and hence a fortiori \( x(F) \subset K \), that is, \( F \) landed in the given inclusion of \( K \) in \( \Omega \).
Proof. By Remark \[13\](iii) we only need to prove (B). Let $x: F \to \Omega$: we want to show that $x$ is the restriction of some $\tilde{x}: K \to \Omega$. First, use Axiom 4 to construct a commutative diagram:

$$
\begin{array}{ccc}
K & \xrightarrow{y_2} & \tilde{\Omega} \\
\downarrow & & \downarrow \\
F & \xrightarrow{x} & \Omega
\end{array}
$$

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

$$y_1: K \subset \Omega \xrightarrow{z} \tilde{\Omega}$$

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 $\Omega$, that is, it gave the sought-for extension $y_2 = \tilde{x}$.

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 $\geq 5$;

(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.

\[9\]In fact, it is even true that $y_2(K) \subset K$, which implies (A).
5 Proofs of the Axioms

5.1 Proofs of Axioms 1 and 4

Lemma 14 (Axiom 1). Emb$_k$(K, L) has at most [K : k] elements.

Proof. We know that [iii, iv] that Emb$_k$(k(a), L) has at most $\deg f_\alpha = [k(a) : k]$ elements. Then proceed inductively using the tower law (easy). □

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

```
      L
     / \
    K   \Omega
       / \ M
      /   \\
     K   E
     /   \\
    /    \\
   /     \\
  K(a)---E
     /   \\
    /    \\
   /     \\
  M     \\
```

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 $x: K(a) \to E$ such that $x(a) = b$:

```
      L
     /  \\
    K(a)   x
        /  \\
       K   E
      /   \\
     /    \\
   /     \\
  K     M
```

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

```
      L
     /  \\
    K(a)   x
        /  \\
       K     E
     /   \\
    /    \\
   /     \\
  \Omega
```

and by composing the relevant arrows $K \subset \Omega$ proves the statement. □
5.2 Proof of Axiom 5

**Proposition 15** (Axiom 5). Let $L$ be a field, $G \subset \text{Aut } L$ a finite subgroup, and write $K = L^G$ the subfield fixed by $G$. Then

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

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

**Proof.** We already know from Lemma 14 that

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

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

**Lemma 16.** Let $L$ be a field, $G \subset \text{Aut } L$ a finite subgroup, and write $K = L^G$ the subfield fixed by $G$. Then $[L : K] \leq |G|$.

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

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

$$a_1 = \begin{pmatrix} \sigma_1(a_1) \\ \vdots \\ \sigma_n(a_1) \end{pmatrix}, \ldots, a_{n+1} = \begin{pmatrix} \sigma_1(a_{n+1}) \\ \vdots \\ \sigma_n(a_{n+1}) \end{pmatrix}$$

are linearly dependent over $L$. Let $k \leq n + 1$ be the smallest number of summands in a nontrivial linear dependence between the $a_i$; by rearranging the indices we may assume that such a dependence holds between $a_1, \ldots, a_k$:

$$x_1 a_1 + \cdots + x_k a_k = 0 \quad (1)$$

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 $x_1, \ldots, x_k$ is a solution of the linear system of equations:

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

Applying $\sigma \in G$ to this reshuffles the $j$ and from this we conclude that $\sigma(a_1), \ldots, \sigma(a_n)$ 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 $K$. \qed
Remark 17. There is a perspective that makes it clear why we expect a solution with all $x_i \in K$. 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 16) 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 $x_1, \ldots, x_{n+1} \in K^{n+1}$ of Equation 2.

6 Biquadratic extensions

6.1 The key statement

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

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

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

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.)

Remark 18. (i) $L$ is the splitting field of the polynomial:

$f(X) = X^4 - 2aX^2 + c \in K[X]$ where $c = a^2 - b$

(ii) If 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:

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

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 19. 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

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

Denote by $G$ the Galois group of the extension. Then
(i) If \(bc\), \(c\) are not squares in \(K\), then \([L : K] = 8\) and \(G = D_8\). The discussion in Section 6.3 below identifies all the intermediate fields, displays the Galois correspondence, and details the action of \(G\) on the roots of \(f(X)\) and \(g(Y)\).

(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, \(b\) 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

(iiiia) 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

(iiiib) 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), (iiiia), and it splits into two quadratic polynomials in case (iiiib). See Lemma 21 for a discussion of this point.

