An Internship Project on

GALOIS FIELD EXTENSIONS

Submitted by

Himanshu Kumar
M.Sc. Mathematics
University of Hyderabad,Telangana

Under the Guidence of

Prof. Umesh Kumar V Dubey

Department of Mathematics

Harish-Chandra Research Institute
Prayagraj, Uttar Pradesh, India
July 2025

DECLARATION BY CANDIDATE

I hereby declare that the internship project titled **"Galois Field Extensions"** is the result of my own work and has been carried out under the guidance of **Prof. Umesh Kumar V. Dubey** This work has not been submitted elsewhere for any academic or professional purpose.

Himanshu Kumar

M.Sc. Mathematics
University of Hyderabad

ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to **Prof. Umesh Kumar V. Dubey**, Department of Mathematics, Harish-Chandra Research Institute, Prayagraj, for his invaluable guidance, constant encouragement, and insightful feedback throughout the course of this internship project on *Galois Field Extensions*. His expertise in algebra and field theory has been instrumental in shaping my understanding of this subject.

I am also thankful to the **Department of Mathematics, University of Hyderabad**, for providing me the opportunity and academic environment to carry out this work.

My heartfelt thanks to all faculty members and fellow students who offered support and shared discussions that enriched my learning experience. **Himanshu Kumar**

M.Sc. Mathematics
University of Hyderabad

Contents

Chapter 1

Introduction

Classical (finite) Galois theory establishes a beautiful correspondence between field extensions and group theory. It provides a one-to-one, inclusion-reversing correspondence between the intermediate fields of a finite Galois extension

$$E/F$$

and the subgroups of the Galois group

$$\text{Galois}(E/F).$$

This powerful framework forms the backbone of many results in algebra and number theory. However, many important extensions in mathematics such as the algebraic closure of $\mathbb{Q}$, or the union of all finite fields $\bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ are infinite. For these, the classical framework of Galois theory must be extended. This leads us to **Infinite Galois Theory**.

Chapter 2

Galois Group

2.1 Definitions

Definition 2.1.1. *An **isomorphism** α of a field K with itself is called an **automorphism** of K. The collection of all automorphisms of K is denoted by* $\mathrm{Aut}(K)$. *If $a \in K$, we shall write $a\alpha$ for $\alpha(a)$.*

Definition 2.1.2. *An automorphism $\alpha \in \mathrm{Aut}(K)$ is said to **fix** an element $a \in K$ if $a\alpha = a$. If F is a subset of K (for example, a subfield), then an automorphism α is said to **fix** F if it fixes all elements of F, i.e.,*

$$a\alpha = a, \quad \text{for all } a \in F.$$

NOTE:

1. Let F be a field. Then the identity map $\mathrm{id}_F : F \to F$ defined by $\mathrm{id}_F(x) = x$ for all $x \in F$ is an automorphism of F. This automorphism is called the *trivial automorphism*. Hence, every field has at least one automorphism.

2. Let K be a field. The prime field of K is generated by $1 \in K$, and any automorphism $\alpha \in \mathrm{Aut}(K)$ satisfies $\alpha(1) = 1$. Therefore, for all b in the prime field of K, we have $\alpha(b) = b$. Any automorphism of a field K fixes its prime subfield.

For example:

- For the field of rational numbers, $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$, since any field automorphism must fix every element of $\mathbb{Q}$.

- For the finite field $\mathbb{F}_p$ (where p is prime), $\mathrm{Aut}(\mathbb{F}_p) = \{\mathrm{id}\}$, because $\mathbb{F}_p$ has no nontrivial automorphisms.

Hence, both $\mathbb{Q}$ and $\mathbb{F}_p$ have only the trivial automorphism.

Definition 2.1.3. *Let K/H be an extension of fields. Let* $\mathrm{Aut}(K/H)$ *denote the collection of automorphisms of K that fix every element of H. That is,*

$$\mathrm{Aut}(K/H) = \{\alpha \in \mathrm{Aut}(K) \mid \alpha(h) = h \text{ for all } h \in H\}.$$

If H is the prime subfield of K, then every automorphism of K automatically fixes H. Therefore,

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

NOTE:

1. Let $\alpha, \tau \in \mathrm{Aut}(K)$ be automorphisms of a field K. Then the compositions $\alpha \circ \tau$ and $\tau \circ \alpha$ are also automorphisms of K.

At this point, it is natural to ask whether $\alpha \circ \tau = \tau \circ \alpha$ always. To address this question, we consider the following example.
Gal $\left(\mathbb{Q}(\sqrt[3]{2}, w)/\mathbb{Q}\right.$ and $K = \mathbb{Q}(\sqrt[3]{2}, w)$
Let $\alpha : \sqrt[3]{2} \to w\sqrt[3]{2}$ and $\tau : \sqrt[3]{2} \to \sqrt[3]{2}$ be two automorphisms. Then,
$a^3 =$ identity as $\omega^3 = 1$ and $\tau^2 =$ identity as $\omega \to \omega^2 \to \omega^4 = \omega$.
Let $\sqrt[3]{2} \in K = \mathbb{Q}(\sqrt[3]{2}, \mathbb{Q})$, which implies

$$\alpha\tau(\sqrt[3]{2}) = \alpha(\tau(\sqrt[3]{2}) = \alpha(\sqrt[3]{2}) = \omega\sqrt[3]{2}$$

and

$$\tau\alpha(\sqrt[3]{2}) = \tau(\omega\sqrt[3]{2}) = \tau(\omega) \cdot \tau(\sqrt[3]{2}) = \omega^2\sqrt[3]{2}.$$

As a consequence, $\tau\alpha \neq \alpha\tau$. Therefore, $\tau\alpha$ may or may not be equal to $\alpha\tau$.

