Abstract Algebra II

Fields and Galois Theory

Undergraduate Course — L3

Contents

Preface

On the morning of 30 May 1832, a twenty-year-old mathematician named Évariste Galois was fatally wounded in a duel. The night before, fully expecting to die, he had spent hours feverishly writing letters and manuscripts, scribbling in the margins *"I have no time"* as he raced to set down the ideas that had consumed him for years. Those hastily written pages would eventually revolutionise mathematics.

Galois had discovered a profound connection between two seemingly disparate areas of algebra: the theory of polynomial equations and the theory of groups. He showed that to every polynomial equation one can attach a group — now called the *Galois group* — and that the solvability of the equation by radicals is completely determined by the structure of this group. In doing so, he not only settled the centuries-old problem of solving polynomial equations of degree five and higher, but he also laid the foundations for what we now call *abstract algebra*.

This course, *Abstract Algebra II*, is devoted to the theory of fields and the Galois correspondence. It is a continuation of a first course in abstract algebra (groups and rings) and is designed for third-year undergraduate students. Our journey will proceed as follows:

- **Chapters 8–10.** We develop the theory of field extensions: algebraic and transcendental elements, splitting fields, separability, algebraic closure, and the structure of finite fields.
- **Chapters 11–13.** We establish the Galois correspondence and apply it: normal extensions, the fundamental theorem, and computational techniques for determining Galois groups.
- **Chapter 14.** We reach the summit: the proof that the general polynomial of degree ≥ 5 is not solvable by radicals.

The prerequisites are a solid understanding of groups, rings, and ideals at the level of a standard first course. We make free use of quotient rings, polynomial rings, and the theory of principal ideal domains.

The reader is encouraged to attempt every exercise; it is only through sustained effort that the beauty and power of Galois theory reveals itself. Many of the exercises develop important examples or complete technical details left to the reader in the text.

The Authors

Notation

Symbol	Meaning
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	Natural numbers, integers, rationals, reals, complex numbers
$\mathbb{F}_q$	Finite field with q elements
K, L, M, F	Fields
L/K	Field extension: L is an extension of K
$[L : K]$	Degree of the extension L/K
$K(\alpha), K(\alpha_1, \ldots, \alpha_n)$	Field generated by α (resp. $\alpha_1, \ldots, \alpha_n$) over K
$K[\alpha]$	Ring generated by α over K
$K[X]$	Polynomial ring over K in one indeterminate
$\mathrm{irr}(\alpha, K)$	Minimal polynomial of α over K
$\deg f$	Degree of a polynomial f
$\mathrm{char}(K)$	Characteristic of a field K
$\mathrm{Gal}(L/K)$	Galois group of the extension L/K
$\mathrm{Aut}(L)$	Automorphism group of L
$\mathrm{Aut}_K(L)$	Group of K-automorphisms of L
$\mathrm{Hom}_K(L, M)$	Set of K-algebra homomorphisms from L to M
$\mathrm{Fix}(H)$	Fixed field of a subgroup $H \leq \mathrm{Aut}(L)$
id	Identity map
f'	Formal derivative of the polynomial f
$\langle S \rangle$	Subgroup (or ideal, or subfield) generated by S
$\lvert G \rvert$, $[G : H]$	Order of a group G, index of H in G
$G \cong H$	G is isomorphic to H
$G \rtimes H$	Semidirect product
S_n, A_n, D_n, C_n	Symmetric, alternating, dihedral, cyclic groups

Part I

Fields and Extensions

Chapter 1

Fields — Algebraic and Transcendental Extensions

1.1 Field extensions and degree

Definition 1.1 (Field extension)**.** A **field extension** is a pair of fields $K \subseteq L$ (equivalently, an injective ring homomorphism $\iota\colon K \hookrightarrow L$). We write L/K and call K the **base field** and L the **extension field**.

Any field extension L/K makes L into a K-vector space via the multiplication of L.

Definition 1.2 (Degree of an extension)**.** The **degree** of the extension L/K, denoted $[L : K]$, is the dimension of L as a K-vector space:

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

If $[L : K] < \infty$, we say L/K is a **finite extension**. Otherwise it is an **infinite extension**.

Example 1.1 (Basic examples). (i) $\mathbb{C}/\mathbb{R}$ has degree $[\mathbb{C} : \mathbb{R}] = 2$, with basis $\{1, i\}$.

(ii) $\mathbb{R}/\mathbb{Q}$ is an infinite extension (in fact $\mathbb{R}$ is uncountable while $\mathbb{Q}$ is countable).

(iii) For any field K, the extension K/K has degree 1.

(iv) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has degree 2, with basis $\{1, \sqrt{2}\}$.

Theorem 1.1 (Tower Law)**.** Let $K \subseteq L \subseteq M$ be fields. Then M/K is finite if and only if both M/L and L/K are finite, in which case

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

Proof. Let $\{e_1, \dots, e_m\}$ be a basis of L over K (so $m = [L : K]$), and let $\{f_1, \dots, f_n\}$ be a basis of M over L (so $n = [M : L]$). We claim that the set

$$\mathcal{B} = \{e_i f_j : 1 \le i \le m,\ 1 \le j \le n\}$$

is a basis of M over K. This set has mn elements, so the result will follow.

Spanning. Let $x \in M$. Since $\{f_1, \dots, f_n\}$ is a basis of M/L, we can write

$$x = \sum_{j=1}^{n} \lambda_j f_j, \quad \lambda_j \in L.$$

Since $\{e_1, \dots, e_m\}$ is a basis of L/K, each λ_j can be written as

$$\lambda_j = \sum_{i=1}^{m} a_{ij} e_i, \quad a_{ij} \in K.$$

Substituting:

$$x = \sum_{j=1}^{n} \Big(\sum_{i=1}^{m} a_{ij} e_i \Big) f_j = \sum_{i,j} a_{ij}\, e_i f_j.$$

Hence $\mathcal{B}$ spans M over K.

Linear independence. Suppose

$$\sum_{i,j} a_{ij}\, e_i f_j = 0, \quad a_{ij} \in K.$$

Rewriting:

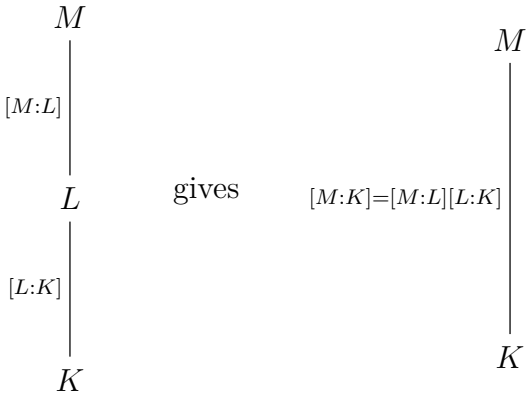
$$\sum_{j=1}^{n} \Big(\sum_{i=1}^{m} a_{ij} e_i \Big) f_j = 0.$$

Set $\mu_j = \sum_{i=1}^{m} a_{ij} e_i \in L$. Since $\{f_1, \dots, f_n\}$ is linearly independent over L, we have $\mu_j = 0$ for all j. But then $\sum_{i=1}^{m} a_{ij} e_i = 0$ with $a_{ij} \in K$, and the linear independence of $\{e_1, \dots, e_m\}$ over K gives $a_{ij} = 0$ for all i, j. Thus $\mathcal{B}$ is linearly independent.

For the "if and only if" part: if $[M : K]$ is finite, then since L is a K-subspace of M and M is a finite-dimensional K-vector space, L is also finite-dimensional over K, so $[L : K]$ is finite. Moreover, any L-linearly independent subset of M is also K-linearly independent (since $L \supseteq K$), so $[M : L] \leq [M : K]$ and $[M : L]$ is finite.

Conversely, if both $[M : L]$ and $[L : K]$ are finite, then the basis $\mathcal{B}$ constructed above shows $[M : K] = [M : L][L : K] < \infty$. □

The following diagram illustrates the tower law.



Corollary 1.1 (Degree divides)**.** If $K \subseteq L \subseteq M$ and $[M : K]$ is finite, then $[L : K]$ divides $[M : K]$.

Proof. By the tower law, $[M : K] = [M : L] \cdot [L : K]$. □

1.2 Algebraic elements and minimal polynomials

Definition 1.3 (Algebraic and transcendental elements)**.** Let L/K be a field extension and $\alpha \in L$.

(i) α is **algebraic** over K if there exists a nonzero polynomial $f \in K[X]$ such that $f(\alpha) = 0$.

(ii) α is **transcendental** over K if it is not algebraic over K.

Definition 1.4 (Evaluation homomorphism)**.** For $\alpha \in L$, the **evaluation homomorphism** is the ring homomorphism

$$\mathrm{ev}_\alpha \colon K[X] \longrightarrow L, \quad f(X) \longmapsto f(\alpha).$$

Its image is the subring $K[\alpha] \subseteq L$, and its kernel $\mathrm{Ker}(\mathrm{ev}_\alpha)$ is an ideal of $K[X]$.

Since $K[X]$ is a principal ideal domain, $\mathrm{Ker}(\mathrm{ev}_\alpha) = (g)$ for some $g \in K[X]$. If α is algebraic, then $g \neq 0$; if α is transcendental, then $g = 0$.

Theorem 1.2 (Existence and uniqueness of the minimal polynomial)**.** Let L/K be a field extension and let $\alpha \in L$ be algebraic over K. There exists a unique monic polynomial $m_\alpha = \mathrm{irr}(\alpha, K) \in K[X]$ such that:

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

(ii) If $f \in K[X]$ satisfies $f(\alpha) = 0$, then $m_\alpha \mid f$ in $K[X]$.

(iii) m_α is irreducible in $K[X]$.

(iv) $\mathrm{Ker}(\mathrm{ev}_\alpha) = (m_\alpha)$.

The polynomial m_α is called the **minimal polynomial** of α over K.

Proof. Since α is algebraic, $I = \mathrm{Ker}(\mathrm{ev}_\alpha)$ is a nonzero ideal of $K[X]$. Because $K[X]$ is a PID, $I = (m_\alpha)$ for a unique monic generator $m_\alpha \in K[X]$.

(i) Since $\mathrm{ev}_\alpha(m_\alpha) = m_\alpha(\alpha)$ and $m_\alpha \in I = \mathrm{Ker}(\mathrm{ev}_\alpha)$, we have $m_\alpha(\alpha) = 0$.

(ii) If $f(\alpha) = 0$, then $f \in I = (m_\alpha)$, so $m_\alpha \mid f$.

(iii) We show m_α is irreducible. Since m_α generates $\mathrm{Ker}(\mathrm{ev}_\alpha)$ and α is algebraic, $\deg m_\alpha \geq 1$. Suppose $m_\alpha = gh$ with $g, h \in K[X]$ and $\deg g, \deg h \geq 1$. Then $0 = m_\alpha(\alpha) = g(\alpha)h(\alpha)$. Since L is a field (and hence an integral domain), either $g(\alpha) = 0$ or $h(\alpha) = 0$. Say $g(\alpha) = 0$; then $g \in (m_\alpha)$, so $m_\alpha \mid g$, which is impossible since $\deg g < \deg m_\alpha$. This contradiction shows m_α is irreducible.

Uniqueness. If m' is another monic polynomial satisfying (i)–(iii), then $m_\alpha \mid m'$ by (ii) applied to m_α, and $m' \mid m_\alpha$ by the analogous property of m'. Since both are monic, $m_\alpha = m'$. □

Example 1.2 (Minimal polynomials). (i) $\mathrm{irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$. Indeed, $\sqrt{2}$ is a root of $X^2 - 2$, and this polynomial is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with

$p = 2$.

(ii) $\operatorname{irr}(i, \mathbb{Q}) = X^2 + 1$. The polynomial $X^2 + 1$ has no rational roots and is therefore irreducible over $\mathbb{Q}$.

(iii) $\operatorname{irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$, irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$.

(iv) $\operatorname{irr}(\sqrt{2}, \mathbb{Q}(\sqrt{2})) = X - \sqrt{2}$, since $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

1.3 The structure of simple extensions

Theorem 1.3 (Structure of simple algebraic extensions)**.** Let L/K be a field extension and $\alpha \in L$ algebraic over K with minimal polynomial $m_\alpha = \operatorname{irr}(\alpha, K)$ of degree n. Then:

(i) There is a K-algebra isomorphism

$$K[X]/(m_\alpha) \xrightarrow{\sim} K(\alpha), \qquad \overline{X} \longmapsto \alpha.$$

(ii) $K(\alpha) = K[\alpha]$, i.e. the field generated by α over K equals the ring generated by α over K.

(iii) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a K-basis of $K(\alpha)$.

(iv) $[K(\alpha) : K] = \deg m_\alpha = n$.

Proof. Consider the evaluation homomorphism $\operatorname{ev}_\alpha \colon K[X] \to L$, $f(X) \mapsto f(\alpha)$. Its image is $K[\alpha]$ and its kernel is (m_α) by Theorem 1.2. By the first isomorphism theorem for rings:

$$K[X]/(m_\alpha) \cong K[\alpha].$$

Since m_α is irreducible in the PID $K[X]$, the ideal (m_α) is maximal, so $K[X]/(m_\alpha)$ is a field. Therefore $K[\alpha]$ is a field, and since it is a subfield of L containing K and α, it must be the smallest such field, i.e. $K[\alpha] = K(\alpha)$. This proves (i) and (ii).

For (iii), every element of $K[X]/(m_\alpha)$ is represented by a polynomial of degree $< n = \deg m_\alpha$ (by the division algorithm), and these representatives are unique. Under the isomorphism, the images of $\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}$ are $1, \alpha, \ldots, \alpha^{n-1}$. Since $\{\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}\}$ is a K-basis of $K[X]/(m_\alpha)$, it follows that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a K-basis of $K(\alpha)$. Part (iv) is immediate from (iii). □

Example 1.3 ($\mathbb{Q}(\sqrt{2})$). Since $\operatorname{irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$ has degree 2, we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \cong \mathbb{Q}[X]/(X^2 - 2).$$

Example 1.4 ($\mathbb{Q}(\sqrt[3]{2})$). Since $\operatorname{irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$ has degree 3, we get $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}.$$

Example 1.5 ($\mathbb{Q}(i)$). Since $\operatorname{irr}(i, \mathbb{Q}) = X^2 + 1$, we have $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ and

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\} \cong \mathbb{Q}[X]/(X^2 + 1).$$

This is the field of **Gaussian rationals**.

1.4 Finite implies algebraic

Theorem 1.4 (Finite implies algebraic)**.** If L/K is a finite extension, then every element of L is algebraic over K.

Proof. Let $n = [L : K]$ and let $\alpha \in L$. Consider the $n+1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ in the n-dimensional K-vector space L. They must be linearly dependent over K, so there exist $a_0, a_1, \ldots, a_n \in K$, not all zero, such that

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0.$$

The polynomial $f(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ is nonzero and satisfies $f(\alpha) = 0$. Hence α is algebraic over K. □

Remark 1.1 (Converse is false). The converse is false in general: an extension can be algebraic but infinite. For example, the algebraic closure $\overline{\mathbb{Q}}/\mathbb{Q}$ is algebraic but $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Definition 1.5 (Algebraic extension)**.** A field extension L/K is **algebraic** if every element of L is algebraic over K. Otherwise it is **transcendental**.

Theorem 1.5 (Algebraic over algebraic is algebraic)**.** If M/L is algebraic and L/K is algebraic, then M/K is algebraic.