6.2 Initial considerations and 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

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

Exercise 20. 1. Write formulas for \(\beta, \alpha, \alpha'\) in terms of \(\gamma, \delta, \delta'\);

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

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

Lemma 21. 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** \((X - \alpha)(X + \alpha') \in K[X] \):

\[(X - \alpha)(X + \alpha') = X^2 - \delta'X - \gamma \quad \text{and} \quad f(X) = (X^2 - \delta'X - \gamma)(X^2 + \delta'X - \gamma)\]
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 \( K \). \( \square \)

It really can happen that \( f \) is reducible:

**Example 22.** 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
\[ 1 + \sqrt{2} = \sqrt{3 + 2\sqrt{2}}, \quad -1 + \sqrt{2} = \sqrt{3 - 2\sqrt{2}}, \quad 1 - \sqrt{2} = -\sqrt{3 - 2\sqrt{2}}, \quad -1 - \sqrt{2} = -\sqrt{3 + 2\sqrt{2}} \]

**Remark 23.** 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 \( K \).

We will need the following:

**Lemma 24.** Let \( F \) be a field and \( A, B \in F \). If \( A \) is a square in \( K(\sqrt{B}) \) then either \( A \) or \( AB \) is a square in \( K \). \( \square \)
6.3 The generic case: \(bc\), \(c\) not squares in \(K\)

**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 24 with \(E = K_1\), \(A = a - \beta\), \(B = a + \beta\). 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 24, this time with \(E = K\), \(A = c\), \(B = b\). 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 of symmetries of the square:

\[
\begin{array}{c}
\alpha' \\
\downarrow \\
-\alpha
\end{array} \quad \begin{array}{c}
\alpha \\
\downarrow \\
-\alpha'
\end{array}
\]

and this identifies the group with \(D_8\).

Below I work with the following generators of \(D_8\): \(\tau\) is the reflection in the horizontal line, and \(\sigma\) the counterclockwise \(\pi/2\)-rotation.

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 $S_4$ on the roots of $f$, and by Proposition 15 it has order $8 = [L : K]$, hence $G = D_8$.

**Step 3 Picture of the Galois correspondence.** This is the lattice of fields lying between $K$ and $L$ and below the corresponding lattice of subgroups of $D_8$:

![Diagram of Galois correspondence](image)

To establish the whole picture is straightforward. For example it is easy to see that $\sigma^2 \tau (\alpha') = \alpha'$ (and $\sigma^2 \tau (\alpha) = -\alpha$) thus the corresponding fixed field is $K(\alpha')$; similarly, $\sigma \tau (\alpha) = \alpha'$, $\sigma \tau (\alpha') = \alpha$, hence the fixed field is $K(\delta)$; etcetera.

### 6.4 $bc$ square in $K$

The situation with fields is as in the following diagram:

$$L = K(\alpha) = K(\alpha') = K(\delta) = K(\delta')$$

$$K(\beta) = K(\gamma)$$

$$K = K(\beta \gamma)$$

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 \( L = K(\alpha) \). Similar arguments show that \( L = K(\alpha') = K(\delta) = K(\delta') \).

We already know that in this case \( f(X) \) is irreducible, so then \([L : K] = [K(\alpha) : K] = \deg f(X) = 4\).

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 \( \pi \)-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.

6.5 \( c \) 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 (iii) the two quadratic factors of the companion polynomial are both irreducible over \( K \). The situation with fields is as in the following diagram:

\[
\begin{array}{c}
\text{L} \\
\downarrow \\
\text{K(\beta)} \quad \text{K(\delta)} \quad \text{K(\delta')}
\end{array}
\]

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 24 — 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.

6.6 Examples of biquadratic extensions

Example 25. If \( K \) is the splitting field of \( X^4 - 2 \) over \( \mathbb{Q} \), then \( G = D_8 \).

Example 26. 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 27. 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 28. 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:
\[
\sqrt{5 + 2\sqrt{6}} = \sqrt{2} + \sqrt{3}
\]

7 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 29 (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)$\Rightarrow$(II)$\Rightarrow$(III)$\Rightarrow$(I), in that order.

(I)$\Rightarrow$(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)$\Rightarrow$(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 $x : K \rightarrow \Omega$ 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)$\Rightarrow$(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 $x : F \rightarrow \Omega$ such that $x(a) = b$. By Lemma 12(A), $x(F) \subset K$, that is, $b \in K$ as was to be shown. \hfill $\Box$

Lemma 30. 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 29 stating that splitting fields [vi] are normal: there are elements $a_1, \ldots, a_n \in K$ such that $K = k(a_1, \ldots, a_n)$, 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. \hfill $\Box$
8 The separable degree

Definition 31. For $k \subset K$, the separable degree $[K : k]_s$ is the number of elements of the (finite) set $\text{Emb}_k(K, \Omega)$ where $k \subset \Omega$ is a normal field extension that also contains $K$.[10]

Remark 32. (i) By Lemma 14 $[K : k]_s \leq [K : k]$;
(ii) By Lemma 30 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 $\Omega$.