Lemma 2.1.4. Aut(K) *is a group under composition and* Aut(K/H) *is a subgroup.*

Lemma 2.1.5. *Let K/H be a field extension and $\beta \in K$ be algebraic over H. Then for any $\alpha \in$* Aut(K/H)*, $\alpha\beta$ is a root of the minimal polynomial for β over H that is,* Aut(K/H) *pa mutes the roots of irreducible polynomials. Equivalently, any polynomial with coefficient in F having β as a root also has $\alpha\beta$ as a root.*

Definition 2.1.6. *The element $\beta \in K$ be **algebraic** over H if β is a root of some nonzero polynomial $h(x) \in H(x)$. If β is not algebraic (that is, it is not the root of any nonzero polynomial with coefficients in H), then β is said to be a **transcendental** over H. The extension K/H is said to be **algebraic** if every element of K is algebraic over H.*

Examples:

1. $K = \mathbb{Q}\sqrt{2}$, where $\mathbb{Q}\sqrt{2} = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$. Now,$\mathbb{Q}$ is a prime subfield of $\mathbb{Q}(\sqrt{2})$, so $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. If $\tau \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2}) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, then $\tau(\sqrt{2}) = \pm\sqrt{2}$ (two roots). Since τ fixes $\mathbb{Q}$, so $\tau(a + b\sqrt{2}) = a \pm b\sqrt{2}$. Let us consider two maps $sd : \sqrt{2} \to \sqrt{2}$ and $\tau : \sqrt{2} \to -\sqrt{2}$. Then, $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{1, \tau\}$, which is a cyclic group of order 2 generated by τ.

2. $K = \mathbb{Q}(\sqrt[3]{2}) = \left\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\right\}$. The minimal polynomial is $x^3 - 2$. Now, by solving $x^3 - 2 = 0$, we will get the roots of the polynomial.

Lemma 2.1.7. *Let $F \leq \mathrm{Aut}(K)$ be a subgroup of the group of automorphisms of K, then by the collection H of elements of K fixed by all elements of F is a subfield of K.*

Let $f \in F$ and $p, q \in H$, then $f(p) = p, f(q) = q$ (by definition).Now,

$$f(p \pm q) = f(p) \pm f(q) = p \pm q,$$

$$f(pq) = f(p)f(q) = pq,$$
$$f(p^{-1}) = (f(p))^{-1} = p^{-1}.$$

H is closed, which concludes that H is a subfield of K.

Definition 2.1.8. *If $F \leq \mathrm{Aut}(K)$, then the subfield of K fixed by all elements of F is called the **fixed field** of F.*

Definition 2.1.9. *The extension field K of H is called **splitting field** for the polynomial $h(x) \in H(x)$ if $h(x)$ factors completely into linear factors (or splits completely) in $K(x)$ and $h(x)$ does not factor completely into linear factors for any proper subset of K containing H.*

NOTE: If $h(x)$ has degree n, then $h(x)$ has at most n roots in H and has precisely n roots in H iff $h(x)$ splits completely in $H(x)$.

Definition 2.1.10. *Let H be a field and $h(x) \in F(x)$ be a polynomial over a splitting field for $h(x)$. We have the factorization*

$$h(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\dots(x-\alpha_k)^{n_k},$$

*where $\alpha_1, \alpha_2, \dots \alpha_k$ are distinct elements of the splitting field and $n_i \geq 1, \forall i$; and α_i is called a multiple root if $n_i > 1$ and is called simple root if $n_i = 1$. The integer n_i is called the multiplicity of the root α_i. A polynomial over H is called **separable** if it has no multiple roots. A polynomial which is not separable is called **inseparable**.*

Lemma 2.1.11. *Let E be the splitting field over H of the polynomial $h(x) \in H(x)$, then $|\operatorname{Aut}(E/H)| \leq [E:H]$ with equality if $h(x)$ is separable over H.*

2.2 Galois Group

Let K/H be a finite extension, then K is said to be Galois over H and K/H is Galois extension if $|\operatorname{Aut}(K/H)| = [K:H]$. If K/H is Galois, then the group of automorphisms $\operatorname{Aut}(K/H)$ is called the Galois group of K/H, denoted by $Gal(K/H)$.