Proof. Let $\alpha \in M$. We must show that α is algebraic over K. Since M/L is algebraic, α is algebraic over L, so there exists a polynomial

$$f(X) = b_0 + b_1X + \cdots + b_nX^n \in L[X], \quad b_n \neq 0,$$

with $f(\alpha) = 0$. Consider the intermediate field $K' = K(b_0, b_1, \ldots, b_n)$.

Since L/K is algebraic, each b_i is algebraic over K. We build a tower of finite extensions:

$$K \subseteq K(b_0) \subseteq K(b_0, b_1) \subseteq \cdots \subseteq K(b_0, \ldots, b_n) = K'.$$

Each step is a simple algebraic extension, hence finite by Theorem 1.3(iv). By the tower law (Theorem 1.1), $[K' : K] < \infty$.

Now α is algebraic over $K' \supseteq L$ (since $f \in K'[X]$ and $f(\alpha) = 0$), so $[K'(\alpha) : K'] \leq n < \infty$. Applying the tower law once more:

$$[K'(\alpha) : K] = [K'(\alpha) : K'] \cdot [K' : K] < \infty.$$

Since $K \subseteq K'(\alpha)$ is a finite extension, α is algebraic over K by Theorem 1.4. □

Corollary 1.2 (Set of algebraic elements is a field)**.** Let L/K be a field extension. The set

$$\overline{K}_L = \{\alpha \in L : \alpha \text{ is algebraic over } K\}$$

is a subfield of L containing K.

Proof. Clearly $K \subseteq \overline{K}_L$. We must show that if $\alpha, \beta \in \overline{K}_L$ with $\beta \neq 0$, then $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, and α/β all lie in $\overline{K}_L$. These elements all belong to $K(\alpha,\beta)$, and

$$[K(\alpha,\beta):K] \leq [K(\alpha):K] \cdot [K(\alpha,\beta):K(\alpha)] < \infty,$$

since α is algebraic over K and β is algebraic over $K(\alpha)$ (because it is algebraic over $K \subseteq K(\alpha)$). By Theorem 1.4, every element of $K(\alpha,\beta)$ is algebraic over K. □

1.5 Transcendental extensions

Definition 1.6 (Purely transcendental extension)**.** Let L/K be a field extension and $\alpha \in L$ transcendental over K. The evaluation homomorphism $\mathrm{ev}_\alpha \colon K[X] \to L$ is injective (since $\mathrm{Ker} = (0)$), so it extends to an injective field homomorphism $K(X) \hookrightarrow L$, giving an isomorphism $K(\alpha) \cong K(X)$, the field of rational functions.

Remark 1.2 (Transcendence degree). The study of transcendental extensions leads to the notion of *transcendence degree*, which measures how many "independent transcendentals" are needed. The transcendence degree of $\mathbb{R}/\mathbb{Q}$ is $|\mathbb{R}|$ (uncountable). We will not develop this theory in detail, as our focus is on algebraic extensions and Galois theory.

1.6 Characteristic and the Frobenius endomorphism

Definition 1.7 (Characteristic)**.** The **characteristic** of a field K, denoted $\mathrm{char}(K)$, is the smallest positive integer p such that $\underbrace{1+1+\cdots+1}_{p} = 0$ in K. If no such integer exists, we set $\mathrm{char}(K) = 0$.

Proposition 1.1 (Characteristic is 0 or prime)**.** The characteristic of a field is either 0 or a prime number.

Proof. The unique ring homomorphism $\mathbb{Z} \to K$, $n \mapsto n \cdot 1_K$, has kernel (p) for some $p \geq 0$ (since $\mathbb{Z}$ is a PID). If $p \neq 0$, the image $\mathbb{Z}/(p)$ embeds in K, so $\mathbb{Z}/(p)$ is an integral domain, which forces p to be prime. □

Definition 1.8 (Prime subfield)**.** The **prime subfield** of K is the intersection of all subfields of K. It is isomorphic to $\mathbb{Q}$ if $\mathrm{char}(K) = 0$, and to $\mathbb{F}_p$ if $\mathrm{char}(K) = p$.

Theorem 1.6 (Frobenius endomorphism)**.** Let K be a field of characteristic $p > 0$. The map

$$\varphi \colon K \longrightarrow K, \quad x \longmapsto x^p,$$

is an injective field homomorphism, called the **Frobenius endomorphism**.

Proof. We verify the homomorphism properties.

Multiplicativity. For all $x, y \in K$: $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$.

Additivity. For all $x, y \in K$: $\varphi(x+y) = (x+y)^p$. By the binomial theorem,

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}.$$

For $1 \le k \le p-1$, the binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is divisible by p (since p is prime and does not divide $k!$ or $(p-k)!$ for $0 < k < p$). Hence $\binom{p}{k} \equiv 0$ in K for $1 \le k \le p-1$, and

$$(x+y)^p = x^p + y^p = \varphi(x) + \varphi(y).$$

$\varphi(1) = 1$**.** This is clear since $1^p = 1$.

Injectivity. Since K is a field and φ is a nonzero ring homomorphism, $\mathrm{Ker}(\varphi)$ is an ideal of K. The only ideals of a field are (0) and K itself. Since $\varphi(1) = 1 \neq 0$, we have $\mathrm{Ker}(\varphi) = (0)$, so φ is injective. □

Remark 1.3 (Frobenius and finite fields). If K is a finite field, then φ is also surjective (an injective map from a finite set to itself is a bijection), so φ is an automorphism. For infinite fields of characteristic p, the Frobenius need not be surjective. For instance, in $\mathbb{F}_p(t)$ (rational functions over $\mathbb{F}_p$), the element t is not a p-th power.

1.7 Finite fields: first examples

Example 1.6 (Finite fields of small order). (i) $\mathbb{F}_2 = \{0, 1\}$, the field with two elements.

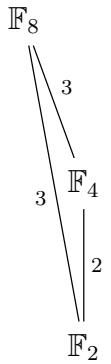
(ii) $\mathbb{F}_4$: since $4 = 2^2$, we seek an irreducible polynomial of degree 2 over $\mathbb{F}_2$. The polynomial $X^2 + X + 1$ is irreducible over $\mathbb{F}_2$ (it has no roots in $\mathbb{F}_2$), so

$$\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1) = \{0, 1, \alpha, 1+\alpha\},$$

where $\alpha^2 = \alpha + 1$.

(iii) $\mathbb{F}_8 \cong \mathbb{F}_2[X]/(X^3 + X + 1)$, since $X^3 + X + 1$ is irreducible over $\mathbb{F}_2$.

The following extension tower illustrates the relationship between these fields.



Note that $\mathbb{F}_4$ is *not* a subfield of $\mathbb{F}_8$ (since $2 \nmid 3$), which is why the diagram shows no direct inclusion arrow from $\mathbb{F}_4$ to $\mathbb{F}_8$.

1.8 Exercises

Exercise 1.1 (Degree computations). Determine $[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}]$ and find a basis for $\mathbb{Q}(\sqrt{3},\sqrt{5})$ over $\mathbb{Q}$. *Hint:* Use the tower law and show that $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$.

Exercise 1.2 (Minimal polynomial over an extension). Find $\operatorname{irr}(\sqrt{2}+\sqrt{3},\mathbb{Q})$ and show that it has degree 4. Deduce that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Exercise 1.3 (Algebraic element in a tower). Let $K \subseteq L \subseteq M$ be field extensions. Show that if $\alpha \in M$ is algebraic over K, then it is algebraic over L, and $\deg(\operatorname{irr}(\alpha, L)) \leq \deg(\operatorname{irr}(\alpha, K))$.

Exercise 1.4 (Degree and divisibility). Let α be algebraic over K with $\deg(\operatorname{irr}(\alpha,K)) = n$. Show that if $f \in K[X]$ satisfies $f(\alpha) = 0$ and $\deg f = n$, then f is a scalar multiple of $\operatorname{irr}(\alpha, K)$.

Exercise 1.5 (Simple extensions of finite fields). Show that $\mathbb{F}_{p^n}$ can be obtained as a simple extension $\mathbb{F}_p(\alpha)$ for some α. *Hint:* Use the fact that $\mathbb{F}_{p^n}^{\times}$ is cyclic (proved later in Theorem 3.6).

Exercise 1.6 (Compositum). Let L_1/K and L_2/K be finite extensions inside a common overfield M. Define the **compositum** L_1L_2 as the smallest subfield of M containing both L_1 and L_2. Show that

$$[L_1L_2 : K] \leq [L_1 : K]\,[L_2 : K],$$

with equality when $\gcd([L_1:K],[L_2:K]) = 1$.

Exercise 1.7 (Transcendence of e and π). State (without proof) the Lindemann–Weierstrass theorem and use it to show that e and π are transcendental over $\mathbb{Q}$.

Exercise 1.8 (Frobenius endomorphism). Let K be a field of characteristic $p > 0$. For $n \geq 1$, define $\varphi^n \colon K \to K$ by $\varphi^n(x) = x^{p^n}$. Show that φ^n is a field homomorphism.

Exercise 1.9 (Subfield criterion). Let L/K be a finite extension with $[L:K] = p$, a prime. Show that there are no intermediate fields strictly between K and L.

Exercise 1.10 (Algebraic numbers form a field). Let $\overline{\mathbb{Q}}$ denote the set of all complex numbers that are algebraic over $\mathbb{Q}$. Verify directly (without using Corollary 1.2) that $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.

Exercise 1.11 (Extension of degree 2). Let K be a field with $\operatorname{char}(K) \neq 2$ and L/K an extension with $[L:K] = 2$. Show that $L = K(\sqrt{d})$ for some $d \in K \setminus K^2$.

Exercise 1.12 (Infinite algebraic extension). Consider $L = \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\sqrt{7},\dots)$ (adjoining $\sqrt{p}$ for every prime p). Show that $L/\mathbb{Q}$ is algebraic but not finite.

Chapter summary

- A **field extension** L/K makes L a K-vector space; the degree $[L:K]$ is its dimension.
- The **tower law** gives $[M:K] = [M:L][L:K]$.
- An algebraic element α has a unique monic irreducible **minimal polynomial** $\operatorname{irr}(\alpha,K)$; the simple extension $K(\alpha) \cong K[X]/(\operatorname{irr}(\alpha,K))$ has degree equal to the degree of $\operatorname{irr}(\alpha,K)$.
- Finite $\Rightarrow$ algebraic, and algebraic over algebraic is algebraic.

- The **Frobenius endomorphism** $x \mapsto x^p$ is an injective field homomorphism in characteristic p.

Chapter 2

Splitting Fields

2.1 Definition and first examples

Definition 2.1 (Root of a polynomial in an extension)**.** Let K be a field and $f \in K[X]$ a polynomial of degree $n \geq 1$. An element α in some extension L/K is a **root** of f if $f(\alpha) = 0$.

Definition 2.2 (Polynomial splits)**.** We say that $f \in K[X]$ **splits** (or **splits completely**) over an extension field $L \supseteq K$ if f factors as a product of linear factors in $L[X]$:

$$f(X) = a \prod_{i=1}^{n} (X - \alpha_i), \quad \alpha_i \in L,\ a \in K^{\times}.$$

Definition 2.3 (Splitting field)**.** Let $f \in K[X]$ with $\deg f \geq 1$. A field $L \supseteq K$ is a **splitting field** of f over K if:

(i) f splits completely over L: writing $f(X) = a \prod_{i=1}^{n} (X - \alpha_i)$ with $\alpha_i \in L$;

(ii) L is generated over K by the roots of f: $L = K(\alpha_1, \ldots, \alpha_n)$.

Condition (ii) ensures that L is the *smallest* extension of K over which f splits.

Remark 2.1 (One root versus all roots). Given an irreducible polynomial $p(X) \in K[X]$ of degree n, the quotient $K[X]/(p(X))$ is a field extension of K of degree n in which p has *at least one* root (namely $\overline{X}$), but p need not split completely there. For example, $X^3 - 2 \in \mathbb{Q}[X]$ has one real root $\sqrt[3]{2}$, but $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ contains no complex cube roots of 2, so $X^3 - 2$ does not split over $\mathbb{Q}(\sqrt[3]{2})$.

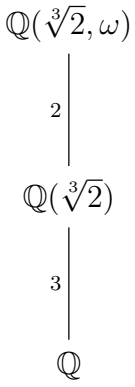
Example 2.1 (Splitting fields).

(i) $X^2 + 1$ **over** $\mathbb{R}$**:** The roots are $\pm i$, so the splitting field is $\mathbb{R}(i) = \mathbb{C}$, with $[\mathbb{C} : \mathbb{R}] = 2$.

(ii) $X^2 - 2$ **over** $\mathbb{Q}$**:** The roots are $\pm\sqrt{2}$, and $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$, so the splitting field is $\mathbb{Q}(\sqrt{2})$ with degree 2 over $\mathbb{Q}$.

(iii) $X^3 - 2$ **over** $\mathbb{Q}$**:** The three roots are $\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega$, $\sqrt[3]{2}\,\omega^2$, where $\omega = e^{2\pi i/3}$. The splitting field is $\mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq \mathbb{C}$.

We compute the degree using the tower



Indeed, $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$, and $\omega\notin\mathbb{Q}(\sqrt[3]{2})\subseteq\mathbb{R}$, so X^2+X+1 remains irreducible over $\mathbb{Q}(\sqrt[3]{2})$ (it has degree 2 and no real roots). Hence $[\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}(\sqrt[3]{2})]=2$ and

$$[\mathbb{Q}(\sqrt[3]{2},\omega):\mathbb{Q}]=3\cdot 2=6.$$

Example 2.2 (Cyclotomic splitting fields). The n-th **cyclotomic polynomial** $\Phi_n(X)\in\mathbb{Z}[X]$ is the minimal polynomial of a primitive n-th root of unity over $\mathbb{Q}$. Its splitting field over $\mathbb{Q}$ is the **cyclotomic field** $\mathbb{Q}(\zeta_n)$, where $\zeta_n=e^{2\pi i/n}$, and $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\varphi(n)$ (Euler's totient function).

2.2 Existence of splitting fields

Theorem 2.1 (Existence of splitting fields)**.** For every field K and every polynomial $f\in K[X]$ with $\deg f=n\geq 1$, there exists a splitting field L of f over K, with $[L:K]\leq n!$.

Proof. We proceed by induction on $n=\deg f$.

Base case ($n=1$). If $\deg f=1$, then f is already linear, $f(X)=a(X-\alpha)$ with $\alpha\in K$, and $L=K$ is a splitting field with $[K:K]=1\leq 1!$.

Inductive step. Assume the result holds for all fields and all polynomials of degree $<n$. Let $f\in K[X]$ have degree n. Let $p(X)\in K[X]$ be an irreducible factor of f with $d=\deg p\geq 1$. Set

$$K_1=K[X]/(p(X)).$$

Then K_1/K is a field extension with $[K_1:K]=d\leq n$, and p has a root $\alpha=\overline{X}$ in K_1. In $K_1[X]$, we can write $f(X)=(X-\alpha)\,g(X)$ for some $g\in K_1[X]$ with $\deg g=n-1$.

By the inductive hypothesis, there exists a splitting field L of g over K_1 with $[L:K_1]\leq(n-1)!$. In $L[X]$, the polynomial g splits completely, and therefore so does $f(X)=(X-\alpha)g(X)$.