Lemma 33. $[K : k]_s$ does not depend on $\Omega$.

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 $\Omega$ be an over-field of $\Omega_1$, $\Omega_2$ whose existence is guaranteed by Axiom 4; by Lemma 12(A) we have

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

Remark 34. 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 35 (Tower law for the separable degree). For a tower $k \subset K \subset L$

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

Proof. Consider a tower $k \subset K \subset L$ and use Lemma 30 to make an extension $L \subset \Omega$ such that $k \subset \Omega$ is normal. The key point is:

Claim the natural restriction:

$$\rho: \text{Emb}_k(L, \Omega) \to \text{Emb}_k(K, \Omega)$$

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

Indeed by Lemma 12(B) $\sigma$ extends to all of $\Omega$ hence a fortiori to $L$.

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

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

[10]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.
9 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 36 (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 $k$.

Corollary 37. (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.

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

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

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

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

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

Proof of Theorem 36. The proof is in SIX steps:

STEP 1 We show: 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 $[\cdot]_s \leq [\cdot]$) we get: if $[K_2 : K_1]_s = 1$ then $[K_2 : K_1] = 1$ and then $K_1 = K_2$.

STEP 2 We show: 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 \([iii]\) \([K_2 : K_1] = 1\) 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** We show: If \(K \subset K(a)\) is separable, then \([K(a) : K] = [K(a) : K]\).

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 \([iii, v]\)

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

**Step 4** We show: If \(k \subset K\) is separable, then \([K : k]_s = [K : k]\). Together with Step 1, 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** We show: (II).

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

**Step 6** We show: (III).

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 \(a \in K\). By (II) \(k \subset k(a)\) 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.

\[\Box\]

### 10 Finite fields

If \(F\) is a finite field, then for some prime \(p > 0\) \(\text{char } F = p\) 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 38.** 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:

\[\text{Fr}_p : a \mapsto a^p\]
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 $F_p \subset F$ 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. □

11 Frobenius lifts

Definition 39. 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 $\chi: P \to K$ is a (multiplicative) character if: $\chi(0) = 1$ and for all $p_1, p_2 \in P$, $\chi(p_1 + p_2) = \chi(p_1)\chi(p_2)$.[11]

Theorem 40 (Linear independence of characters, aka Dedekind independence Theorem). Let $K$ be a field, $P$ a monoid. Any set

$$\{\chi_1, \ldots, \chi_n: P \to K\}$$

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

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

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

necessarily all $\lambda_i \neq 0$. Find $p \in P$ such that $\chi_1(p) \neq \chi_2(p)$ and then write a new relation:

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

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

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

Note that the new relation is not the zero relation, because if it were, then we would have for all $i$ $\lambda_i(p) = 0$, contradicting $\chi_1(p) \neq \lambda_2(p)$. Hence for all $i$ $\chi_i(p) = \chi_1(p)$, which contradicts $\chi_2(p) \neq \chi_1(p)$. □

[11]For us, it will always be the case that $\chi(P) \subset K^\times$, but I am not requiring this in the definition.
To make a pedagogical point, we show as a Corollary that if $L$ is a field, $G$ a finite group of automorphisms of $L$, and $K \subset L^G$, then $|G| \leq [L : K]$. Recall that we proved this fact earlier in the course by a different method. The proof follows from considering two different interpretations of the elements $\sigma_1, \ldots, \sigma_n$ of $G$:

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

$$\sigma: P = L^x \to L$$

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

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

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

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

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

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

**Theorem 41.** 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; $\mathbb{F}_p \subset F$ a splitting field of $f_p$. Let $\lambda_1, \ldots, \lambda_n \in K$ and let

$$R = \mathbb{Z}[\lambda_1, \ldots, \lambda_n]$$

We have:

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

(ii) Any such $\psi$ 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 $\psi': R \to F$ is a ring homomorphism if and only if there exists $\sigma \in \text{Gal}(K/\mathbb{Q})$ such that $\psi' = \psi \sigma$. In particular there exists $\sigma \in \text{Gal}(K/\mathbb{Q})$ such that $\text{Fr}_p \psi = \psi \sigma$, where $\text{Fr}_p \in \text{Gal}(F/\mathbb{F}_p)$ is the Frobenius automorphism.