Lemma 2.2.1. *If K is the splitting field over H of a separable polynomial $h(x)$, then $K(H)$ is Galois.*

Definition 2.2.2. *If $h(x)$ is a separable polynomial over H, then the Galois group of $h(x)$ over H is the Galois group of the splitting field of $h(x)$ over H.*

Example: Field extension of $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$,
where $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$. Minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$ and the roots of the minimal polynomial is given by $\sqrt{2}, -\sqrt{2}$. Now, consider the possible automorphisms $id : a + b\sqrt{2} \to a + b\sqrt{2}$ and $\sigma : \sqrt{2} \to -\sqrt{2}$. Again, $\operatorname{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, 6\}$. Therefore, $|\operatorname{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$; both are equal. Therefore, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois extension. Now, $\operatorname{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, 6\}$ is Galois group and $Gal(\mathbb{Q}(\sqrt{2})/\sqrt{2}) = \{id, 6\} \cong \mathbb{Z}/2\mathbb{Z}$, cyclic group of order 2.

Lemma 2.2.3. *The group $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois group.*

Proof. Minimal polynomial of $\mathbb{Q}(\sqrt[3]{2})$ is given by $x^3 - 2 = 0$. The roots of the minimal polynomial are $x = \sqrt[3]{2}, \left(-3\sqrt{2} + i\sqrt{32^2/3}\right)/2, \left(-3\sqrt{2} - i\sqrt{32^2/3}\right)/2$. Since the minimal polynomial has only one real root, so only one automorphism is possible. Therefore, $|\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$. But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$,

which will contradict our statement. Therefore, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois extension and henceforth not a Galois group. □

Lemma 2.2.4. *The group* $\mathbb{Q}(\sqrt{2},\sqrt{3})$ *is Galois over* $\mathbb{Q}$.

Proof. Minimal polynomial of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is given by $(x^2-2)(x^2-3)$. The roots of the minimal polynomial are, $x=\pm\sqrt{2},\pm\sqrt{3}$. Therefore, degree $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$. Then the possible automorphisms are given by,

$$id:\sqrt{2}\to\sqrt{2} \quad \text{or} \quad id:\sqrt{3}\to\sqrt{3},$$
$$\sigma:\sqrt{2}\to-\sqrt{2} \quad \text{or} \quad \sigma:\sqrt{3}\to\sqrt{3},$$
$$\tau:\sqrt{2}\to\sqrt{2} \quad \text{or} \quad \tau:\sqrt{3}\to-\sqrt{3},$$
$$\sigma\tau:\sqrt{2}\to-\sqrt{2} \quad \text{or} \quad \sigma\tau:\sqrt{3}\to-\sqrt{3}.$$

Now, $\sigma\tau(-\sqrt{2})=\sigma(\sqrt{2})=-\sqrt{2}$ and $\sigma\tau(\sqrt{3})=\sigma(-\sqrt{3})=-\sqrt{3}$ and $\mathrm{Aut}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})\right)=\{id,\sigma,\tau,\sigma\tau\}$. Therefore, $|\,\mathrm{Aut}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})\right)|=4=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$. Therefore, this is a Galois extension and $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is Galois over $\mathbb{Q}$ and $Gal\left(\mathbb{Q}(\sqrt{2},\sqrt{3})\right)=\{id,\sigma,\tau,\sigma\tau\}\cong\frac{\mathbb{Z}}{2\mathbb{Z}}\times\frac{\mathbb{Z}}{2\mathbb{Z}}\cong K_4$. □

Klens four group:

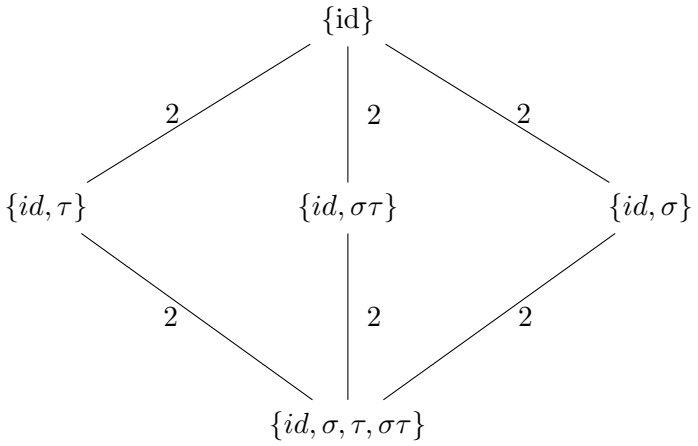
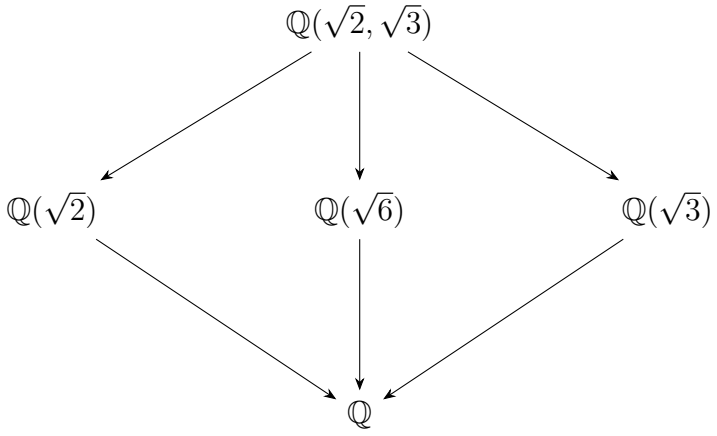


Diagram of fixed fields:

Subgroup $H\leq G$	**fixed field** (H)
$G=V_4$ or K_4	$\mathbb{Q}$
Subgroup fixing $\sqrt{2}$	$\mathbb{Q}(\sqrt{3})$
Subgroup fixing $\sqrt{3}$	$\mathbb{Q}(\sqrt{2})$
Subgroup fixing $\sqrt{6}$	$\mathbb{Q}(\sqrt{6})$
Trivial subgroup $\{id\}$	$\mathbb{Q}(\sqrt{2},\sqrt{3})$



2.3 Fundamental Theorem of Galois Theory

Let K/H be a Galois extension and set $G = Gal(K/H)$. Then there is a bijection

$$\left\{ \text{ subfields } E \subseteq K \text{ containing } H \right\} \longleftrightarrow \left\{ \text{ subgroups } F \subseteq G \right\}$$

given by the correspondences:

$$E \mapsto \mathrm{Gal}(K/E) = \{\sigma \in G \mid \sigma|_E = \mathrm{id}_E\},$$
$$F \mapsto \text{the fixed field } K^F = \{x \in K \mid \sigma(x) = x \text{ for all } \sigma \in F\},$$

which are inverse to each other. Under this correspondence:

1. **(Inclusion Reversing)**: If E_1, E_2 correspond to F_1, F_2 respectively, then
$$E_1 \subseteq E_2 \quad \text{if and only if} \quad F_2 \subseteq F_1.$$

2. **(Degree Formula)**:
$$[K : E] = |F| \quad \text{and} \quad [E : H] = [G : F],$$
the index of F in G.

3. The extension K/E is always Galois, with Galois group:
$$\mathrm{Gal}(K/E) = F.$$

4. The field E is Galois over H if and only if F is a normal subgroup of G. In that case, the Galois group is isomorphic to the quotient group:

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

More generally, even if F is not necessarily normal in G, the isomorphisms of E (into a fixed algebraic closure of H containing K) which fix H are in one-to-one correspondence with the cosets σF of F in G.

(5) If E_1, E_2 correspond to F_1, F_2 respectively, then:

- The intersection $E_1 \cap E_2$ corresponds to the subgroup $\langle F_1, F_2 \rangle$ generated by F_1 and F_2.
- The composite field E_1E_2 corresponds to the intersection $F_1 \cap F_2$.

Example:$\mathbb{Q}(\sqrt{2}+\sqrt{3})$
Consider the field $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. This is clearly a subfield of the Galois extension $\mathbb{Q}(\sqrt{2},\sqrt{3})$.
The other roots of the minimal polynomial for $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ are therefore the distinct conjugates of $\sqrt{2}+\sqrt{3}$ under the Galois group. These conjugates are:

$$\pm\sqrt{2} \pm \sqrt{3},$$

which are easily seen to be distinct.
Thus, the minimal polynomial is:

$$(x-(\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3})).$$

Expanding this product, we find the minimal polynomial:

$$x^4 - 10x^2 + 1.$$

It follows that this polynomial is irreducible over $\mathbb{Q}$, and hence:

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3}),$$

either by degree considerations or by noting that only the identity automorphism in the Galois group $\{\mathrm{id}, \sigma, \tau, \sigma\tau\}$ fixes $\sqrt{2}+\sqrt{3}$. Therefore, the fixing group for this field is the same as for $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Chapter 3

Infinite Galois Group

3.1 Infinite Galois Group, Transcendals Extensions

Definition 3.1.1.

1. *A subset $\{a_1, a_2, \ldots, a_n\} \subseteq E$ is called **algebraically independent over** F if there is no nonzero polynomial $f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$ such that*
$$f(a_1, a_2, \ldots, a_n) = 0.$$
*An arbitrary subset $S \subseteq E$ is called **algebraically independent over** F if every finite subset of S is algebraically independent. The elements of S are called **independent transcendentals** over F.*

2. *A **transcendence base** for E/F is a maximal subset (with respect to inclusion) of E which is algebraically independent over F.*

Note that if E/F is algebraic, the empty set is the only algebraically independent subset of E. In particular, elements of an algebraically independent set are necessarily transcendental.

Moreover, one easily checks that $S \subseteq E$ is an algebraically independent set over F if and only if each $s \in S$ is transcendental over $F(S \setminus \{s\})$.

It is also an easy exercise to see that S is a transcendence base for E/F if and only if S is a set of algebraically independent transcendentals over F and E is algebraic over $F(S)$.

Theorem 3.1.2. *The extension E/F has a transcendence base and any two transcendence bases of E/F have the same cardinality.*

Sketch of Proof. The existence of a transcendence base follows from Zorn's Lemma.

The uniqueness of the cardinality of a transcendence base follows from the same "Replacement Lemma" idea used in linear algebra to show that any two bases of a vector space have the same cardinality. □

Definition 3.1.3. *The cardinality of a transcendence base for E/F is called the* ***transcendence degree*** *of E/F.*

Algebraic extensions are precisely the extensions of transcendence degree 0. One special case of this theorem is when E is finitely generated over F, that is,

$$E = F(a_1, a_2, \ldots, a_r),$$

for some (not necessarily algebraically independent) elements $a_1, \ldots, a_r$ of E. It is clear that we may renumber $a_1, \ldots, a_r$ so that $a_1, \ldots, a_m$ are independent transcendentals and $a_{m+1}, \ldots, a_r$ are algebraic over $F(a_1, \ldots, a_m)$ (so E is a finite extension of the latter field). In this case, E is called a **function field in m variables over F**. Such fields play a fundamental role in algebraic geometry as fields of functions on m-dimensional surfaces. For instance, when $F = \mathbb{C}$ and $m = 1$, these fields arise in analysis as fields of meromorphic functions on compact Riemann surfaces.