Let $\alpha_1=\alpha,\alpha_2,\ldots,\alpha_n$ be the roots of f in L. The subfield $K(\alpha_1,\ldots,\alpha_n)\subseteq L$ is a splitting field of f over K. (In fact L itself equals $K(\alpha_1,\ldots,\alpha_n)$ by minimality of L as a splitting field of g over $K_1=K(\alpha_1)$.)

For the degree bound:

$$[L:K]=[L:K_1]\cdot[K_1:K]\leq(n-1)!\cdot d\leq(n-1)!\cdot n=n!.$$ □

2.3 Extension of isomorphisms

The key technical tool for proving uniqueness of splitting fields is the following lemma about extending field isomorphisms.

Lemma 2.1 (Extension of isomorphisms)**.** Let $\sigma\colon K \xrightarrow{\sim} K'$ be a field isomorphism. Let $f \in K[X]$ be irreducible and let $f' = \sigma(f) \in K'[X]$ (obtained by applying σ to each coefficient). Suppose α is a root of f in some extension L/K and β is a root of f' in some extension L'/K'. Then σ extends to an isomorphism

$$\tilde{\sigma}\colon K(\alpha) \xrightarrow{\sim} K'(\beta)$$

with $\tilde{\sigma}(\alpha) = \beta$ and $\tilde{\sigma}|_K = \sigma$.

Proof. Since f is irreducible over K, it is (up to a unit) the minimal polynomial of α over K. By Theorem 1.3, we have isomorphisms

$$K(\alpha) \cong K[X]/(f), \qquad K'(\beta) \cong K'[X]/(f').$$

More precisely, the evaluation homomorphisms give

$$\psi\colon K[X]/(f) \xrightarrow{\sim} K(\alpha), \quad \overline{X} \mapsto \alpha,$$

$$\psi'\colon K'[X]/(f') \xrightarrow{\sim} K'(\beta), \quad \overline{X} \mapsto \beta.$$

The isomorphism $\sigma\colon K \to K'$ induces an isomorphism $\hat{\sigma}\colon K[X] \to K'[X]$ by applying σ to each coefficient and fixing X. Since $\hat{\sigma}(f) = f'$, $\hat{\sigma}$ maps the ideal (f) onto (f') and therefore induces an isomorphism

$$\bar{\sigma}\colon K[X]/(f) \xrightarrow{\sim} K'[X]/(f').$$

The desired extension is then

$$\tilde{\sigma} = \psi' \circ \bar{\sigma} \circ \psi^{-1}\colon K(\alpha) \xrightarrow{\sim} K'(\beta).$$

By construction, $\tilde{\sigma}(\alpha) = \psi'(\bar{\sigma}(\overline{X})) = \psi'(\overline{X}) = \beta$, and for $a \in K$, $\tilde{\sigma}(a) = \psi'(\bar{\sigma}(\overline{a})) = \psi'(\overline{\sigma(a)}) = \sigma(a)$. □

2.4 Uniqueness of splitting fields

Theorem 2.2 (Uniqueness of splitting fields)**.** Let $\sigma\colon K \xrightarrow{\sim} K'$ be a field isomorphism and let $f \in K[X]$ with $f' = \sigma(f) \in K'[X]$. Let L be a splitting field of f over K and L' a splitting field of f' over K'. Then σ extends to an isomorphism $\tilde{\sigma}\colon L \xrightarrow{\sim} L'$.
In particular (taking $K = K'$, $\sigma = \mathrm{id}_K$), any two splitting fields of f over K are K-isomorphic.

Proof. We proceed by induction on $n = [L : K]$.

Base case ($n = 1$). If $[L : K] = 1$, then $L = K$ and f already splits over K. Then $f' = \sigma(f)$ already splits over K', so $L' = K'$ (by minimality). The map σ itself is the desired isomorphism.

Inductive step. Assume $n > 1$ and that the result holds for all splitting fields of smaller degree over their base.

Since $[L : K] > 1$, the polynomial f has an irreducible factor $p \in K[X]$ with $\deg p \geq 2$. Let $\alpha \in L$ be a root of p and set $p' = \sigma(p) \in K'[X]$. Since f' splits over L' and $p' \mid f'$, the polynomial p' has a root $\beta \in L'$.

By Lemma 2.1, σ extends to an isomorphism

$$\sigma_1 \colon K(\alpha) \xrightarrow{\sim} K'(\beta), \quad \sigma_1(\alpha) = \beta.$$

Now L is a splitting field of f over $K(\alpha)$ (since $L = K(\alpha_1, \ldots, \alpha_n) = K(\alpha)(\alpha_2, \ldots, \alpha_n)$ and f splits over L), and similarly L' is a splitting field of f' over $K'(\beta)$. Moreover,

$$[L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]} = \frac{n}{[K(\alpha) : K]} < n,$$

since $[K(\alpha) : K] = \deg p \geq 2$.

By the inductive hypothesis applied to $\sigma_1 \colon K(\alpha) \to K'(\beta)$, there exists an isomorphism $\tilde{\sigma} \colon L \xrightarrow{\sim} L'$ extending σ_1. Since σ_1 extends σ, so does $\tilde{\sigma}$. □

Corollary 2.1 (Splitting fields are unique up to isomorphism)**.** Any two splitting fields of $f \in K[X]$ over K are K-isomorphic. The isomorphism need not be unique.

2.5 Multiple roots and separability

Definition 2.4 (Multiple root)**.** Let $f \in K[X]$ and let L be a splitting field of f over K. A root $\alpha \in L$ of f is a **multiple root** (or **repeated root**) if $(X - \alpha)^2 \mid f$ in $L[X]$. If $(X - \alpha)^m \mid f$ but $(X - \alpha)^{m+1} \nmid f$, we say α has **multiplicity** m. A root of multiplicity 1 is called **simple**.

Definition 2.5 (Formal derivative)**.** For $f = \sum_{k=0}^{n} a_k X^k \in K[X]$, the **formal derivative** is

$$f' = \sum_{k=1}^{n} k\, a_k X^{k-1} \in K[X].$$

The usual rules hold: $(f + g)' = f' + g'$, $(fg)' = f'g + fg'$, $(cf)' = cf'$ for $c \in K$.

Proposition 2.1 (Multiple roots and the derivative)**.** Let $f \in K[X]$ be nonconstant and let α be a root of f in some extension of K. Then α is a multiple root of f if and only if $f'(\alpha) = 0$.

Proof. Write $f(X) = (X - \alpha)^m g(X)$ in the splitting field, where $g(\alpha) \neq 0$ and $m \geq 1$.

($\Rightarrow$) If $m \geq 2$, then $f'(X) = m(X - \alpha)^{m-1} g(X) + (X - \alpha)^m g'(X)$, so $f'(\alpha) = 0$.

($\Leftarrow$) If $m = 1$, then $f(X) = (X - \alpha)g(X)$ and $f'(X) = g(X) + (X - \alpha)g'(X)$, giving $f'(\alpha) = g(\alpha) \neq 0$. □

Corollary 2.2 (Criterion for no multiple roots)**.** A polynomial $f \in K[X]$ has no multiple roots (in any extension) if and only if $\gcd(f, f') = 1$ in $K[X]$.

Proof. The polynomial f has a multiple root α (in some extension) if and only if f and f' share the root α, which happens if and only if some irreducible factor of f divides both f and f', i.e. $\gcd(f, f') \neq 1$. □

Definition 2.6 (Separable polynomial)**.** A polynomial $f \in K[X]$ is **separable** if it has no multiple roots in any extension of K, equivalently if $\gcd(f, f') = 1$. An irreducible polynomial f is separable if and only if $f' \neq 0$.

Definition 2.7 (Separable extension)**.** An algebraic extension L/K is **separable** if the minimal polynomial $\mathrm{irr}(\alpha, K)$ is separable for every $\alpha \in L$.

Theorem 2.3 (Characteristic zero implies separable)**.** If $\mathrm{char}(K) = 0$, then every irreducible polynomial in $K[X]$ is separable. Hence every algebraic extension of K is separable.

Proof. Let $f \in K[X]$ be irreducible with $\deg f = n \geq 1$. Write $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ with $a_n \neq 0$. The formal derivative is

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

Since $\mathrm{char}(K) = 0$, the integer n is nonzero in K, and $a_n \neq 0$, so $n a_n \neq 0$ in K. Therefore $\deg f' = n - 1$, in particular $f' \neq 0$.

Since f is irreducible and $\deg f' < \deg f$, the polynomial f cannot divide f'. But f is irreducible, so $\gcd(f, f') = 1$ (the gcd must be 1 or an associate of f; it cannot be an associate of f since $f \nmid f'$). By Corollary 2.2, f is separable. □

Proposition 2.2 (Inseparable irreducible polynomials in characteristic p)**.** Let K be a field with $\mathrm{char}(K) = p > 0$ and let $f \in K[X]$ be irreducible. Then f is inseparable if and only if $f' = 0$, which happens if and only if $f(X) = g(X^p)$ for some $g \in K[X]$.

Proof. If f is inseparable, then $\gcd(f, f') \neq 1$. Since f is irreducible and $\deg f' < \deg f$, we cannot have $f \mid f'$ unless $f' = 0$. Since the gcd of f and f' divides f and f is irreducible, $\gcd(f, f')$ is either 1 or an associate of f. If $\gcd(f, f') \neq 1$, then $f \mid f'$, which forces $f' = 0$.

Conversely, if $f' = 0$, then $\gcd(f, f') = f \neq 1$, so f is inseparable.

Now $f' = 0$ means that $k a_k = 0$ for all $k \geq 1$. In characteristic p, this holds if and only if $a_k = 0$ whenever $p \nmid k$, i.e. f involves only powers of X that are multiples of p: $f(X) = \sum_j b_j X^{pj} = g(X^p)$ where $g(Y) = \sum_j b_j Y^j$. □

Definition 2.8 (Perfect field)**.** A field K is **perfect** if every irreducible polynomial in $K[X]$ is separable. Equivalently:

- If $\mathrm{char}(K) = 0$, then K is automatically perfect.
- If $\mathrm{char}(K) = p > 0$, then K is perfect if and only if the Frobenius $\varphi\colon K \to K$, $x \mapsto x^p$, is surjective (i.e. every element of K has a p-th root in K).

Proposition 2.3 (Finite fields are perfect)**.** Every finite field is perfect.

Proof. Let K be a finite field of characteristic p. The Frobenius $\varphi\colon K \to K$ is injective (Theorem 1.6). Since K is finite, an injective map from K to itself is surjective. Hence φ is surjective, and K is perfect. □

2.6 Exercises

Exercise 2.1 (Splitting field of $X^4 - 2$). Find the splitting field of $X^4 - 2$ over $\mathbb{Q}$ and compute its degree over $\mathbb{Q}$.

Exercise 2.2 (Splitting field over a finite field). Find the splitting field of $X^4 + X + 1$ over $\mathbb{F}_2$ and its degree.

Exercise 2.3 (Adjoining one root versus all roots). Give an example of an irreducible polynomial $f \in \mathbb{Q}[X]$ of degree 3 such that adjoining one root of f does not produce the splitting field. Compute $[K(\alpha) : \mathbb{Q}]$ and [splitting field : $\mathbb{Q}$].

Exercise 2.4 (Splitting field of a product). Let $f, g \in K[X]$. Show that the splitting field of fg over K is the compositum of the splitting fields of f and g.

Exercise 2.5 (Counting embeddings). Let $f \in K[X]$ be irreducible of degree n and let L be a splitting field of f. Show that the number of K-embeddings $K[X]/(f) \hookrightarrow L$ equals the number of distinct roots of f in L, which is n if f is separable.

Exercise 2.6 (Separable implies distinct roots). Let $f \in K[X]$ be a separable polynomial of degree n. Prove that f has exactly n distinct roots in any splitting field.

Exercise 2.7 (Inseparable example). Let $K = \mathbb{F}_p(t)$ (the field of rational functions over $\mathbb{F}_p$). Show that $X^p - t \in K[X]$ is irreducible but inseparable.

Exercise 2.8 (Derivative and gcd). Let $f \in K[X]$ be a nonconstant polynomial. Show that $f/\gcd(f, f')$ is a separable polynomial with the same roots as f (but all with multiplicity one).

Exercise 2.9 (Splitting field degree bound). Show that if $f \in K[X]$ is irreducible of degree n, then the degree of the splitting field L of f over K satisfies $n \mid [L : K]$ and $[L : K] \mid n!$.

Exercise 2.10 (Cyclotomic polynomials). (a) Compute $\Phi_n(X)$ for $n = 1, 2, 3, 4, 5, 6, 8, 12$.

(b) Show that $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ for p prime.

(c) Prove that $\Phi_p(X)$ is irreducible over $\mathbb{Q}$ for p prime. *Hint:* Substitute $X \mapsto X + 1$ and apply Eisenstein.

Exercise 2.11 (Separability in characteristic p). Let K be a field of characteristic $p > 0$ and $f \in K[X]$ irreducible. Show that there exists a unique integer $e \geq 0$ and a unique separable irreducible polynomial $g \in K[X]$ such that $f(X) = g(X^{p^e})$.

Exercise 2.12 (Splitting field is always finite). Let $f \in K[X]$ with $\deg f = n \geq 1$. Prove that the splitting field of f over K is always a finite extension of K, with degree at most $n!$.

Chapter summary

- A **splitting field** of $f \in K[X]$ is the smallest extension of K over which f factors into linear factors.
- Splitting fields **exist** (by adjoining roots iteratively) and are **unique up to K-isomorphism** (by the extension-of-isomorphisms lemma).
- The degree of the splitting field of f divides $(\deg f)!$.
- A polynomial is **separable** if and only if $\gcd(f, f') = 1$, equivalently it has no multiple roots.
- In characteristic 0, every irreducible polynomial is separable. In characteristic p, an irreducible f is inseparable iff $f(X) = g(X^p)$.
- **Perfect fields** are those where every irreducible is separable; all fields of characteristic 0 and all finite fields are perfect.

Chapter 3

Algebraic Closure

3.1 Algebraically closed fields

Definition 3.1 (Algebraically closed field)**.** A field K is **algebraically closed** if every nonconstant polynomial in $K[X]$ has a root in K, or equivalently, every nonconstant polynomial in $K[X]$ splits completely into linear factors over K.

Proposition 3.1 (Equivalent characterisations)**.** For a field K, the following are equivalent:

(i) K is algebraically closed.

(ii) Every nonconstant $f \in K[X]$ splits into linear factors.

(iii) The only irreducible polynomials in $K[X]$ are the linear ones.

(iv) K has no proper algebraic extension.

Proof. (i)⇔(ii): If every nonconstant polynomial has a root $\alpha \in K$, we can factor out $(X-\alpha)$ and repeat by induction on degree to split f completely. The converse is immediate.

(ii)⇒(iii): If $f \in K[X]$ is irreducible, then f splits into linear factors, so $\deg f = 1$.

(iii)⇒(iv): Let L/K be algebraic and $\alpha \in L$. Then $\operatorname{irr}(\alpha, K)$ is irreducible, hence linear by (iii), so $\alpha \in K$. Thus $L = K$.

(iv)⇒(i): Let $f \in K[X]$ be nonconstant with irreducible factor p. Then $K[X]/(p)$ is an algebraic extension of K, so $K[X]/(p) = K$ by (iv), giving $\deg p = 1$. Hence f has a root in K. □

Definition 3.2 (Algebraic closure)**.** An **algebraic closure** of a field K is a field $\overline{K} \supseteq K$ such that:

(i) $\overline{K}$ is algebraically closed.

(ii) $\overline{K}/K$ is algebraic.