**Definition 42.** The element $\sigma \in \text{Gal}(K/\mathbb{Q})$ such that $\text{Fr}_p \psi = \psi \sigma$ in the above Theorem (iii) is called a Frobenius lift.

**Proof.** Step 1 $R$ is a finitely generated free $\mathbb{Z}$-module.

Let $\lambda_1, \ldots, \lambda_n \in K$ be the roots of $f$. It is more-or-less obvious that $R$ is generated as a $\mathbb{Z}$-module by the set of $\lambda_1^{k_1} \ldots \lambda_n^{k_n}$ where all $0 \leq k_i \leq n - 1$. (Use the equation.)
Step 2 Let \( u_1, \ldots, u_d \) 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 \( u_1, \ldots, u_d \) 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 \(^{12}\) because it contains all the roots of \( f \), \( \mathbb{Q}R = K \) and this implies that the \( u_1, \ldots, u_d \) generate \( K \) as a \( \mathbb{Q} \)-vector space.

Step 3 (i) holds.

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

Step 4 (ii) holds.

This is basically obvious. Applying \( \psi \) 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 5 (iii) holds.

It is clear that \( G \) acts on \( R \) as a group of ring automorphisms. It follows that for all \( \sigma \in G \), \( \psi \sigma: R \to F \) is a ring homomorphism. Now fix \( \psi: R \to F \) and consider \( \psi_1 = \psi \sigma_1, \ldots, \psi_d = \psi \sigma_d: R \to F \): 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).

Suppose now that \( \psi_{d+1}: R \to F \) is one other homomorphism. Fix a basis \( u_1, \ldots, u_d \) of \( R \) as a \( \mathbb{Z} \)-module (we showed in Step 2 that \( |G| = [K : \mathbb{Q}] = \text{rk}_\mathbb{Z} R! \)). 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 43. 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 \( n_1, \ldots, n_k \). 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. \( \square \)

12 Cyclotomic polynomials over \( \mathbb{Q} \)

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

\[^{12}\text{In general if } E \subset L \text{ is an algebraic extension and } E \subset R \subset L \text{ is a ring, then } R \text{ is a field. Indeed if } a \in R, \text{ then } a \text{ is the root of a polynomial}
\]

\[f(X) = a_0X^N + a_1X^{N-1} + \cdots + 1\]

\[\text{with coefficients in } E \text{ and hence in } R. \text{ Thus}
\]

\[
1/a = -a_0a^{N-1} - a_1a^{N-2} - \cdots - a_{N-1} \in R
\]
proof of the irreducibility of $\Phi_n(X) \in \mathbb{Q}[X]$ (if $n$ is prime, or the power of a prime, there is an elementary proof of irreducibility using the Eisenstein criterion).

**Theorem 44.** Denote by $\mu_n$ 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. The following equivalent facts hold:

1. The cyclotomic polynomial:
   $$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \left( X - e^{2\pi ik/n} \right) \in \mathbb{Q}[X]$$
   is irreducible;

2. $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n)$ where
   $$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{ k \mid 0 \leq k < n \text{ and } \text{hcf}(k, n) = 1 \}|$$
   is Euler’s function;

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

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

To show that $\rho : G_n \to (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective, we need to construct enough elements of $G_n$, 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 $\psi : A \to B$ is a ring homomorphism, then it induces a group homomorphism $\psi : \mu_n(A) \to \mu_n(B)$.

If $p$ is a prime not dividing $n$, then $x^n - 1 \in \mathbb{F}_p[X]$ is separable, and hence Theorem 41 applies. We work with the notation of Theorem 41 in particular,

$$R = \mathbb{Z}[\zeta_n] \text{ where } \zeta_n = e^{2\pi i/n}$$

$\mathbb{F}_p \subset F$ is the splitting field of $x^n - 1 \in \mathbb{F}_p[X]$, and $\psi : R \to F$ the ring homomorphism whose existence is proved in Theorem 41. According to that theorem $\psi$ 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 $\mathbb{F}_p[X]$; 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 $\mu_n$

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

---

13I should say “a” splitting field but I have in mind the model $\mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n) \subset \mathbb{C}$ where $\zeta_n = e^{2\pi i/n}$. 24
is a group homomorphism. But we just said that it is also a set-theoretic bijection, therefore it is a group isomorphism. Because \( \mu_n = \mu_n(R) \) is a cyclic group of order \( n \) (generated, for instance, by \( \zeta_n = e^{2\pi i/n} \)), this implies that \( \mu_n(F) \) is also cyclic of order \( n \). For both groups, the group of automorphisms is canonically \( (\mathbb{Z}/n\mathbb{Z})^\times \). 