Note that if S_1 and S_2 are transcendence bases for E/F it is not necessarily the case that $F(S_1) = F(S_2)$. For example, if t is transcendental over $\mathbb{Q}$, then $\{t\}$ and $\{t^2\}$ are both transcendence bases for $\mathbb{Q}(t)/\mathbb{Q}$, but (as we shall see shortly) $\mathbb{Q}(t^2)$ is a proper subfield of $\mathbb{Q}(t)$.

We now see that if $X_1, X_2, \ldots, X_n$ are indeterminates over F and

$$f(x) = (x - X_1)(x - X_2) \cdots (x - X_n) \tag{14.28}$$

is the general polynomial of degree n, then the set of n elementary symmetric functions $s_1, s_2, \ldots, s_n$ in the X_i are also independent transcendentals over F. This is because $X_1, \ldots, X_n$ is a transcendence base for $E = F(X_1, \ldots, X_n)$ over F (so the transcendence degree is n), and E is algebraic over $F(s_1, \ldots, s_n)$ (of degree $n!$). The theorem forces $s_1, \ldots, s_n$ to be a transcendence base for this extension as well (in particular, they are independent transcendentals). The general polynomial of degree n over F may therefore equivalently be defined by taking $a_1, \ldots, a_n$ to be any independent transcendentals (or indeterminates) and letting

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \tag{14.29}$$

where the roots of f are denoted by $X_1, \ldots, X_n$ (and $s_i = (-1)^i a_i$).

Definition 3.1.4. *An extension E/F is called* purely transcendental *if it has a transcendence base S such that $E = F(S)$.*

In the preceding discussion, both $F(X_1, \ldots, X_n)$ and $F(s_1, \ldots, s_n)$ are purely transcendental over F. As an exercise, one can show that $\mathbb{Q}(t, \sqrt{t})$ is not a purely transcendental extension of $\mathbb{Q}$, even though it contains no elements that are algebraic over $\mathbb{Q}$ other than those in $\mathbb{Q}$ itself (i.e., the process of decomposing a general extension into a purely transcendental extension followed by an algebraic extension cannot generally be reversed so that the algebraic piece occurs first).

If E is a purely transcendental extension of F of transcendence degree $n = 1$ or 2 and L is an intermediate field, $F \subseteq L \subseteq E$ with the same transcendence degree, then L is again a purely transcendental extension of F (Lüroth ($n = 1$), Castelnuovo ($n = 2$)). This result is not true if the transcendence degree is ≥ 3, however, although examples where L fails to be purely transcendental are difficult to construct. For extensions of transcendence degree 1, the intermediate fields are described by the following theorem.

Theorem 3.1.5. *Let t be transcendental over a field F.*

1. ***(Lüroth)** If $F \subseteq K \subseteq F(t)$, then $K = F(r)$ for some $r \in F(t)$. In particular, every nontrivial intermediate field of $F(t)/F$ is purely transcendental over F.*

2. *If $P = P(t), Q = Q(t)$ are nonzero, relatively prime polynomials in $F[t]$, and not both constant, then*

$$[F(t) : F(P/Q)] = \max(\deg P, \deg Q).$$

Proof. The proof of part (2) is outlined in Exercise 18 of Section 13.2.

By part (2), we see that $F(P/Q) = F(t)$ if and only if P and Q are nonzero, relatively prime polynomials of degree at least 1 (i.e., not both constant). Thus,

$$F(r) = F(t) \iff r = \frac{at + b}{ct + d}, \quad \text{where } a, b, c, d \in F \text{ and } ad - bc \neq 0,$$

i.e., r is a **fractional linear transformation** of t.

For any $r \in F(t) \setminus F$, the map $t \mapsto r$ extends to an embedding of $F(t)$ into itself which fixes F. This embedding is surjective (i.e., an automorphism of $F(t)$ over F) if and only if r is a fractional linear transformation.

Define a map

$$\mathrm{GL}_2(F) \to \mathrm{Aut}(F(t)/F)$$

by

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \alpha_A,$$

where α_A is the automorphism of $F(t)$ defined by

$$\alpha_A(t) = \frac{at+b}{ct+d}.$$

This map is a surjective group homomorphism whose kernel consists of scalar matrices. Hence,

$$\mathrm{Aut}(F(t)/F) \cong \mathrm{PGL}_2(F),$$

where $\mathrm{PGL}_2(F) = \mathrm{GL}_2(F)/\{\lambda I \mid \lambda \in F^\times\}$.

If F is a finite field of order q, then $\mathrm{Aut}(F(t)/F) \cong \mathrm{PGL}_2(F)$ is a finite group of order

$$q(q-1)(q+1).$$

By Corollary 11, if K is the fixed field of $\mathrm{Aut}(F(t)/F)$, then $F(t)$ is Galois over K, with

$$\mathrm{Gal}(F(t)/K) = \mathrm{Aut}(F(t)/F).$$

In particular, $K \neq F$ in this case.