Remark 3.1 (Minimality). Condition (ii) means that $\overline{K}$ is the "smallest" algebraically closed field containing K. Any algebraically closed field $\Omega \supseteq K$ contains (an isomorphic

copy of) $\overline{K}$ as a subfield.

3.2 Existence and uniqueness

Theorem 3.1 (Existence of algebraic closure)**.** Every field K has an algebraic closure.

Proof sketch. We outline the classical proof using Zorn's lemma. Consider a "sufficiently large" set $\Omega \supseteq K$ and let $\mathcal{F}$ be the collection of all algebraic extensions L/K with $L \subseteq \Omega$, partially ordered by inclusion.

Every chain in $\mathcal{F}$ has an upper bound (the union of the chain is again an algebraic extension of K). By Zorn's lemma, $\mathcal{F}$ has a maximal element $\overline{K}$.

We claim $\overline{K}$ is algebraically closed. If not, there exists a nonconstant irreducible $f \in \overline{K}[X]$ with $\deg f \geq 2$. Then $\overline{K}[X]/(f)$ is a proper algebraic extension of $\overline{K}$, and since $\overline{K}/K$ is algebraic, the extension $\overline{K}[X]/(f)$ is also algebraic over K (by Theorem 1.5). One can embed $\overline{K}[X]/(f)$ into Ω (with care about set-theoretic issues), contradicting the maximality of $\overline{K}$.

The main technical subtlety is the choice of Ω to avoid set-theoretic paradoxes. Artin's original proof handles this by constructing a single polynomial ring in sufficiently many variables and quotienting by an appropriate ideal. We refer the reader to Lang's *Algebra* for the complete argument. □

Theorem 3.2 (Uniqueness of algebraic closure)**.** Any two algebraic closures of K are K-isomorphic. The isomorphism is not unique in general.

Proof sketch. The proof uses the same extension-of-isomorphisms technique as Theorem 2.2, together with Zorn's lemma. One considers the set of all pairs (L, σ) where $K \subseteq L \subseteq \overline{K}$ and $\sigma \colon L \hookrightarrow \overline{K}'$ is a K-embedding. Zorn's lemma gives a maximal such pair, and maximality forces $L = \overline{K}$ and σ to be surjective. □

3.3 The Fundamental Theorem of Algebra

Theorem 3.3 (Fundamental Theorem of Algebra)**.** The field $\mathbb{C}$ of complex numbers is algebraically closed. Equivalently, $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.

Remark 3.2 (Historical note). The theorem was first stated by d'Alembert (1746) and proved with varying degrees of rigour by Euler, Lagrange, Laplace, and others. The first complete proof is generally attributed to Gauss (1799), who gave four proofs during his lifetime. Modern proofs use complex analysis (Liouville's theorem), topology (winding numbers), or algebra combined with the intermediate value theorem. We will return to give an algebraic proof using Galois theory after developing the necessary machinery.

3.4 Finite fields

We now develop the complete theory of finite fields, one of the most beautiful applications of the ideas developed so far.

Theorem 3.4 (Structure of finite fields)**.** (i) Every finite field has order p^n for some prime p and integer $n \geq 1$.

(ii) For each prime p and integer $n \geq 1$, there exists a field of order p^n, unique up to isomorphism. We denote it $\mathbb{F}_{p^n}$.

(iii) $\mathbb{F}_{p^n}$ is a splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$.

Proof. **(i)** Let K be a finite field with $\mathrm{char}(K) = p$. Then the prime subfield of K is $\mathbb{F}_p$, and K is a finite-dimensional $\mathbb{F}_p$-vector space. If $[K : \mathbb{F}_p] = n$, then $|K| = p^n$.

(iii) and existence in (ii). We show that $\mathbb{F}_{p^n}$ can be realised as the splitting field of $f(X) = X^{p^n} - X$ over $\mathbb{F}_p$.

First, $f'(X) = p^n X^{p^n-1} - 1 = -1$ (since $p^n \equiv 0$ in $\mathbb{F}_p$), so $\gcd(f, f') = 1$, and f has p^n distinct roots in any splitting field L of f over $\mathbb{F}_p$.

Let $S = \{\alpha \in L : \alpha^{p^n} = \alpha\}$ be the set of roots of f in L. We claim S is a subfield of L with $|S| = p^n$.

S is a subfield:

- $0^{p^n} = 0$ and $1^{p^n} = 1$, so $0, 1 \in S$.
- If $\alpha, \beta \in S$, then $(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta$ (using the Frobenius), so $\alpha - \beta \in S$.
- If $\alpha, \beta \in S$ with $\beta \neq 0$, then $(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{p^n})^{-1} = \alpha\beta^{-1}$, so $\alpha\beta^{-1} \in S$.

Since f has exactly p^n distinct roots, $|S| = p^n$.

Since S is a subfield of L containing all roots of f and $\mathbb{F}_p \subseteq S$, and L is the splitting field of f over $\mathbb{F}_p$ (hence the smallest field containing $\mathbb{F}_p$ and all roots of f), we conclude $L = S$. Thus $|L| = p^n$.

Uniqueness in (ii). Suppose K is any field with $|K| = p^n$. Then $K^\times$ is a group of order $p^n - 1$, so $\alpha^{p^n-1} = 1$ for all $\alpha \in K^\times$, hence $\alpha^{p^n} = \alpha$ for all $\alpha \in K^\times$. This also holds for $\alpha = 0$. Therefore every element of K is a root of $X^{p^n} - X$, and K is a splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. By the uniqueness of splitting fields (Theorem 2.2), $K \cong \mathbb{F}_{p^n}$. □

3.4.1 The subfield lattice

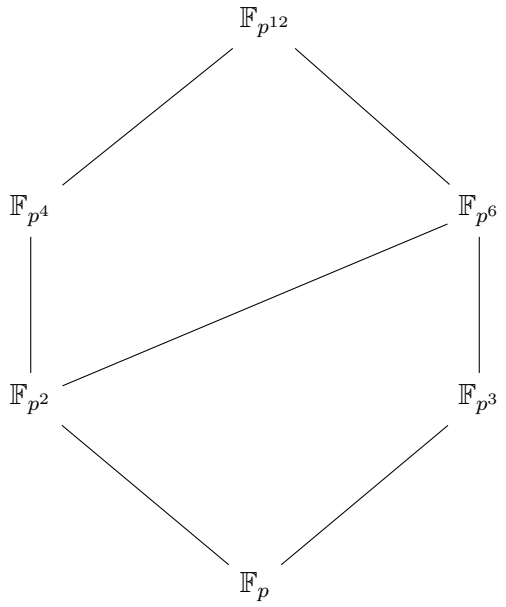
Theorem 3.5 (Subfields of $\mathbb{F}_{p^n}$)**.** The subfields of $\mathbb{F}_{p^n}$ are precisely the fields $\mathbb{F}_{p^d}$ where $d \mid n$. For each such divisor d there is a unique subfield isomorphic to $\mathbb{F}_{p^d}$.

Proof. If $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$, then $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_{p^d}$, so $p^n = (p^d)^{[\mathbb{F}_{p^n}:\mathbb{F}_{p^d}]}$, giving $n = d \cdot [\mathbb{F}_{p^n} : \mathbb{F}_{p^d}]$, hence $d \mid n$.

Conversely, suppose $d \mid n$. Then $p^d - 1 \mid p^n - 1$ (since $X^d - 1 \mid X^n - 1$ in $\mathbb{Z}[X]$ when $d \mid n$), so $X^{p^d} - X \mid X^{p^n} - X$ in $\mathbb{F}_p[X]$. (To verify this divisibility: $\alpha^{p^d} = \alpha$ implies $\alpha^{p^n} = \alpha$, which follows by applying the Frobenius φ^d repeatedly: $\alpha^{p^{2d}} = (\alpha^{p^d})^{p^d} = \alpha^{p^d} = \alpha$, and by induction $\alpha^{p^{kd}} = \alpha$ for all k; taking $k = n/d$ gives $\alpha^{p^n} = \alpha$.)

Hence every root of $X^{p^d} - X$ in $\mathbb{F}_{p^n}$ is also a root of $X^{p^n} - X$. Since $X^{p^d} - X$ has exactly p^d roots (it is separable, as shown in the proof of Theorem 3.4), the set $S_d = \{\alpha \in \mathbb{F}_{p^n} : \alpha^{p^d} = \alpha\}$ has exactly p^d elements and is a subfield (by the same argument as before). This S_d is the unique subfield of $\mathbb{F}_{p^n}$ isomorphic to $\mathbb{F}_{p^d}$. □

Example 3.1 (Subfield lattice of $\mathbb{F}_{p^{12}}$). The divisors of 12 are $1, 2, 3, 4, 6, 12$, and the divisibility relations among them give the following lattice:



Each line segment represents a field extension; the lower field is a subfield of the upper field.

3.4.2 The multiplicative group of a finite field

Theorem 3.6 (Multiplicative group is cyclic)**.** For any finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$.

Proof. Let $q-1 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime factorisation of $q-1$. We will show that $\mathbb{F}_q^\times$ contains an element of order $p_i^{a_i}$ for each i; their product then has order $q-1$, proving cyclicity.

Fix i and write $q-1 = p_i^{a_i} \cdot m$ where $m = (q-1)/p_i^{a_i}$.

Step 1. The polynomial $X^m - 1 \in \mathbb{F}_q[X]$ has degree m and therefore at most m roots in $\mathbb{F}_q$. Since $|\mathbb{F}_q^\times| = q-1 > m$, there exists an element $b \in \mathbb{F}_q^\times$ with $b^m \neq 1$.

Step 2. Set $c = b^{(q-1)/p_i^{a_i}} = b^m$. Wait — let us be more careful. We want an element of order exactly $p_i^{a_i}$. Consider $\alpha = b^{m/1} = b^{(q-1)/p_i^{a_i}}$. No, let us use a cleaner argument.

Set $\beta = b^{(q-1)/p_i^{a_i}}$. Then $\beta^{p_i^{a_i}} = b^{q-1} = 1$, so $\operatorname{ord}(\beta) \mid p_i^{a_i}$, hence $\operatorname{ord}(\beta) = p_i^{e_i}$ for some $0 \le e_i \le a_i$.

Step 3. We claim $e_i \geq 1$. If $e_i = 0$, then $\beta = 1$, so $b^{(q-1)/p_i^{a_i}} = 1$, i.e. $b^m = 1$, contradicting the choice of b. So $e_i \geq 1$.

Step 4. Now set $\gamma_i = \beta^{p_i^{e_i - a_i}}$. Wait — since $e_i \leq a_i$, set $\gamma_i = \beta^{p_i^{e_i}/p_i^{a_i}}$, but this need not be an integer. Let us instead use the following cleaner approach.

Since $\operatorname{ord}(\beta) = p_i^{e_i}$ with $e_i \geq 1$, the element $\gamma_i = \beta^{p_i^{e_i - a_i}}$ if $e_i = a_i$ gives $\gamma_i = \beta$ with order $p_i^{a_i}$, and we are done.

If $e_i < a_i$, we need to modify our choice. Consider the set $S = \{x^m : x \in \mathbb{F}_q^\times\}$. This is a subgroup of $\mathbb{F}_q^\times$. An element $x \in \mathbb{F}_q^\times$ satisfies $x^m = 1$ if and only if x is a root of $X^m - 1$, and there are at most m such elements. By the homomorphism $\mathbb{F}_q^\times \to \mathbb{F}_q^\times$, $x \mapsto x^m$, we have $|S| = |\mathbb{F}_q^\times| / |\operatorname{Ker}| = (q-1)/|\{x : x^m = 1\}|$.

Since $X^m - 1$ divides $X^{q-1} - 1$ in $\mathbb{F}_q[X]$ (because $m \mid q-1$), and $X^{q-1} - 1$ has exactly $q-1$ roots in $\mathbb{F}_q$, the polynomial $X^m - 1$ has exactly m roots in $\mathbb{F}_q$. (In a finite field, $X^d - 1$ has exactly d roots whenever $d \mid q-1$, which follows because $\mathbb{F}_q^\times$ is a group of order $q-1$ and $X^{q-1} - 1 = \prod_{\alpha \in \mathbb{F}_q^\times} (X - \alpha)$, so $X^d - 1 = \gcd(X^d - 1, X^{q-1} - 1)$ has exactly d roots.)

Therefore $|S| = (q-1)/m = p_i^{a_i}$. So S is a subgroup of $\mathbb{F}_q^\times$ of order $p_i^{a_i}$.

Step 5. By the classification of finite abelian groups, every subgroup of $\mathbb{F}_q^\times$ of order $p_i^{a_i}$ is a p_i-group. We claim it is cyclic. Indeed, if it were not cyclic, then every element $s \in S$ would satisfy $s^{p_i^{a_i-1}} = 1$, giving $|S|$ roots of the polynomial $X^{p_i^{a_i-1}} - 1$, namely $p_i^{a_i}$ roots. But this polynomial has degree $p_i^{a_i-1} < p_i^{a_i}$, so it can have at most $p_i^{a_i-1}$ roots in the field $\mathbb{F}_q$ — a contradiction.

Therefore S contains an element γ_i of order $p_i^{a_i}$.

Step 6. Having found $\gamma_i \in \mathbb{F}_q^\times$ of order $p_i^{a_i}$ for each $1 \le i \le r$, set $\gamma = \gamma_1 \gamma_2 \cdots \gamma_r$.

Since $\gcd(p_i^{a_i}, p_j^{a_j}) = 1$ for $i \neq j$, and the γ_i are elements of the abelian group $\mathbb{F}_q^\times$, we have

$$\operatorname{ord}(\gamma) = \operatorname{lcm}(\operatorname{ord}(\gamma_1), \ldots, \operatorname{ord}(\gamma_r)).$$

Actually, we need to be slightly more careful. Since each γ_i has order $p_i^{a_i}$ and $\gamma_i \in S_i = \{x^{m_i} : x \in \mathbb{F}_q^\times\}$ where $m_i = (q-1)/p_i^{a_i}$, the subgroups S_i and S_j (for $i \neq j$) satisfy $S_i \cap S_j = \{1\}$ (since $|S_i \cap S_j|$ divides $\gcd(|S_i|, |S_j|) = 1$). It follows that the product $\gamma = \gamma_1 \cdots \gamma_r$ has order

$$\operatorname{ord}(\gamma) = \prod_{i=1}^{r} p_i^{a_i} = q - 1.$$

Therefore $\mathbb{F}_q^\times = \langle \gamma \rangle$ is cyclic. □

Remark 3.3 (Generators). A generator of $\mathbb{F}_q^\times$ is called a **primitive element** of $\mathbb{F}_q$. By the theory of cyclic groups, there are exactly $\varphi(q-1)$ primitive elements.

Corollary 3.1 (Finite subgroups of multiplicative groups)**.** Let K be any field and let G be a finite subgroup of $K^\times$. Then G is cyclic.

Proof. The proof of Step 5 above applies verbatim: if $|G| = n$ and G were not cyclic, then every element of G would satisfy $x^{n/p} = 1$ for some prime $p \mid n$, but $X^{n/p} - 1$ has at most $n/p < n$ roots in the field K.

More precisely, let $|G| = n$ and suppose G is not cyclic. Then the exponent of G (the least common multiple of the orders of all elements) is $e < n$. Every $g \in G$ satisfies $g^e = 1$, so G consists of roots of $X^e - 1$. But this polynomial has at most e roots in the field K, giving $n = |G| \le e < n$, a contradiction. □

3.5 Exercises

Exercise 3.1 (Algebraically closed ⇒ infinite). Prove that every algebraically closed field is infinite. *Hint:* Adapt Euclid's proof that there are infinitely many primes.