Consider the Frobenius automorphism \( \text{Fr}_p: F \to F \). \( \text{Fr}_p \) acts on \( \mu_n(F) \) as the group automorphism 

\[ \text{Fr}_p: z \mapsto z^p. \]

By Theorem 41 there exists \( \sigma \in G_n \) such that \( \text{Fr}_p \psi = \psi \sigma \), and \( \sigma \) 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 \( \mu_n \) 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 \( \text{hcf}(p, n) = 1 \), 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 \( G_n = (\mathbb{Z}/n\mathbb{Z})^\times \).

\[ \square \]

### 13 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/](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/](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.

### 14 Worksheets

#### 14.1 Worksheet 1

**Q 1.** This question is designed to get you up to speed with arithmetic in \( \mathbb{Q}[x] \).

(a) Find the quotient and remainder when \( x^5 + x + 1 \) is divided by \( x^2 + 1 \).

---

\[ ^{14} \text{We knew this already — every finite group of the multiplicative group of a field is cyclic — but this is a new proof.} \]

\[ ^{15} \text{I don’t want to make too much of a big deal, but the point is this. Let } C_n \text{ be a cyclic group of order } n. \text{ I have not chosen a generator. An element } k \in (\mathbb{Z}/n\mathbb{Z})^\times \text{ acts on } C_n \text{ as } g \mapsto g^k. \text{ This gives } (\mathbb{Z}/n\mathbb{Z})^\times = \text{Aut } C_n. \]
(b) Find the remainder when \( x^{2019} + 32x^{53} + 8 \) is divided by \( x - 1 \).
(c) Find polynomials \( s(x) \) and \( t(x) \) such that
\[
(2x^3 + 2x^2 + 3x + 2)s(x) + (x^2 + 1)t(x) = 1.
\]
[Bonus question: how did I know for sure that these polynomials were coprime?]
(d) Find a hcf for \( x^4 + 4 \) and \( x^3 - 2x + 4 \). Express it as \( a(x)(x^4 + 4) + b(x)(x^3 - 2x + 4) \).
(e) Find polynomials \( \lambda(x) \) and \( \mu(x) \) such that \((1 + x)\lambda(x) + (x^3 - 2)\mu(x) = 1\).

Q 2. Write \( \xi = \sqrt{2} \). This question is about understanding the field operations in \( \mathbb{Q}(\xi) \) explicitly.

(a) Find rational numbers \( a, b \) and \( c \) such that \( a + b\xi + c\xi^2 = 1/(1 + \xi) \).
[\text{Hint: use Part (e) of the previous question.}]
(b) Fix rational numbers \( A, B \). Find rational numbers \( a, b \) and \( c \) (depending on \( A, B \)) such that \( a + b\xi + c\xi^2 = 1/(A + B\xi + \xi^2) \).

Q 3. Prove that if \( f, g \in K[x] \) and at least one is non-zero, and if \( s, t \) are both hcf’s of \( f \) and \( g \), then \( s = \lambda t \) for some \( \lambda \in K^\times \).

Q 4. (a) We know that whether or not a polynomial is irreducible depends on which field it’s considered as being over: for example \( x^2 + 1 \) is irreducible in \( \mathbb{Q}[x] \) but not in \( \mathbb{C}[x] \). But show that the notion of divisibility does not depend on such issues. More precisely show that if \( K \subseteq L \) are fields, if \( f, g \in K[x] \), and if \( f \mid g \) in \( L[x] \) then \( f \mid g \) in \( K[x] \).

(b) Is it true that if \( f, g \in \mathbb{Z}[x] \) and \( f \mid g \) in \( \mathbb{Q}[x] \) then \( f \mid g \) in \( \mathbb{Z}[x] \)? [\text{Hint: No.} Is it true under the extra assumption that \( f \) is monic? [\text{Hint: Yes.}]

Q 5. (a) Prove that if \( n \in \mathbb{Z} \) and \( \sqrt{n} \notin \mathbb{Z} \) then \( \sqrt{n} \notin \mathbb{Q} \).