This provides further examples of the Galois correspondence, which can be written out explicitly for small values of q. For instance, if $q = |F| = 2$, then $\mathrm{PGL}_2(F)$ is a nonabelian group of order 6, hence isomorphic to S_3, and has the following lattice of subgroups: The field $F(t)$ is of degree 6 over

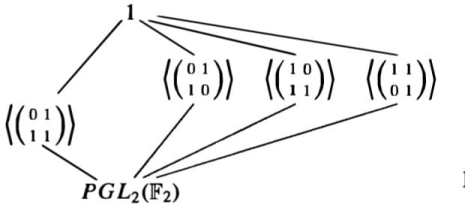


Figure 3.1:

the fixed field K of $\mathrm{Aut}(F(t)/F)$, and the lattice of subfields $K \subseteq L \subseteq F(t)$ is dual to the lattice of subgroups of S_3. The cyclic subgroup $\langle a \rangle$ is easily

found (via the preceding theorem) by finding a rational function r in t which is fixed by a such that

$$[\mathrm{IF}(t) : \mathrm{IF}(r)] = |a|.$$

For example, if

$$a : t \mapsto \frac{1}{1+t},$$

then a has order 3. The rational function

$$r = t + a(t) + a^2(t) = \frac{t^3 + t + 1}{t(t+1)}$$

is fixed by a and $[\mathrm{IF}(t) : \mathrm{IF}(r)] = 3$ (by part (2) of the theorem). Since $\mathrm{IF}(r)$ is contained in the fixed field of $\langle a \rangle$ and the degree of $\mathrm{IF}(t)$ over the fixed field is 3, $\mathrm{IF}(r)$ is the fixed field of $\langle a \rangle$. In this way, one can explicitly describe the lattice of all subfields of $\mathrm{IF}(t)$ containing K, shown in Figure 3.2.

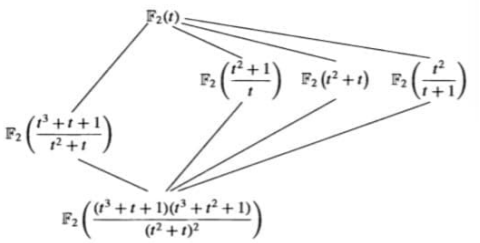


Figure 3.2:

Purely transcendental extensions of $\mathbb{Q}$ play an important role in the problem of realizing finite groups as Galois groups over $\mathbb{Q}$. We describe a deep result of Hilbert which is fundamental to this area of research. If $a_1, a_2, \ldots, a_n$ are independent indeterminates over a field F, we may evaluate (or specialize) $a_1, \ldots, a_n$ at any elements of F, i.e., substitute values in F for the "variables" $a_1, a_2, \ldots, a_n$. If E is a Galois extension of $F(a_1, \ldots, a_n)$, then E is obtained as a splitting field of a polynomial whose coefficients lie in $F[a_1, \ldots, a_n]$. Any specialization of $a_1, \ldots, a_n$ into F maps this polynomial into one whose coefficients lie in F. The specialization of E is the splitting field of the resulting specialized polynomial.

Theorem 3.1.6 (Hilbert)**.** *Let $x_1, x_2, \ldots, x_n$ be independent transcendentals over $\mathbb{Q}$, let $E = \mathbb{Q}(x_1, \ldots, x_n)$, and let G be a finite group of automorphisms of E with fixed field K. If K is a purely transcendental extension of $\mathbb{Q}$ with transcendence basis $a_1, a_2, \ldots, a_n$, then there are infinitely many specializations of $a_1, \ldots, a_n$ in $\mathbb{Q}$ such that E specializes to a Galois extension of $\mathbb{Q}$ with Galois group isomorphic to G.*

Hilbert's Theorem gives a sufficient condition for the specialized extension not to collapse. In general, the Galois group of the specialized extension is a subgroup of G (cf. Proposition 19) and may be a proper subgroup of G. It is also known that the fixed...

Corollary. S_n is a Galois group over $\mathbb{Q}$, for all n.

Proof of the Corollary: We have already proved that the fixed field of S_n acting in the obvious fashion on $\mathbb{Q}(x_1, \ldots, x_n)$ is purely transcendental over $\mathbb{Q}$ (with the elementary symmetric functions as a transcendence base), so Hilbert's Theorem immediately implies the corollary.

The hypothesis that K be purely transcendental over $\mathbb{Q}$ is crucial to the proof of Hilbert's Theorem. Every finite group is isomorphic to a subgroup of S_n and so acts on $\mathbb{Q}(x_1, \ldots, x_n)$ for some n. It is not known, however, even for the subgroup A_n of S_n whether its fixed field under the obvious action is a purely transcendental extension of $\mathbb{Q}$ (although it is known by other means that A_n is a Galois group over $\mathbb{Q}$ for all n). Thus there are a number of important open problems in this area of research.

One should also notice that Hilbert's Theorem does not work when the base field $\mathbb{Q}$ is replaced by an arbitrary field F (suppose F were algebraically closed, for instance). In particular, as noted earlier, the general polynomial $f(x)$ in Section 6 has Galois group S_n over $F(a_1, \ldots, a_n)$ for any F, but when F is a finite field, the specialized extension

obtained from its splitting field is always cyclic.