Exercise 3.2 (Algebraic closure of $\mathbb{F}_p$). Show that $\overline{\mathbb{F}_p} = \bigcup_{n \ge 1} \mathbb{F}_{p^n}$ (where the union is taken inside a fixed algebraic closure). Verify that this union is indeed a field and that it is algebraically closed.

Exercise 3.3 (Subfields of $\mathbb{F}_{p^{30}}$). List all subfields of $\mathbb{F}_{p^{30}}$ and draw the inclusion lattice.

Exercise 3.4 (Number of irreducible polynomials). Let $N_q(n)$ denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$. Show that

$$q^n = \sum_{d \mid n} d\, N_q(d),$$

and deduce by Möbius inversion that

$$N_q(n) = \frac{1}{n} \sum_{d \mid n} \mu(n/d)\, q^d,$$

where μ is the Möbius function.

Exercise 3.5 (Explicit irreducible over $\mathbb{F}_2$). Find all irreducible polynomials of degree 4 over $\mathbb{F}_2$. How many are there? Verify your answer using the formula from Exercise 3.4.

Exercise 3.6 (Frobenius generates the Galois group). Show that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n, generated by the Frobenius automorphism $\varphi\colon x \mapsto x^p$.

Exercise 3.7 (Finite field extensions). Show that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$. When $m \mid n$, show $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = n/m$.

Exercise 3.8 (Primitive elements). (a) Find a primitive element (generator of $\mathbb{F}_q^\times$) for $\mathbb{F}_7$, $\mathbb{F}_{11}$, and $\mathbb{F}_{13}$.

(b) Find a primitive element for $\mathbb{F}_4$ and $\mathbb{F}_8$.

(c) Show that 2 is a primitive element of $\mathbb{F}_{11}$ but not of $\mathbb{F}_{13}$.

Exercise 3.9 (Wedderburn's little theorem (guided)). Let D be a finite division ring (not assumed commutative).

(a) Show that the centre $Z(D)$ is a field, say $Z(D) \cong \mathbb{F}_q$ with $q = p^m$.

(b) Show $|D| = q^n$ for some $n \geq 1$.

(c) For each $x \in D$, the centraliser $C_D(x)$ is a division subring containing $Z(D)$, so $|C_D(x)| = q^{d(x)}$ with $d(x) \mid n$.

(d) Write the class equation for $D^\times$ and use cyclotomic polynomial arguments to derive a contradiction if $n > 1$.

This proves Wedderburn's theorem: every finite division ring is a field.

Exercise 3.10 (Artin–Schreier polynomials). Let K be a field of characteristic $p > 0$ and $a \in K$ such that $X^p - X - a$ has no root in K. Show that $X^p - X - a$ is irreducible over K. *Hint:* If α is a root, show that all roots are $\alpha, \alpha + 1, \ldots, \alpha + (p-1)$.

Chapter summary

- A field is **algebraically closed** if every nonconstant polynomial has a root; equivalently, the only irreducible polynomials are linear.
- Every field K has an **algebraic closure** $\overline{K}$, unique up to K-isomorphism (existence uses Zorn's lemma).

- The **Fundamental Theorem of Algebra** asserts that $\mathbb{C}$ is algebraically closed.
- For each prime power $q = p^n$, there is a unique (up to isomorphism) finite field $\mathbb{F}_q$, which is the splitting field of $X^q - X$ over $\mathbb{F}_p$.
- The subfields of $\mathbb{F}_{p^n}$ are exactly $\mathbb{F}_{p^d}$ for $d \mid n$.
- The multiplicative group $\mathbb{F}_q^\times$ is **cyclic** of order $q - 1$.

Chapter 4

Galois Extensions

In the preceding chapters we studied the notions of normality and separability for algebraic field extensions. We now bring them together in the central concept of *Galois extension* and begin the study of the group of automorphisms that will lead, in Chapter 5, to the Fundamental Theorem of Galois Theory.

4.1 The Automorphism Group and Fixed Fields

Definition 4.1 (Automorphism group of an extension)**.** Let L/K be a field extension. The *automorphism group of* L/K is

$$\mathrm{Aut}(L/K) \;=\; \big\{\, \sigma \in \mathrm{Aut}(L) \;\big|\; \sigma(a) = a \text{ for all } a \in K \big\}.$$

When L/K is a Galois extension (Definition 4.3), we write $\mathrm{Gal}(L/K)$ instead of $\mathrm{Aut}(L/K)$ and call it the *Galois group* of the extension.

Definition 4.2 (Fixed field)**.** Let L be a field and $H \leq \mathrm{Aut}(L)$ a subgroup. The *fixed field* of H is

$$\mathrm{Fix}(H) \;=\; L^H \;=\; \big\{\, a \in L \;\big|\; \sigma(a) = a \text{ for all } \sigma \in H \big\}.$$

Remark 4.1 (Elementary properties).

1. L^H is indeed a subfield of L.
2. If $H_1 \leq H_2 \leq \mathrm{Aut}(L)$, then $L^{H_2} \subseteq L^{H_1}$.
3. For any subgroup $H \leq \mathrm{Aut}(L)$, one has $H \leq \mathrm{Aut}\big(L/L^H\big)$.

4.2 Galois Extensions: Definition and Characterisations

Definition 4.3 (Galois extension)**.** A finite extension L/K is called a *Galois extension* if it is both *normal* and *separable*.

Theorem 4.1 (Equivalent characterisations of Galois extensions)**.** Let L/K be a finite extension of degree $n = [L : K]$. The following are equivalent:

1. L/K is normal and separable.
2. L is the splitting field of some separable polynomial $f \in K[X]$.
3. $|\mathrm{Aut}(L/K)| = n$.
4. $L^{\mathrm{Aut}(L/K)} = K$ (the fixed field of $\mathrm{Aut}(L/K)$ is K).

We prove the equivalences in several steps across this section.

4.2.1 Normal Extensions and Splitting Fields

Theorem 4.2 (Normal $\Longleftrightarrow$ splitting field)**.** Let L/K be a finite extension. Then L/K is normal if and only if L is the splitting field over K of some polynomial $f \in K[X]$.

Proof. ($\Longrightarrow$) Suppose L/K is normal and write $L = K(\alpha_1, \ldots, \alpha_r)$ for finitely many algebraic elements α_i. Let $f_i = \mathrm{irr}(\alpha_i, K) \in K[X]$ be the minimal polynomial of α_i over K. By normality, every irreducible polynomial in $K[X]$ having a root in L splits completely in L; in particular each f_i splits in $L[X]$. Set $f = f_1 f_2 \cdots f_r$. Then $f \in K[X]$, all roots of f lie in L, and L is generated over K by these roots. Hence L is a splitting field of f over K.

($\Longleftarrow$) Suppose L is the splitting field of $f \in K[X]$. We must show that every irreducible $g \in K[X]$ having a root $\beta \in L$ splits completely in L. Let $\beta' \in \overline{K}$ be any root of g. Since g is irreducible over K, the map $\beta \mapsto \beta'$ extends to a K-isomorphism $\varphi\colon K(\beta) \xrightarrow{\sim} K(\beta')$. Because L is a splitting field of f over K, and $K(\beta) \subseteq L$, we may extend φ to an embedding $\tilde{\varphi}\colon L \hookrightarrow \overline{K}$. But L, being a splitting field, is mapped to itself by any such embedding (the roots of f are permuted), so $\tilde{\varphi}(L) = L$. In particular $\beta' = \tilde{\varphi}(\beta) \in L$. Since β' was an arbitrary root of g, the polynomial g splits in L. □

4.2.2 Order of the Galois Group

Theorem 4.3 ($|\mathrm{Gal}(L/K)| = [L : K]$ for Galois extensions)**.** If L/K is a finite Galois extension, then $|\mathrm{Gal}(L/K)| = [L : K]$.

Proof. Set $n = [L : K]$. We prove both inequalities.

Step 1: $|\mathrm{Aut}(L/K)| \leq n$.

Write $L = K(\alpha_1, \ldots, \alpha_r)$. Every $\sigma \in \mathrm{Aut}(L/K)$ is determined by the images $\sigma(\alpha_1), \ldots, \sigma(\alpha_r)$. For each i, the element $\sigma(\alpha_i)$ must be a root of $\mathrm{irr}(\alpha_i, K)$, so there are at most $\deg \mathrm{irr}(\alpha_i, K)$ choices. A standard induction on r using the tower

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq L$$

shows that the number of K-embeddings of L into $\overline{K}$ is at most

$$[K(\alpha_1) : K] \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \cdots = [L : K] = n.$$

Since every element of $\mathrm{Aut}(L/K)$ restricts to such a K-embedding, we get $|\mathrm{Aut}(L/K)| \leq n$.

Step 2: $|\mathrm{Aut}(L/K)| \geq n$.

Since L/K is separable, we may write $L = K(\alpha)$ by the Primitive Element Theorem (Theorem 5.2; we prove it independently in Chapter 5). Let $f = \mathrm{irr}(\alpha, K)$. Then $\deg f = [K(\alpha) : K] = n$. Because L/K is normal, f splits in L; because L/K is separable, f has n distinct roots $\alpha_1, \ldots, \alpha_n \in L$. For each i the assignment $\alpha \mapsto \alpha_i$ extends to a unique K-automorphism $\sigma_i \in \mathrm{Aut}(L/K)$. These σ_i are pairwise distinct, so $|\mathrm{Aut}(L/K)| \geq n$.

Combining Steps 1 and 2 yields $|\mathrm{Aut}(L/K)| = n = [L : K]$. □

4.2.3 Artin's Lemma

Lemma 4.1 (Artin's lemma)**.** Let L be a field and G a finite subgroup of $\mathrm{Aut}(L)$ with $|G| = n$. Then $[L : L^G] = n$. In particular L/L^G is a Galois extension with $\mathrm{Gal}(L/L^G) = G$.

Proof. Set $K = L^G$. We prove $[L : K] = n$.

Step 1: $[L : K] \leq n$.

Suppose for contradiction that $[L : K] > n$. Choose $n + 1$ elements $\alpha_1, \ldots, \alpha_{n+1} \in L$ that are K-linearly independent. Write $G = \{\sigma_1, \ldots, \sigma_n\}$. Consider the homogeneous system of n linear equations in $n + 1$ unknowns $x_1, \ldots, x_{n+1}$:

$$\sum_{j=1}^{n+1} \sigma_i(\alpha_j)\, x_j = 0, \qquad i = 1, \ldots, n.$$

Since there are more unknowns than equations, there exists a non-trivial solution $(c_1, \ldots, c_{n+1}) \in L^{n+1} \setminus \{0\}$. Choose such a solution with the fewest non-zero entries. After reordering, assume $c_1, \ldots, c_m \neq 0$ and $c_{m+1} = \cdots = c_{n+1} = 0$, with m minimal. Dividing by c_m, we may assume $c_m = 1$.

If all $c_j \in K$, then taking $\sigma_i = \mathrm{id}$ gives $\sum_j c_j \alpha_j = 0$, contradicting the K-linear independence of the α_j. So some $c_j \notin K$; say $c_1 \notin K$. Then there exists $\tau \in G$ with $\tau(c_1) \neq c_1$. Applying τ to the system:

$$\sum_{j=1}^{m} \tau(\sigma_i(\alpha_j))\, \tau(c_j) = 0 \quad \text{for all } i.$$

Since τ permutes G, $\{\tau\sigma_1, \ldots, \tau\sigma_n\} = G$, so this is the same system with c_j replaced by $\tau(c_j)$. Subtracting from the original:

$$\sum_{j=1}^{m} \sigma_i(\alpha_j)\big(c_j - \tau(c_j)\big) = 0 \quad \text{for all } i.$$

Since $c_m = \tau(c_m) = 1$, the m-th coefficient vanishes, and $c_1 - \tau(c_1) \neq 0$. This gives a non-trivial solution with fewer than m non-zero entries, contradicting the minimality of m.

Step 2: $[L : K] \geq n$.

We always have $G \leq \mathrm{Aut}(L/K)$. By Step 1, $[L : K] \leq n$, and Theorem 4.3 (Step 1 of its proof, which applies to any finite extension) gives $|\mathrm{Aut}(L/K)| \leq [L : K]$. Hence $n = |G| \leq |\mathrm{Aut}(L/K)| \leq [L : K] \leq n$, so all inequalities are equalities.

Therefore $[L : K] = n$, $\mathrm{Aut}(L/K) = G$, and L/K is Galois. □

Proof of Theorem 4.1. 1 ⇒ 2: By Theorem 4.2, normality implies L is a splitting field of some $f \in K[X]$. Since L/K is separable, the roots of the minimal polynomials generating L are separable, and we can choose f to be separable (take f to be the product of the distinct irreducible factors of the minimal polynomials).

2 ⇒ 1: A splitting field of a separable polynomial is normal (Theorem 4.2). Since the roots of f are separable over K, every element of $L = K(\alpha_1, \ldots, \alpha_r)$ is separable over K.

1 ⇒ 3: This is Theorem 4.3.

3 ⇒ 4: Set $G = \mathrm{Aut}(L/K)$ and $E = L^G$. Then $K \subseteq E$ and $G \leq \mathrm{Aut}(L/E)$. Artin's lemma gives $[L : E] = |G| = n = [L : K]$, so $E = K$.

4 ⇒ 1: Set $G = \mathrm{Aut}(L/K)$ and suppose $L^G = K$. By Artin's lemma, $[L : K] = |G|$ and L/K is Galois, hence normal and separable. □

4.3 Detailed Examples of Galois Groups

4.3.1 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}\,)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$

Example 4.1 ($\mathrm{Gal}(\mathbb{Q}(\sqrt{2}\,)/\mathbb{Q})$). The polynomial $f = X^2 - 2$ is irreducible over $\mathbb{Q}$ (Eisenstein at $p = 2$) and separable. Its splitting field is $\mathbb{Q}(\sqrt{2}\,)$, which is therefore Galois over $\mathbb{Q}$ of degree 2.

Any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}\,)/\mathbb{Q})$ satisfies $\sigma(\sqrt{2}\,)^2 = \sigma(2) = 2$, so $\sigma(\sqrt{2}\,) = \pm\sqrt{2}$. This gives exactly two automorphisms: the identity and $\sigma\colon \sqrt{2} \mapsto -\sqrt{2}$. Hence

$$\mathrm{Gal}\big(\mathbb{Q}(\sqrt{2}\,)/\mathbb{Q}\big) \;=\; \{\mathrm{id},\, \sigma\} \;\cong\; \mathbb{Z}/2\mathbb{Z}.$$

4.3.2 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$

Example 4.2 (Full computation of $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$). Let $\omega = e^{2\pi i/3} = (-1 + \sqrt{-3}\,)/2$ be a primitive cube root of unity and consider $f = X^3 - 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein at $p = 2$. Its three roots are

$$\alpha_1 = \sqrt[3]{2}, \qquad \alpha_2 = \omega\sqrt[3]{2}, \qquad \alpha_3 = \omega^2\sqrt[3]{2}.$$

The splitting field is $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

Degree computation. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $\omega \notin \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, so $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})] = 2$ (the minimal polynomial of ω over $\mathbb{Q}(\sqrt[3]{2})$ is $X^2 + X + 1$). Thus $[L : \mathbb{Q}] = 6$.