(b) Prove that \( \sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \). What is the minimum polynomial of \( \sqrt{3} \) over \( \mathbb{Q}(\sqrt{2}) \)?
(c) Use the Tower Law to prove that \([\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4\). Write down a basis for the \( \mathbb{Q} \)-vector space \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \).

Q 6. (a) Prove that \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \).
[\text{Hint: the smallest subfield of the complex numbers containing \( \mathbb{Q} \) and \( \sqrt{2} + \sqrt{3} \) must contain loads of other things too: write some of them down.}]

(b) Deduce that \( x^4 - 10x^2 + 1 \) is irreducible over \( \mathbb{Q} \).

Q 7. Is \( \sqrt{10} \in \mathbb{Q}(\sqrt{6}, \sqrt{15}) \)?

Q 8. Prove that: If \( K \subseteq L \subseteq E \) are fields, and one of \([L : K] \) or \([E : L] \) is infinite, then \([E : K] \) is infinite.
Remark: for those unfamiliar with infinite-dimensional vector spaces, a vector space \( V \) over a field is infinite-dimensional iff it has no finite spanning set, iff for every \( n \geq 1 \) there exist \( n \) elements \( v_1, v_2, \ldots, v_n \) which are linearly independent.

Q 9. (a) Prove that if \( K \subseteq L \) is a finite extension of fields and \( V/L \) is a finite-dimensional vector space then \( \dim_K(V) = [L : K]\dim_L(V) \).

(b) Prove that if \( K \subseteq L \subseteq E \) and \([E : K] = [L : K] \) is finite, then \( L = E \).
Q 10. Let $K$ be a field with $\text{char}(K) \neq 3$ and such that $f(x) = x^3 - 3x + 1 \in K[x]$ is irreducible. Let $L = K(\alpha)$ where $\alpha$ is a root of $f(x)$. Show that $f$ splits completely over $L$. [Hint: Factor $f$ over $L[x]$ as $(x - \alpha)g(x)$. Now solve for $g(x) = 0$ in $L$ observing that $12 - 3\alpha^2 = (-4 + \alpha + 2\alpha^2)^2$.]

Q 11 (*). Let $K$ be a field of characteristic 0 containing an element $\omega \in K$ with

$$\omega^2 + \omega + 1 = 0.$$ 

(For example you can take $K = \mathbb{Q}(\omega)$ where $\omega = \exp \frac{2\pi i}{3}$.) In this question we carve a trick-free path to the formula for the solutions of the equation

$$y^3 + 3px + 2q = 0 \quad (†)$$

(where $p, q \in K$) that only involves taking radicals (i.e., $\sqrt[n]{\cdot}$ of something).

We assume that $K \subset L$ is the splitting field of the polynomial of Equation (†) and we denote by $\alpha_1, \alpha_2, \alpha_3 \in L$ the three roots. (You can already prove that such a field extension exists but I don’t care that you do this here.)

We know that the Galois group $G$ permutes the three roots.

(a) Write the action of the cyclic permutation $\sigma = (123)$ on the elements

$$u = \alpha_1 + \omega \alpha_2 + \omega^2 \alpha_3, \quad v = \alpha_1 + \omega^2 \alpha_2 + \omega \alpha_3.$$ 

and conclude that $\sigma(u) = \omega u$ and $\sigma(v) = \omega^2 v$. \[16\]

(b) Find a formula expressing the three roots $\alpha_1, \alpha_2, \alpha_3$ in terms of $u$ and $v$. \[Hint: \alpha_1 + \alpha_2 + \alpha_3 = 0.]

(c) Consider the transposition $\tau = (23)$: show that $\tau(u) = v$ and $\tau(v) = u$, and hence argue that $u^3 + v^3$ and $u^3v^3$ are fixed by all of $S_3$ — and hence by all of $G$, irrespective of what $G$ is. In other words, it follows from the Galois Correspondence that $u^3 + v^3$ and $u^3v^3 \in K$: show that this is indeed the case by finding explicit formulas for these quantities. Thus write down an explicit quadratic polynomial in $K[X]$ of which $u^3, v^3$ are the two roots. Solve the quadratic equation, and combine with (b) to derive the cubic formula.

\[16\] Whether or not there is an element of $G$ that acts as $\sigma$ on the three roots is not relevant at this point. Such an element may or may not exist.
14.2 Worksheet 2
14.3 Worksheet 3
14.4 Worksheet 4
14.5 Worksheet 5

15 Solutions
15.1 Worksheet 1
15.2 Worksheet 2
15.3 Worksheet 3
15.4 Worksheet 4
15.5 Worksheet 5

References