We next expand on the theory of inseparable extensions described in Section 13.5. Let p be a prime and let F be a field of characteristic p.

3.2 Inseperable Extensions

Definition 3.2.1. *An algebraic extension E/F is called* purely inseparable *if for each $a \in E$, the minimal polynomial of a over F has only one distinct root.*

It is easy to see that the following are equivalent:

1. E/F is purely inseparable.
2. If $a \in E$ is separable over F, then $a \in F$.
3. For every $a \in E$, there exists $n \geq 0$ such that $a^{p^n} \in F$, and the minimal polynomial $m_{a,F}(x) = x^{p^n} - a^{p^n}$.

The following easy proposition describes composites of separable and purely inseparable extensions:

Proposition 1. *Let E/F be an algebraic extension. Suppose E_1 is a separable extension of F and E_2 is a purely inseparable extension of F. Then the composite field E_1E_2 is a finite extension of F whose separable degree is $[E_1 : F]$ and whose inseparable degree is $[E_2 : F]$.*

Proposition 2. *Let E/F be an algebraic extension. Then there is a unique field E_{sep} with $F \subseteq E_{\text{sep}} \subseteq E$ such that E_{sep} is separable over F, and E is purely inseparable over E_{sep}. The field E_{sep} is the set of elements of E which are separable over F.*

The degree $[E_{\text{sep}} : F]$ is called the *separable degree* of E/F, and the degree $[E : E_{\text{sep}}]$ is called the *inseparable degree* of E/F (often denoted $[E : F]_s$ and $[E : F]_i$, respectively). The product of these two degrees is the (ordinary) degree of the field extension.
Corollary Separable degrees (respectively inseparable degrees) are multiplicative.
When E is generated over F by a root of an irreducible polynomial $p(x) \in F[x]$, the separable and inseparable degrees of the extension E/F are the same as the separable and inseparable degrees of the polynomial $p(x)$, as defined in Section 13.5.

The proposition asserts that any algebraic extension may be decomposed into a separable extension followed by a purely inseparable one. Exercise 3 at the end of this section outlines an example illustrating that this decomposition cannot generally be reversed; namely, there exist extensions which are not separable extensions of a purely inseparable extension.

We shall shortly state conditions under which the decomposition into separable and purely inseparable subextensions *can* be reversed.

We now know that an arbitrary extension E/F can be decomposed into:

- a purely transcendental extension $F(S)$ of F,
- followed by a separable algebraic extension E_1 of $F(S)$,
- followed by a purely inseparable extension E/E_1.

In certain instances, the inseparability in the algebraic extension at the "top" may be removed by a judicious choice of transcendence base:

Proposition 3. *If E is a finitely generated extension of a perfect field F, then there is a transcendence base T of E/F such that E is a separable (algebraic) extension of $F(T)$.*

A transcendence base T as described in the proposition is called a *separating transcendence base*. Exercise 4 at the end of this section illustrates this with a nontrivial example.

Recall that an extension E/F is *normal* if it is the splitting field of some (possibly infinite) set of polynomials in $F[x]$. In particular, normal extensions are algebraic but not necessarily finite or separable. We previously used the synonymous term *splitting field*, and the term *normal* is reintroduced here in the context of arbitrary algebraic extensions, since it is frequently used in the literature — often in the context of embeddings of a field into an algebraic closure.

Although the following set of equivalences can be gleaned from the preceding sections, the reader should write out a complete proof, checking that the arguments work for both infinite and inseparable extensions. In order to discuss the set of subgroups of $\mathrm{Gal}(E/F)$, we must introduce a topology on this group (called the *Krull topology*). The axioms for the collection of (topologically) closed subsets of a topological space are precisely the bookkeeping devices which single out the relevant subgroups.

Galois theory for finite extensions forces certain subgroups of finite index to be closed sets, and these in turn determine the topology on the entire group (as we might expect, since every extension of F inside E is a composite of finite extensions).

Moreover, the Galois group $\mathrm{Gal}(E/F)$ is the inverse limit of the collection of finite groups $\mathrm{Gal}(K/F)$, where K runs over all finite Galois extensions of F contained in E.

$$\mathrm{Gal}(E/F) \cong \varprojlim_{K \subseteq E} \mathrm{Gal}(K/F)$$

Definition 3.2.2. *An extension E/F is called* Galois *if it is algebraic, normal, and separable. In this case,* $\mathrm{Aut}(E/F)$ *is called the* Galois group *of the extension and is denoted by* $\mathrm{Gal}(E/F)$.

For infinite extensions, there need not be a bijection between the set of all subgroups of the Galois group and the set of all subfields of E containing F, as the following example illustrates.

Let E be the subfield of $\mathbb{R}$ obtained by adjoining to $\mathbb{Q}$ all square roots of positive rational numbers. One easily sees that E may also be described as the splitting field of the set of polynomials

$$x^2 - p,$$

where p runs over all primes in $\mathbb{Z}^+$. Note that E is a (countably) infinite Galois extension of $\mathbb{Q}$.