The six automorphisms. By Theorem 4.3, $|\,\mathrm{Gal}(L/\mathbb{Q})| = 6$. Each $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is determined by

$$\sigma(\sqrt[3]{2}) \in \{\alpha_1, \alpha_2, \alpha_3\} \quad \text{and} \quad \sigma(\omega) \in \{\omega, \omega^2\}.$$

Label the automorphisms by their action on the roots:

	$\sigma(\sqrt[3]{2})$	$\sigma(\omega)$
id	α_1	ω
τ	α_1	ω^2
ρ	α_2	ω
ρ^2	α_3	ω
$\rho\tau$	α_2	ω^2
$\rho^2\tau$	α_3	ω^2

Here ρ acts on $\{\alpha_1, \alpha_2, \alpha_3\}$ as the 3-cycle (1 2 3) and τ as the transposition induced by complex conjugation (swapping $\omega \leftrightarrow \omega^2$, which acts as (2 3) on the roots). These generate S_3, confirming

$$\mathrm{Gal}\big(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}\big) \;\cong\; S_3.$$

4.3.3 $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ The Frobenius Automorphism

Theorem 4.4 (Galois group of a finite field extension)**.** For every prime p and integer $n \geq 1$, the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \;=\; \langle \varphi \rangle \;\cong\; \mathbb{Z}/n\mathbb{Z},$$

where $\varphi\colon x \mapsto x^p$ is the *Frobenius automorphism.*

Proof. **Step 1: φ is a well-defined automorphism.** For $x, y \in \mathbb{F}_{p^n}$ we have

$$\varphi(x+y) = (x+y)^p = x^p + y^p = \varphi(x) + \varphi(y)$$

(the binomial coefficients $\binom{p}{k}$ with $0 < k < p$ are divisible by p, hence vanish in characteristic p), and $\varphi(xy) = (xy)^p = x^p y^p = \varphi(x)\varphi(y)$. Since φ is a non-zero ring homomorphism from a field to itself, it is injective. As $\mathbb{F}_{p^n}$ is finite, φ is also surjective, hence an automorphism. For $a \in \mathbb{F}_p$, Fermat's little theorem gives $\varphi(a) = a^p = a$, so $\varphi \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Step 2: φ has order exactly n. We have $\varphi^k(x) = x^{p^k}$. Thus $\varphi^k = \mathrm{id}$ if and only if $x^{p^k} = x$ for all $x \in \mathbb{F}_{p^n}$. The elements of $\mathbb{F}_{p^n}$ are precisely the roots of $X^{p^n} - X$, so $\varphi^n = \mathrm{id}$. If $\varphi^k = \mathrm{id}$ for some $k < n$, then every element of $\mathbb{F}_{p^n}$ would be a root of $X^{p^k} - X$, which has at most $p^k < p^n$ roots a contradiction.

Step 3: Conclusion. We have $\langle \varphi \rangle \leq \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ with $|\langle \varphi \rangle| = n$. Since $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leq n$, equality holds: $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \varphi \rangle \cong \mathbb{Z}/n\mathbb{Z}$. □

4.3.4 Cyclotomic Extensions

Theorem 4.5 (Galois group of cyclotomic extensions)**.** Let $n \geq 1$ and $\zeta_n = e^{2\pi i/n}$. Then $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois with

$$\mathrm{Gal}\big(\mathbb{Q}(\zeta_n)/\mathbb{Q}\big) \;\cong\; (\mathbb{Z}/n\mathbb{Z})^\times.$$

In particular $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where φ is Euler's totient function.

Proof sketch. The minimal polynomial of ζ_n over $\mathbb{Q}$ is the n-th cyclotomic polynomial $\Phi_n \in \mathbb{Z}[X]$, which is irreducible over $\mathbb{Q}$ (a classical result proved, e.g., by reduction modulo p). Hence $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n = \varphi(n)$. Since $\mathbb{Q}(\zeta_n)$ is the splitting field of $X^n - 1$ (a separable polynomial), the extension is Galois. Every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ satisfies $\sigma(\zeta_n)^n = 1$, so $\sigma(\zeta_n) = \zeta_n^a$ for a unique $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. The map $\sigma \mapsto a$ is readily checked to be a group isomorphism. □

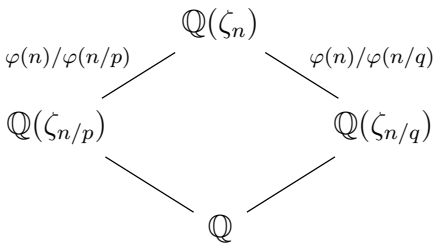


Figure 4.1: Subfield lattice of $\mathbb{Q}(\zeta_n)$ for $n = pq$ (distinct primes).

4.4 Exercises

Exercise 4.1 (Automorphisms of $\mathbb{Q}(\sqrt{5}\,)$). Determine $\mathrm{Gal}(\mathbb{Q}(\sqrt{5}\,)/\mathbb{Q})$ and all intermediate fields.

Exercise 4.2 (Fourth roots of unity). Show that $\mathbb{Q}(i)/\mathbb{Q}$ is Galois, determine $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, and verify the degree–order equality.

Exercise 4.3 (Splitting field of $X^4 - 2$). Let L be the splitting field of $X^4 - 2$ over $\mathbb{Q}$.

1. Show $[L : \mathbb{Q}] = 8$.
2. Prove that $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$ (the dihedral group of order 8).

Exercise 4.4 (Fixed field computation). Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}\,)$ and $\sigma\colon \sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$. Compute $L^{\langle\sigma\rangle}$.

Exercise 4.5 (Artin's lemma in practice). Let $\sigma\colon \mathbb{C} \to \mathbb{C}$ be complex conjugation and $G = \{1, \sigma\}$. Use Artin's lemma to prove that $[\mathbb{C} : \mathbb{R}] = 2$ without using any prior knowledge of $\mathbb{C}/\mathbb{R}$.

Exercise 4.6 (Frobenius powers). Let φ denote the Frobenius automorphism of $\mathbb{F}_{p^6}/\mathbb{F}_p$. List all subgroups of $\langle\varphi\rangle$ and the corresponding fixed fields.

Exercise 4.7 (Cyclotomic polynomials). Compute $\Phi_{12}(X)$ and verify that $\deg \Phi_{12} = \varphi(12) = 4$.

Exercise 4.8 (Normal closure). Show that the normal closure of $\mathbb{Q}(\sqrt[3]{2}\,)/\mathbb{Q}$ in $\mathbb{C}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$, and compute its Galois group.

Exercise 4.9 (Non-Galois extension). Prove that $\mathbb{Q}(\sqrt[3]{2}\,)/\mathbb{Q}$ is not a Galois extension by showing $|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}\,)/\mathbb{Q})| = 1 < 3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

Exercise 4.10 (Galois group over $\mathbb{F}_p$). Let $f \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree n. Show that the splitting field of f is $\mathbb{F}_{p^n}$ and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$.

Exercise 4.11 (Separability and Galois). Give an example of a normal extension that is not Galois. *Hint:* work in characteristic p.

Chapter Summary

- A finite extension L/K is **Galois** if and only if it is normal and separable; equivalently, L is the splitting field of a separable polynomial, or $|\mathrm{Aut}(L/K)| = [L : K]$, or $L^{\mathrm{Aut}(L/K)} = K$.
- **Artin's lemma**: for a finite $G \leq \mathrm{Aut}(L)$, $[L : L^G] = |G|$.
- **Frobenius**: $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle x \mapsto x^p \rangle \cong \mathbb{Z}/n\mathbb{Z}$.
- **Cyclotomic**: $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Chapter 5

Galois Theory The Fundamental Theorem

The Fundamental Theorem of Galois Theory establishes a precise dictionary between the internal structure of a Galois group and the lattice of intermediate fields. It is one of the crowning achievements of algebra and has profound consequences across mathematics.

5.1 Statement and Proof of the Fundamental Theorem

Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Denote by

$$\mathcal{F} \;=\; \{E \mid K \subseteq E \subseteq L\}$$

the set of intermediate fields, and by

$$\mathcal{G} \;=\; \{H \mid H \leq G\}$$

the set of subgroups of G.

Theorem 5.1 (Fundamental Theorem of Galois Theory)**.** Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$.

1. **(Galois correspondence).** The maps

$$\begin{aligned} \Phi\colon \mathcal{F} &\longrightarrow \mathcal{G}, & E &\longmapsto \mathrm{Gal}(L/E), \\ \Psi\colon \mathcal{G} &\longrightarrow \mathcal{F}, & H &\longmapsto L^H = \mathrm{Fix}(H), \end{aligned}$$

   are inclusion-reversing bijections, inverse to each other: $\Psi \circ \Phi = \mathrm{id}_{\mathcal{F}}$ and $\Phi \circ \Psi = \mathrm{id}_{\mathcal{G}}$.

2. **(Degree–index formula).** For every intermediate field E and the corresponding subgroup $H = \mathrm{Gal}(L/E)$:

$$[L : E] \;=\; |H|, \qquad [E : K] \;=\; [G : H] \;=\; |G|/|H|.$$

3. **(Normality criterion).** An intermediate field E is normal over K (equivalently, E/K is Galois) if and only if the corresponding subgroup $H = \mathrm{Gal}(L/E)$

is a normal subgroup of G. In that case,

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

Proof. We prove each part in turn.

Part 1: The bijection.

$\Psi \circ \Phi = \mathrm{id}$: Let $E \in \mathcal{F}$. We must show $L^{\mathrm{Gal}(L/E)} = E$. Since L/K is Galois (normal and separable), and E is an intermediate field, L/E is also separable. Moreover L is a splitting field of some separable polynomial over K, hence also over E, so L/E is normal. Therefore L/E is Galois, and the characterisation (Theorem 4.1, 4) gives $L^{\mathrm{Gal}(L/E)} = E$.

$\Phi \circ \Psi = \mathrm{id}$: Let $H \in \mathcal{G}$. We must show $\mathrm{Gal}(L/L^H) = H$. By Artin's lemma (Lemma 4.1), L/L^H is Galois with $\mathrm{Gal}(L/L^H) = H$.

Since both compositions are the identity, Φ and Ψ are mutually inverse bijections. The inclusion-reversing property is immediate: $E_1 \subseteq E_2$ implies $\mathrm{Gal}(L/E_2) \leq \mathrm{Gal}(L/E_1)$, and $H_1 \leq H_2$ implies $L^{H_2} \subseteq L^{H_1}$.

Part 2: Degree and index.

Let $H = \mathrm{Gal}(L/E)$. Since L/E is Galois (as shown above), Theorem 4.3 gives $[L : E] = |H|$. By the tower law,

$$[E : K] \;=\; \frac{[L : K]}{[L : E]} \;=\; \frac{|G|}{|H|} \;=\; [G : H].$$

Part 3: Normal subgroups and normal extensions.

($\Longrightarrow$) Suppose E/K is normal (hence Galois, since L/K separable implies E/K separable). We show $H = \mathrm{Gal}(L/E) \trianglelefteq G$. Let $\sigma \in G$ and $\tau \in H$; we need $\sigma\tau\sigma^{-1} \in H$, i.e., $\sigma\tau\sigma^{-1}$ fixes E pointwise. For $a \in E$, since E/K is normal and $\sigma|_E$ is a K-embedding of E into L, we have $\sigma(E) = E$ (a normal extension is stable under any K-embedding). So $\sigma^{-1}(a) \in E$, hence $\tau(\sigma^{-1}(a)) = \sigma^{-1}(a)$ (because $\tau \in \mathrm{Gal}(L/E)$), and therefore $\sigma\tau\sigma^{-1}(a) = \sigma(\sigma^{-1}(a)) = a$. Thus $\sigma\tau\sigma^{-1} \in H$.

Moreover, the restriction map $G \to \mathrm{Gal}(E/K)$, $\sigma \mapsto \sigma|_E$, is a well-defined surjective homomorphism (surjectivity uses the fact that any K-automorphism of E extends to L since L/E is Galois). Its kernel is H, so by the first isomorphism theorem, $\mathrm{Gal}(E/K) \cong G/H$.

($\Longleftarrow$) Suppose $H \trianglelefteq G$. We show $E = L^H$ is normal over K. Let $\alpha \in E$ and $f = \mathrm{irr}(\alpha, K)$. If β is any root of f in L, there exists $\sigma \in G$ with $\sigma(\alpha) = \beta$ (since L/K is normal and f is irreducible). For any $\tau \in H$ we have $\sigma^{-1}\tau\sigma \in H$ (since H is normal), so

$$\tau(\beta) = \tau(\sigma(\alpha)) = \sigma\big(\sigma^{-1}\tau\sigma(\alpha)\big) = \sigma(\alpha) = \beta,$$

since $\sigma^{-1}\tau\sigma \in H$ fixes $\alpha \in E = L^H$. Thus $\beta \in L^H = E$, and f splits in E. Therefore E/K is normal. □

$$\mathcal{F} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \mathcal{G} \qquad \begin{array}{l} E \longmapsto \mathrm{Gal}(L/E) \\ L^H \longleftarrow\!| \; H \end{array}$$

Figure 5.1: The Galois correspondence: intermediate fields $\leftrightarrow$ subgroups, inclusion-reversing.

5.2 Worked Examples with Complete Lattice Computations

5.2.1 $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$: The Klein Four-Group

Example 5.1 ($\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ and V_4). Let $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$. Since L is the splitting field of $(X^2-2)(X^2-3)\in\mathbb{Q}[X]$ (separable), $L/\mathbb{Q}$ is Galois of degree 4. Define:

$$\sigma\colon \sqrt{2}\mapsto -\sqrt{2},\ \sqrt{3}\mapsto \sqrt{3},$$
$$\tau\colon \sqrt{2}\mapsto \sqrt{2},\ \sqrt{3}\mapsto -\sqrt{3}.$$

Then $G=\mathrm{Gal}(L/\mathbb{Q})=\{1,\sigma,\tau,\sigma\tau\}\cong V_4=(\mathbb{Z}/2\mathbb{Z})^2$.

The subgroups and corresponding fixed fields are:

Subgroup H	Fixed field L^H	$[L^H:\mathbb{Q}]$
$\{1\}$	$L=\mathbb{Q}(\sqrt{2},\sqrt{3})$	4
$\langle\sigma\rangle$	$\mathbb{Q}(\sqrt{3})$	2
$\langle\tau\rangle$	$\mathbb{Q}(\sqrt{2})$	2
$\langle\sigma\tau\rangle$	$\mathbb{Q}(\sqrt{6})$	2
G	$\mathbb{Q}$	1

All subgroups of V_4 are normal (since V_4 is abelian), and correspondingly every intermediate field is Galois over $\mathbb{Q}$.

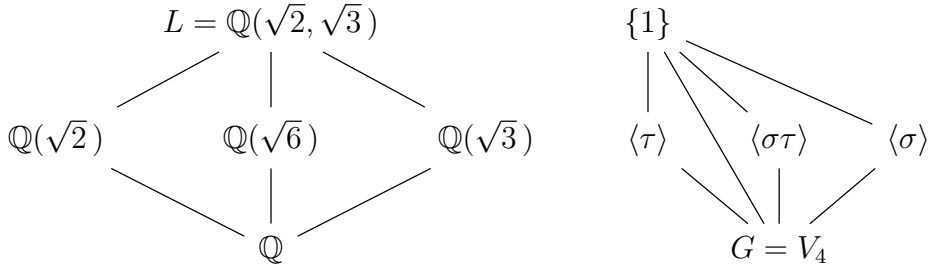


Figure 5.2: Lattice of intermediate fields (left) and subgroups (right) for $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$. The correspondence reverses inclusions.