Since every automorphism α of E is determined by its action on the square roots of the primes and α either fixes or negates each of these, it follows that α^2 is the identity automorphism. Thus, $\mathrm{Aut}(E)$ is an infinite elementary abelian 2-group. In particular, $\mathrm{Aut}(E)$ is an infinite-dimensional vector space over $\mathbb{F}_2$.

By an exercise in the section on dual spaces (Section 11.3), the number of nonzero homomorphisms of $\mathrm{Aut}(E)$ into $\mathbb{F}_2$ is uncountable, whence their kernels (which are subspaces of codimension 1) are uncountable in number (and distinct). Thus, $\mathrm{Aut}(E)$ has uncountably many subgroups of index 2, whereas $\mathbb{Q}$ has only a countable number of quadratic extensions.
The basic problem is that many (most) subgroups of $\mathrm{Gal}(E/F)$ do not correspond (in a bijective fashion) to subfields of E containing F. In order to pick out the relevant subgroups, one must introduce a suitable topology on $\mathrm{Gal}(E/F)$ (such as the Krull topology), which singles out the closed subgroups corresponding to intermediate fields. To make sense of the set of subgroups of $\mathrm{Gal}(E/F)$, we must introduce a topology on this group, called the *Krull topology*. The axioms for the collection of (topologically) closed subsets of a topological space serve as bookkeeping tools to single out the relevant subgroups — these are listed in Section 15.2.

Galois theory for finite extensions forces certain subgroups of finite index to be closed, and these in turn determine the topology on the entire group. This is to be expected, since every extension of F inside E is a composite of finite extensions.

Moreover, the Galois group $\mathrm{Gal}(E/F)$ is the inverse limit of the collection of finite groups $\mathrm{Gal}(K/F)$, where K runs over all finite Galois extensions of F contained in E:

$$\mathrm{Gal}(E/F) \cong \varprojlim_{K \subseteq E} \mathrm{Gal}(K/F).$$

Theorem 3.2.3 (Krull)**.** *Let E/F be a Galois extension with Galois group G. Topologize G by taking as a base for the closed sets the subgroups of G which are the fixing subgroups of the finite extensions of F in E, together with all left and right cosets of these subgroups.*

Then, with this ("Krull") topology, the closed subgroups of G correspond bijectively with the subfields of E containing F, and the corresponding lattices are dual. Closed normal subgroups of G correspond to normal extensions of F in E.

One important area of current research is to describe (as a topological group) the Galois group of certain field extensions such as $\overline{F}/F$, where $\overline{F}$ is the algebraic closure of F. Little is known about the latter group when

$F = \mathbb{Q}$ (in particular, its normal subgroups of finite index, i.e., which finite groups occur as Galois groups over $\mathbb{Q}$, are not known).

If E is the algebraic closure of the finite field $\mathbb{F}_p$, then

- The Galois group of this extension is the topologically cyclic group $\widehat{\mathbb{Z}}$ (the profinite completion of $\mathbb{Z}$) with the Frobenius automorphism as a topological generator.
- The group $\widehat{\mathbb{Z}}$ is an uncountable group (in particular, it is not isomorphic to $\mathbb{Z}$) with the property that every closed subgroup of finite index is normal with cyclic quotient.
- Note that $\widehat{\mathbb{Z}}$ must also have nontrivial infinite closed subgroups (unlike $\mathbb{Z}$), since E contains proper subfields which are infinite over $\mathbb{F}_p$ (such as the composite of all extensions of $\mathbb{F}_p$ of q-power degree, for any prime q).
- This Galois extension of $\mathbb{F}_p$ has Galois group $\mathbb{Z}_q$, the q-adic integers.

Chapter 4

Conclusion

Through this internship project on **Galois Field Extensions**, I have explored both the classical and modern perspectives of Galois theory, with particular focus on **infinite Galois extensions**. Starting from foundational concepts such as *field automorphisms*, *Galois groups*, and *splitting fields*, I gained a clear understanding of finite Galois extensions and the **Fundamental Theorem of Galois Theory**, which establishes a deep correspondence between subgroups of the Galois group and intermediate fields.
Progressing further, I examined **infinite Galois groups** and extensions involving *transcendental and inseparable elements*. I learned how the classical Galois correspondence can be generalized using **Krull topology**, which provides a topological structure on the Galois group to handle infinite extensions. The study of *transcendence bases*, *purely transcendental extensions*, and **Hilbert's Irreducibility Theorem** broadened my understanding of fields beyond algebraic extensions.

Key insights include:

- The bijective, inclusion-reversing correspondence between subfields and subgroups in finite Galois extensions.
- The role of **normal and separable extensions** in defining Galois groups.
- The concept of *transcendence degree* and how it characterizes non-algebraic extensions.
- The importance of **Krull topology** for describing infinite Galois groups via inverse limits.

- Applications of Galois theory in *constructing field extensions with desired Galois groups*, as illustrated by **Hilbert's Theorem** and the realization of symmetric groups over $\mathbb{Q}$.

Overall, this project has deepened my appreciation for the intricate relationship between field theory and group theory, and has equipped me with foundational tools essential for further research in algebra, number theory, and algebraic geometry.

Bibliography

[1] David S. Dummit and Richard M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, 2004.