5.2.2 $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$: The Symmetric Group S_3

Example 5.2 ($\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ and S_3). From Example 4.2, $G=\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q})\cong S_3$, with $|G|=6$ and $[L:\mathbb{Q}]=6$. Recall $\rho=(1\ 2\ 3)$ and $\tau=(2\ 3)$ (in terms of the roots $\alpha_1,\alpha_2,\alpha_3$ of X^3-2).

The subgroups of S_3 and corresponding fixed fields:

Subgroup H	$\lvert H\rvert$	L^H	$[L^H:\mathbb{Q}]$
$\{1\}$	1	L	6
$\langle\tau\rangle=\{1,(2\ 3)\}$	2	$\mathbb{Q}(\sqrt[3]{2}\,)$	3
$\langle\rho\tau\rangle=\{1,(1\ 3)\}$	2	$\mathbb{Q}(\omega\sqrt[3]{2}\,)$	3
$\langle\rho^2\tau\rangle=\{1,(1\ 2)\}$	2	$\mathbb{Q}(\omega^2\sqrt[3]{2}\,)$	3
$\langle\rho\rangle=\{1,(1\ 2\ 3),(1\ 3\ 2)\}$	3	$\mathbb{Q}(\omega)$	2
$G=S_3$	6	$\mathbb{Q}$	1

The only normal subgroups of S_3 are $\{1\}$, $\langle\rho\rangle\cong\mathbb{Z}/3\mathbb{Z}$, and S_3 itself. Correspondingly, the only intermediate fields that are Galois over $\mathbb{Q}$ are L, $\mathbb{Q}(\omega)$, and $\mathbb{Q}$. Indeed:

- $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois (splitting field of X^2+X+1) with $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})\cong S_3/\langle\rho\rangle\cong\mathbb{Z}/2\mathbb{Z}$.
- $\mathbb{Q}(\sqrt[3]{2}\,)/\mathbb{Q}$ is *not* normal (hence not Galois), consistent with $\langle\tau\rangle$ not being normal in S_3.

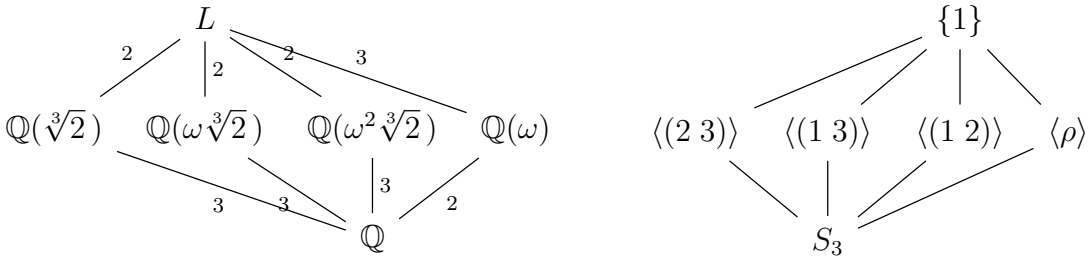


Figure 5.3: Lattice of intermediate fields (left) and subgroups (right) for $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$. Edge labels indicate degrees/indices.

5.2.3 $\mathbb{F}_{p^{12}}/\mathbb{F}_p$: Cyclic Galois Group

Example 5.3 ($\mathbb{F}_{p^{12}}/\mathbb{F}_p$ and $\mathbb{Z}/12\mathbb{Z}$). By Theorem 4.4, $\mathrm{Gal}(\mathbb{F}_{p^{12}}/\mathbb{F}_p)=\langle\varphi\rangle\cong\mathbb{Z}/12\mathbb{Z}$, where φ is the Frobenius.

The subgroups of $\mathbb{Z}/12\mathbb{Z}$ are $\langle d\rangle\cong\mathbb{Z}/(12/d)\mathbb{Z}$ for each divisor d of 12: $d\in\{1,2,3,4,6,12\}$. The fixed field of $\langle\varphi^d\rangle$ is $\mathbb{F}_{p^d}$.

Subgroup $\langle\varphi^d\rangle$	Order	Fixed field
$\langle\varphi\rangle$	12	$\mathbb{F}_p$
$\langle\varphi^2\rangle$	6	$\mathbb{F}_{p^2}$
$\langle\varphi^3\rangle$	4	$\mathbb{F}_{p^3}$
$\langle\varphi^4\rangle$	3	$\mathbb{F}_{p^4}$
$\langle\varphi^6\rangle$	2	$\mathbb{F}_{p^6}$
$\{1\}$	1	$\mathbb{F}_{p^{12}}$

Since $\mathbb{Z}/12\mathbb{Z}$ is abelian, every subgroup is normal, so every $\mathbb{F}_{p^d}/\mathbb{F}_p$ is Galois as expected.

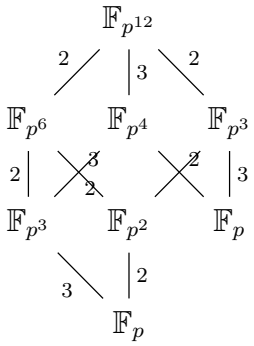


Figure 5.4: Subfield lattice of $\mathbb{F}_{p^{12}}/\mathbb{F}_p$. The divisibility lattice of 12 governs the structure.

5.3 The Primitive Element Theorem

Theorem 5.2 (Primitive Element Theorem)**.** Let L/K be a finite separable extension. Then there exists $\alpha \in L$ such that $L = K(\alpha)$. Such an α is called a *primitive element* of the extension.

Proof. If K is finite, then L is also finite, and $L^\times$ is cyclic (a finite subgroup of the multiplicative group of a field is cyclic). Any generator α of $L^\times$ satisfies $L = K(\alpha)$.

Assume K is infinite. It suffices to treat the case $L = K(\beta, \gamma)$ (the general case follows by induction). Let $f = \mathrm{irr}(\beta, K)$ with roots $\beta = \beta_1, \dots, \beta_m$ and $g = \mathrm{irr}(\gamma, K)$ with roots $\gamma = \gamma_1, \dots, \gamma_n$ in $\overline{K}$. Since L/K is separable, the roots of f and g are distinct.

For $i \geq 1$ and $j \geq 2$, the equation $\beta_i + t\gamma_j = \beta + t\gamma$ (equivalently $t = (\beta_i - \beta)/(\gamma - \gamma_j)$) has at most one solution $t \in K$. Since K is infinite, we may choose $c \in K$ avoiding all such values. Set $\alpha = \beta + c\gamma$. We claim $L = K(\alpha)$.

Clearly $K(\alpha) \subseteq K(\beta, \gamma) = L$. For the reverse, set $h(X) = f(\alpha - cX) \in K(\alpha)[X]$. Then $h(\gamma) = f(\beta) = 0$, so γ is a common root of $h(X)$ and $g(X)$ in $\overline{K}$. We show $\gcd(h, g)$ in $K(\alpha)[X]$ has γ as its only root.

If γ_j (with $j \geq 2$) were also a root of h, then $f(\alpha - c\gamma_j) = 0$, so $\alpha - c\gamma_j = \beta_i$ for some i. Then $\beta + c\gamma - c\gamma_j = \beta_i$, i.e., $c = (\beta_i - \beta)/(\gamma - \gamma_j)$, contradicting our choice of c.

Therefore $\gcd(h, g)$ in $K(\alpha)[X]$ is the minimal polynomial of γ over $K(\alpha)$, which must be linear, giving $\gamma \in K(\alpha)$. Hence $\beta = \alpha - c\gamma \in K(\alpha)$, and $L = K(\beta, \gamma) \subseteq K(\alpha)$. □

Example 5.4 (Primitive element of $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,)$). We have $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,) = \mathbb{Q}(\sqrt{2} + \sqrt{3}\,)$. Indeed, if $\alpha = \sqrt{2} + \sqrt{3}$, then $\alpha^2 = 5 + 2\sqrt{6}$, so $\sqrt{6} \in \mathbb{Q}(\alpha)$, whence $\sqrt{3} = \alpha\sqrt{6} - 3\alpha = (\alpha^2 - 5)/2 \cdot \alpha^{-1}$... more directly: $\alpha^2 = 5 + 2\sqrt{6}$ gives $\sqrt{6} \in \mathbb{Q}(\alpha)$; then $\sqrt{3} = \sqrt{6}/\sqrt{2}$ and $\sqrt{2} = \alpha - \sqrt{3} \in \mathbb{Q}(\alpha)$.

5.4 Exercises

Exercise 5.1 (Full Galois correspondence for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}\,)/\mathbb{Q}$). Show that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}\,)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$ and list all 16 subgroups with their fixed fields.

Exercise 5.2 (Galois correspondence for $X^4 - 2$). Draw the complete lattice of subgroups of D_4 and the corresponding lattice of intermediate fields for the splitting field of $X^4 - 2$ over $\mathbb{Q}$. Identify which intermediate extensions are Galois over $\mathbb{Q}$.

Exercise 5.3 (The FTGT for cyclic extensions). Let L/K be a Galois extension with $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$. Prove that the intermediate fields are in bijection with the divisors of n, and that every intermediate extension is Galois over K.

Exercise 5.4 (Degree formula verification). In Example 5.2, verify the degree–index formula $[E : K] = [G : H]$ for each intermediate field E.

Exercise 5.5 (Non-abelian Galois group). Give an example of a Galois extension L/K with an intermediate field E such that E/K is *not* Galois.

Exercise 5.6 (Galois closure). Let L/K be a finite separable extension. Prove that there exists a smallest Galois extension M/K containing L, and express $\mathrm{Gal}(M/K)$ as a subgroup of a symmetric group.

Exercise 5.7 (Intersection and compositum). Let L/K be Galois with $G = \mathrm{Gal}(L/K)$, and let E_1, E_2 be intermediate fields with corresponding subgroups H_1, H_2. Show:

1. $E_1 \cap E_2 \longleftrightarrow \langle H_1, H_2 \rangle$.
2. $E_1 E_2 \longleftrightarrow H_1 \cap H_2$.

Exercise 5.8 (Primitive element for $\mathbb{Q}(\sqrt[4]{2}, i)$). Find a primitive element for $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$.

Exercise 5.9 (Finite fields and the FTGT). Apply the Fundamental Theorem to $\mathbb{F}_{p^{30}}/\mathbb{F}_p$. List all intermediate fields and draw the lattice.

Exercise 5.10 (Abelian extensions of $\mathbb{Q}$). Show that every finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension $\mathbb{Q}(\zeta_n)$. *(This is the Kronecker–Weber theorem; give a proof sketch.)*

Exercise 5.11 (Quotient groups and intermediate Galois groups). Let L/K be Galois and E an intermediate field with E/K Galois. Show that the restriction map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ is surjective with kernel $\mathrm{Gal}(L/E)$, recovering $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$.

Chapter Summary

- The **Fundamental Theorem of Galois Theory** establishes an inclusion-reversing bijection between intermediate fields of a Galois extension L/K and subgroups of $\mathrm{Gal}(L/K)$.
- **Degree–index duality**: $[E : K] = [G : \mathrm{Gal}(L/E)]$.
- **Normality criterion**: E/K is Galois $\Leftrightarrow \mathrm{Gal}(L/E) \trianglelefteq \mathrm{Gal}(L/K)$, and then $\mathrm{Gal}(E/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/E)$.
- The **Primitive Element Theorem** guarantees that every finite separable extension is simple: $L = K(\alpha)$.

Chapter 6

Applications of Galois Theory

In this final chapter we present three celebrated applications of Galois theory: the classical Greek construction problems, the solvability of polynomial equations by radicals, and a proof of the Fundamental Theorem of Algebra.

6.1 Ruler-and-Compass Constructibility

6.1.1 Constructible Numbers

Starting from two marked points at distance 1, a real number α is *constructible* if a segment of length $|\alpha|$ can be produced in finitely many steps using an unmarked straightedge and a compass.

Definition 6.1 (Field of constructible numbers)**.** A real number α is *constructible* if it can be obtained from $\{0, 1\}$ by a finite sequence of additions, subtractions, multiplications, divisions, and extractions of square roots of positive numbers.

Theorem 6.1 (Constructible numbers form a field)**.** The set of constructible numbers forms a subfield of $\mathbb{R}$, closed under taking square roots of positive elements.

Proof. Each basic straightedge-and-compass operation corresponds to:

- intersecting two lines (solving a linear system yields elements of the current field);
- intersecting a line with a circle, or two circles (solving a quadratic equation yields elements in a degree ≤ 2 extension of the current field).

Hence the set of constructible numbers is closed under $+, -, \times, \div$ and $\sqrt{\ }$ (for positive elements). Closure under the four arithmetic operations shows it is a field. □

Theorem 6.2 (Degree criterion for constructibility)**.** If $\alpha \in \mathbb{R}$ is constructible, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$ for some $s \geq 0$.

Proof. Starting from $K_0 = \mathbb{Q}$, each construction step produces a point in a field K_{i+1} with $[K_{i+1} : K_i] \in \{1, 2\}$ (line–line intersections stay in the same field; line–circle or

circle–circle intersections adjoin at most a square root). After r steps, $\alpha \in K_r$ where

$$[K_r : \mathbb{Q}] = [K_r : K_{r-1}] \cdots [K_1 : K_0] = 2^s$$

for some $s \leq r$. By the tower law, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divides $[K_r : \mathbb{Q}] = 2^s$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is also a power of 2. □

Remark 6.1 (Converse). The converse is not quite true in general: $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ being a power of 2 is necessary but not sufficient. However, α is constructible if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2 *and* the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree a power of 2 over $\mathbb{Q}$ (equivalently, the Galois group is a 2-group).

6.1.2 The Three Classical Impossibilities

Corollary 6.1 (Doubling the cube is impossible)**.** It is impossible to construct, with ruler and compass alone, the side of a cube of volume 2.

Proof. The required length is $\sqrt[3]{2}$. We have $\operatorname{irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$ (irreducible by Eisenstein at $p = 2$), so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Since 3 is not a power of 2, the construction is impossible by Theorem 6.2. □

Corollary 6.2 (Trisecting a general angle is impossible)**.** There is no ruler-and-compass construction that trisects every given angle.

Proof. It suffices to show that the angle 60 cannot be trisected, i.e., that $\cos 20$ is not constructible. The triple-angle formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ with $\theta = 20$ gives $4c^3 - 3c = \cos 60 = 1/2$, where $c = \cos 20$. Setting $c = t/2$: $t^3 - 3t - 1 = 0$. This polynomial is irreducible over $\mathbb{Q}$ (it has no rational roots by the rational root theorem), so $[\mathbb{Q}(\cos 20) : \mathbb{Q}] = 3$. Again $3 \neq 2^s$, so the construction is impossible. □

Corollary 6.3 (Squaring the circle is impossible)**.** It is impossible to construct with ruler and compass a square of area π.

Proof. The required side length is $\sqrt{\pi}$, so it suffices to show π is not constructible. But π is transcendental (Lindemann, 1882), hence $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$, which is certainly not a power of 2. □

6.1.3 Constructibility of Regular Polygons

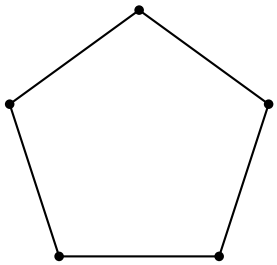
Theorem 6.3 (Gauss–Wantzel)**.** A regular n-gon (with $n \geq 3$) is constructible with ruler and compass if and only if

$$n = 2^a \, p_1 \, p_2 \cdots p_r,$$

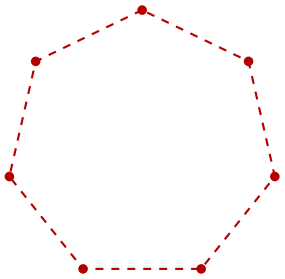
where $a \geq 0$ and $p_1, \ldots, p_r$ are *distinct* Fermat primes, i.e., primes of the form $F_k = 2^{2^k} + 1$.

Proof sketch. Constructing a regular n-gon amounts to constructing $\cos(2\pi/n)$. One has $\mathbb{Q}(\cos(2\pi/n)) \subseteq \mathbb{Q}(\zeta_n)$ with $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\cos(2\pi/n))] = 2$. By Theorem 4.5, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. The angle $2\pi/n$ is constructible if and only if $\varphi(n)$ is a power of 2, which holds precisely when n has the given form. □

Remark 6.2 (Known Fermat primes). The known Fermat primes are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. It is unknown whether any others exist. Thus the constructible regular n-gons for odd n include $n = 3, 5, 15, 17, 51, 85, 255, 257, \ldots$



Regular pentagon ($n = 5 = F_1$)



Regular heptagon ($n = 7$): impossible

Figure 6.1: The regular pentagon is constructible (5 is a Fermat prime); the regular heptagon is not ($\varphi(7) = 6 \neq 2^s$).

6.2 Solvability by Radicals

6.2.1 Radical Extensions and Solvable Groups

Definition 6.2 (Radical extension)**.** A field extension L/K is a *radical extension* if there exists a tower

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = L$$

where each $K_{i+1} = K_i(\alpha_i)$ with $\alpha_i^{n_i} \in K_i$ for some $n_i \geq 1$.

Definition 6.3 (Solvable by radicals)**.** A polynomial $f \in K[X]$ is *solvable by radicals* if its splitting field is contained in some radical extension of K.

Definition 6.4 (Solvable group)**.** A group G is *solvable* if there exists a chain of subgroups

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G$$

such that each quotient G_{i+1}/G_i is abelian.

Example 6.1 (Solvable groups).

1. Every abelian group is solvable (take $r = 1$).
2. S_3 is solvable: $\{1\} \trianglelefteq A_3 \trianglelefteq S_3$ with $A_3/\{1\} \cong \mathbb{Z}/3\mathbb{Z}$ and $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$.
3. S_4 is solvable: $\{1\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$.

6.2.2 S_n Is Not Solvable for $n \geq 5$

Theorem 6.4 (S_n is not solvable for $n \geq 5$)**.** For $n \geq 5$, the symmetric group S_n is not solvable.

Proof. We first establish that A_n is simple for $n \geq 5$, then use this to prove S_n is not solvable.

Step 1: A_n is simple for $n \geq 5$. Let $N \trianglelefteq A_n$ with $N \neq \{1\}$. We show $N = A_n$ by proving N contains all 3-cycles (which generate A_n).

Let $\sigma \in N \setminus \{1\}$. We consider cases based on the cycle structure of σ.

Case 1: σ contains a cycle of length ≥ 3, say σ moves $1 \mapsto 2 \mapsto 3$. Let $\tau = (3\ 4\ 5) \in A_n$. Then the commutator $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} \in N$ is a non-identity element that can be shown (by direct computation, considering sub-cases) to yield a permutation moving fewer elements than σ. Iterating, we reduce to elements that are products of fewer cycles.

Case 2: σ is a product of disjoint transpositions, say $\sigma = (1\ 2)(3\ 4)\cdots$. Then for $\tau = (1\ 2\ 3) \in A_n$, $\tau\sigma\tau^{-1} = (2\ 3)(1\ 4)\cdots \in N$, and multiplying: $\sigma \cdot \tau\sigma\tau^{-1} = (1\ 3\ 4\ 2)\cdots \in N$ (or a shorter permutation), reducing to Case 1 or giving a 3-cycle directly.

In all cases, since $n \geq 5$ provides enough "room" to manoeuvre with conjugation, one shows that N must contain a 3-cycle. Since all 3-cycles are conjugate in A_n (for $n \geq 5$), N contains all 3-cycles, hence $N = A_n$.

Step 2: S_n is not solvable. Suppose S_n is solvable with composition series $\{1\} = G_0 \trianglelefteq \cdots \trianglelefteq G_r = S_n$ (abelian quotients). Then $A_n \cap G_i$ gives a composition series for A_n with abelian quotients, so A_n would be solvable. But the only normal subgroups of A_n (for $n \geq 5$) are $\{1\}$ and A_n, and $A_n/\{1\} = A_n$ is not abelian for $n \geq 5$. Contradiction. □

6.2.3 Galois's Theorem and the Abel–Ruffini Theorem

Theorem 6.5 (Galois's theorem)**.** Let $f \in K[X]$ be a separable polynomial with splitting field L over K, where $\mathrm{char}(K) = 0$. Then f is solvable by radicals if and only if $\mathrm{Gal}(L/K)$ is a solvable group.

Proof sketch. ($\Longrightarrow$) If f is solvable by radicals, the splitting field L is contained in a radical tower $K = K_0 \subset K_1 \subset \cdots \subset K_r$. After adjoining appropriate roots of unity, each step $K_i \subset K_{i+1}$ becomes a cyclic (hence abelian) Galois extension (Kummer theory). The Galois group $\mathrm{Gal}(L/K)$ is then a quotient of a group with an abelian composition series, hence is solvable.

($\Longleftarrow$) If $\mathrm{Gal}(L/K)$ is solvable, one constructs a radical tower containing L by reversing the argument: the composition series with abelian (in fact cyclic) quotients corresponds, via Kummer theory and the Fundamental Theorem, to successive radical adjunctions. □

Theorem 6.6 (Abel–Ruffini)**.** The general polynomial equation of degree $n \geq 5$ is not solvable by radicals. More precisely, for each $n \geq 5$ there exist polynomials $f \in \mathbb{Q}[X]$ of degree n whose Galois group over $\mathbb{Q}$ is S_n, and since S_n is not solvable (Theorem 6.4), f is not solvable by radicals.

Example 6.2 ($X^5 - 4X + 2$ has Galois group S_5). Consider $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$.

1. **Irreducibility.** By Eisenstein's criterion at $p = 2$, f is irreducible over $\mathbb{Q}$.

2. **Real roots.** One checks that f has exactly three real roots and two complex conjugate roots (by analysing $f' = 5X^4 - 4$: the critical points are at $x = \pm(4/5)^{1/4}$; evaluating f at these points and at $\pm\infty$ shows three real zeros).

3. **Galois group.** The Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ embeds into S_5 (acting on the five roots). Since f is irreducible of degree 5, G acts transitively, so $5 \mid |G|$. Complex conjugation gives a transposition in G (swapping the two complex roots). A transitive subgroup of S_5 containing a transposition and an element of order 5 (by Cauchy's theorem, since $5 \mid |G|$) is all of S_5. Hence $G \cong S_5$.

Since S_5 is not solvable, f is not solvable by radicals.

6.3 The Fundamental Theorem of Algebra

Theorem 6.7 (Fundamental Theorem of Algebra)**.** The field $\mathbb{C}$ is algebraically closed: every non-constant polynomial $f \in \mathbb{C}[X]$ has a root in $\mathbb{C}$.

Proof via Galois theory. We use two analytic facts: (i) every polynomial in $\mathbb{R}[X]$ of odd degree has a real root; (ii) every positive real number has a real square root.

Let $f \in \mathbb{R}[X]$ be irreducible. Let L be the splitting field of f over $\mathbb{R}$. Then $L/\mathbb{R}$ is a finite Galois extension; set $G = \mathrm{Gal}(L/\mathbb{R})$ and $|G| = 2^s \cdot m$ with m odd.

Step 1: $m = 1$ (i.e., $|G|$ is a power of 2).

Let P be a Sylow 2-subgroup of G and $E = L^P$. Then $[E : \mathbb{R}] = [G : P] = m$. By the Primitive Element Theorem, $E = \mathbb{R}(\alpha)$ and $\mathrm{irr}(\alpha, \mathbb{R})$ has odd degree m. By fact (i), this polynomial has a root in $\mathbb{R}$, so $m = 1$ (since it is irreducible and has a real root, it must be linear). Hence $|G| = 2^s$.

Step 2: $s \leq 1$ (i.e., $|G| \leq 2$).

Suppose $s \geq 2$. Since G is a 2-group, it has a subgroup H of index 2 (indeed, of index 2 in some subgroup of index 2, etc.). Let $M = L^H$. Then $[M : \mathbb{R}] = 2$, so $M = \mathbb{R}(\beta)$ with $\mathrm{irr}(\beta, \mathbb{R}) = X^2 + bX + c$ for some $b, c \in \mathbb{R}$. By fact (ii), the discriminant $b^2 - 4c$ satisfies: if $b^2 - 4c < 0$, then $\beta = (-b \pm i\sqrt{4c - b^2})/2 \in \mathbb{C}$. But we are working with $L/\mathbb{R}$, and $\mathbb{C} = \mathbb{R}(i)$ already contains all roots of quadratics over $\mathbb{R}$. So $M \subseteq \mathbb{C}$; but $[M : \mathbb{R}] = 2 = [\mathbb{C} : \mathbb{R}]$, hence $M = \mathbb{C}$.

Now consider $\mathrm{Gal}(L/\mathbb{C})$. If $\mathrm{Gal}(L/\mathbb{C})$ had a subgroup of index 2, the same argument would produce a degree-2 extension of $\mathbb{C}$, say $\mathbb{C}(\gamma)$ with $\gamma^2 + b'\gamma + c' = 0$ for $b', c' \in \mathbb{C}$. But the quadratic formula shows $\gamma \in \mathbb{C}$ (since $\mathbb{C}$ is closed under square roots by fact (ii) and the polar form of complex numbers). This is a contradiction: the extension would be trivial.

Since $\mathrm{Gal}(L/\mathbb{C})$ is a 2-group that has no subgroup of index 2 (other than itself if it is non-trivial), we must have $\mathrm{Gal}(L/\mathbb{C}) = \{1\}$, i.e., $L = \mathbb{C}$. Hence $|G| = [\mathbb{C} : \mathbb{R}] = 2$ and $s = 1$.

Conclusion. Every irreducible $f \in \mathbb{R}[X]$ has $\deg f \leq 2$. Equivalently, every $f \in \mathbb{R}[X]$ factors into linear and quadratic factors over $\mathbb{R}$, hence into linear factors over $\mathbb{C}$. It follows that $\mathbb{C}$ is algebraically closed. □

6.4 Concluding Remarks: Further Directions

Galois theory, far from being a closed chapter, serves as a gateway to some of the deepest areas of modern mathematics.

- **Algebraic geometry.** The Galois group of the function field of an algebraic curve encodes arithmetic and geometric information. Étale cohomology, developed by Grothendieck, generalises Galois theory to schemes and is the foundation of modern arithmetic geometry.
- **Algebraic number theory.** The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is the central object of study. Class field theory classifies abelian extensions of number fields via Artin reciprocity, while the Langlands programme seeks a vast non-abelian generalisation.
- **Inverse Galois problem.** Which finite groups arise as $\mathrm{Gal}(L/\mathbb{Q})$? This remains one of the great open questions. Shafarevich proved every solvable group occurs; the general case is open.
- **Differential Galois theory.** Replacing polynomial equations by linear differential equations, the Picard–Vessiot theory develops a Galois correspondence for differential fields, with applications to the integrability of dynamical systems.
- **Representation theory.** Representations of Galois groups (Artin representations, ℓ-adic representations) are at the heart of the Langlands programme.

6.5 Exercises

Exercise 6.1 (Constructibility of $\cos(2\pi/17)$). Use the fact that $\mathrm{Gal}(\mathbb{Q}(\zeta_{17})/\mathbb{Q}) \cong (\mathbb{Z}/17\mathbb{Z})^{\times} \cong \mathbb{Z}/16\mathbb{Z}$ to explain why the regular 17-gon is constructible. Describe the tower of quadratic extensions.

Exercise 6.2 (Non-constructibility of $\sqrt[3]{2}$). Give a self-contained proof that $\sqrt[3]{2}$ is not constructible.

Exercise 6.3 (Solvable Galois groups of cubics and quartics). Show that the Galois group of any irreducible polynomial of degree ≤ 4 over $\mathbb{Q}$ is solvable, and conclude that every such polynomial is solvable by radicals.

Exercise 6.4 (Explicit radical solution of a cubic). Solve $X^3 - 3X + 1 = 0$ by radicals. *Hint:* the discriminant is 81, a perfect square, so $\mathrm{Gal} \cong \mathbb{Z}/3\mathbb{Z}$.

Exercise 6.5 (Galois group of $X^5 - 2$). Show that $\mathrm{Gal}(\mathbb{Q}(\sqrt[5]{2}, \zeta_5)/\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \rtimes (\mathbb{Z}/5\mathbb{Z})^{\times}$ (the Frobenius group of order 20), and conclude that $X^5 - 2$ is solvable by radicals.

Exercise 6.6 (Another unsolvable quintic). Show that $X^5 - 6X + 3 \in \mathbb{Q}[X]$ has Galois group S_5 and is therefore not solvable by radicals.

Exercise 6.7 (FTA via Liouville). Give an alternative proof of the Fundamental Theorem of Algebra using Liouville's theorem from complex analysis.

Exercise 6.8 (Constructible regular polygons). For which $n \leq 30$ is the regular n-gon constructible? List all such n.

Exercise 6.9 (Composition series of S_4). Write down a composition series for S_4 and verify that all composition factors are cyclic of prime order.

Exercise 6.10 (Solvability and the discriminant). Let $f \in \mathbb{Q}[X]$ be irreducible of degree 5 with discriminant Δ. Show that if $\sqrt{\Delta} \in \mathbb{Q}$, then $\mathrm{Gal}(f) \leq A_5$. Since A_5 is not solvable, such a polynomial is still generally not solvable by radicals.

Chapter Summary

- A real number α is **constructible** only if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2. This rules out doubling the cube, trisecting a general angle, and squaring the circle.
- **Gauss–Wantzel**: a regular n-gon is constructible $\Leftrightarrow n = 2^a p_1 \cdots p_r$ with distinct Fermat primes p_i.
- **Galois's theorem**: a polynomial (in characteristic 0) is solvable by radicals $\Leftrightarrow$ its Galois group is solvable.
- Since S_n is not solvable for $n \geq 5$, the **general quintic** is not solvable by radicals (**Abel–Ruffini**).
- The **Fundamental Theorem of Algebra** admits an elegant proof using Galois theory and Sylow theory.

Bibliography

[1] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, Hoboken, NJ, 2004.

[2] S. Lang, *Algebra*, rev. 3rd ed., Graduate Texts in Mathematics 211, Springer-Verlag, New York, 2002.

[3] M. Artin, *Algebra*, 2nd ed., Pearson, Boston, 2011.

[4] N. Jacobson, *Basic Algebra I & II*, 2nd ed., W. H. Freeman, New York, 1985–1989.

[5] N. Bourbaki, *Algèbre*, Chapitres 4 à 7, Springer-Verlag, Berlin, 2007.

[6] D. Perrin, *Algèbre: Cours de mathématiques pures*, Éditions de l'École Polytechnique, 2019.

[7] I. Stewart, *Galois Theory*, 4th ed., CRC Press, Boca Raton, 2015.

Index