Galois Theory

A Self-Contained Exposition

From First Principles to the Unsolvability of the Quintic

Abstract

These notes build Galois theory from the ground up, assuming no prior knowledge beyond basic arithmetic. We develop set theory, group theory, ring and field theory, and the theory of polynomials, before arriving at the central objects: field extensions and the Galois group. The exposition culminates in two classical impossibility results: the insolubility of certain geometric construction problems, and the non-existence of a general radical formula for polynomial equations of degree five or higher.

Contents

1 Sets and Functions

Before any algebra can begin, we need a shared language for collections of objects and the maps between them.

Definition 1.1 (Set)**.** A **set** is a collection of distinct objects, called **elements**. We write $a \in A$ to mean a is an element of set A.

A **subset** $B \subseteq A$ is a set whose elements all belong to A. A **partition** of A is a collection of non-empty, pairwise disjoint subsets whose union is A.

Definition 1.2 (Function)**.** A **function** $f : A \to B$ assigns to each element $a \in A$ exactly one element $f(a) \in B$. We call A the **domain** and B the **codomain**.

Definition 1.3 (Types of Functions)**.** A function $f : A \to B$ is:

- **injective** (one-to-one) if $f(a_1) = f(a_2)$ implies $a_1 = a_2$;
- **surjective** (onto) if for every $b \in B$ there exists $a \in A$ with $f(a) = b$;
- **bijective** if it is both injective and surjective.

Definition 1.4 (Equivalence Relation)**.** A relation $\sim$ on a set A is an **equivalence relation** if it is reflexive ($a \sim a$), symmetric ($a \sim b \Rightarrow b \sim a$), and transitive ($a \sim b$ and $b \sim c$ implies $a \sim c$). The **equivalence class** of a is $[a] = \{b \in A : b \sim a\}$.

Equivalence classes always partition the set A. This is the prototype for quotient constructions throughout algebra.

2 Group Theory

Groups are the algebraic structures that encode symmetry. They are the central actors in Galois theory.

2.1 Groups: Definition and First Examples

Definition 2.1 (Group)**.** A **group** is a set G together with a binary operation $\cdot : G \times G \to G$ satisfying:

(i) **Associativity:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in G$;

(ii) **Identity:** there exists $e \in G$ such that $e \cdot a = a \cdot e = a$ for all $a \in G$;

(iii) **Inverses:** for each $a \in G$ there exists $a^{-1} \in G$ with $a \cdot a^{-1} = a^{-1} \cdot a = e$.

If additionally $a \cdot b = b \cdot a$ for all $a, b \in G$, the group is called **abelian**.

Example 2.1 (Fundamental Examples)**.**

- $(\mathbb{Z}, +)$: the integers under addition. Identity is 0, inverse of n is $-n$. Abelian.
- $(\mathbb{Z}/n\mathbb{Z}, +)$: integers modulo n, i.e. $\{0, 1, \ldots, n-1\}$ with addition mod n. Abelian, finite, of order n.
- $(S_n, \circ)$: the **symmetric group**, the set of all bijections $\{1, \ldots, n\} \to \{1, \ldots, n\}$ under composition. Non-abelian for $n \geq 3$.

2.2 Subgroups, Cosets, and Lagrange's Theorem

Definition 2.2 (Subgroup)**.** A subset $H \subseteq G$ is a **subgroup**, written $H \leq G$, if it is itself a group under the same operation.

Definition 2.3 (Coset)**.** For $H \leq G$ and $g \in G$, the **left coset** of H by g is $gH = \{gh : h \in H\}$.

The left cosets of H partition G, each having the same size $|H|$. This gives:

Theorem 2.1 (Lagrange)**.** *If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$. In particular,*

$$|G| = [G : H] \cdot |H|$$

*where $[G : H]$ is the number of distinct cosets, called the **index** of H in G.*

2.3 Homomorphisms and Isomorphisms

Definition 2.4 (Homomorphism)**.** A function $\varphi : G \to H$ between groups is a **homomorphism** if

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{for all } a, b \in G.$$

The **kernel** is $\ker \varphi = \{g \in G : \varphi(g) = e_H\}$ and the **image** is $\operatorname{im} \varphi = \{\varphi(g) : g \in G\}$.

Definition 2.5 (Isomorphism)**.** A bijective homomorphism is an **isomorphism**. We write $G \cong H$ if an isomorphism exists; the groups are then structurally identical.

2.4 Normal Subgroups and Quotient Groups

Definition 2.6 (Normal Subgroup)**.** A subgroup $H \leq G$ is **normal**, written $H \trianglelefteq G$, if

$$gHg^{-1} = H \quad \text{for all } g \in G.$$

Equivalently, the left and right cosets coincide: $gH = Hg$ for all $g \in G$.

Normality is precisely the condition required for the cosets of H to themselves form a group.

Definition 2.7 (Quotient Group)**.** If $H \trianglelefteq G$, the **quotient group** G/H is the set of cosets $\{gH : g \in G\}$ with multiplication

$$(aH)(bH) = (ab)H.$$

Its order is $|G/H| = |G|/|H|$. The quotient G/H is G with every element of H collapsed to the identity.

Example 2.2. $\mathbb{Z}/n\mathbb{Z}$ is the quotient of $(\mathbb{Z}, +)$ by the subgroup $n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$. The cosets are the residue classes modulo n.

2.5 Cyclic Groups

Definition 2.8 (Cyclic Group)**.** A group G is **cyclic** if it is generated by a single element:

$$G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

Every cyclic group is abelian. Up to isomorphism there are exactly two families: $\mathbb{Z}$ (infinite) and $\mathbb{Z}/n\mathbb{Z}$ (finite of order n). The elements of $\mathbb{Z}/n\mathbb{Z}$ that generate the whole group are those k with $\gcd(k, n) = 1$; there are $\varphi(n)$ of them.

2.6 Group Actions and Orbits

Definition 2.9 (Group Action)**.** A **group action** of G on a set X is a function $G \times X \to X$, written $(g, x) \mapsto g \cdot x$, satisfying $e \cdot x = x$ and $(gh) \cdot x = g \cdot (h \cdot x)$.

Definition 2.10 (Orbit)**.** The **orbit** of $x \in X$ is $\mathrm{Orb}(x) = \{g \cdot x : g \in G\}$.

Orbits partition X. In Galois theory, the group $\mathrm{Gal}(K/F)$ acts on the roots of a polynomial by permutation. The orbit of a root α is precisely the set of all its algebraic conjugates — roots of the same minimal polynomial over F.

2.7 Permutation Groups and the Alternating Group

Definition 2.11 (Symmetric Group)**.** S_n is the group of all permutations of $\{1, \ldots, n\}$ under composition. $|S_n| = n!$

Every permutation decomposes into disjoint cycles and has a well-defined **sign**: $+1$ (even) or -1 (odd).

Definition 2.12 (Alternating Group)**.** $A_n \trianglelefteq S_n$ is the subgroup of *even* permutations. $|A_n| = n!/2$.

The key fact: A_n is **simple** (no normal subgroups other than $\{e\}$ and itself) for $n \geq 5$. This is the group-theoretic engine behind the unsolvability of the quintic.

2.8 Solvable Groups

Definition 2.13 (Solvable Group)**.** A group G is **solvable** if there exists a chain

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = G$$

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

The **derived series** gives a canonical such chain. Define $G^{(0)} = G$ and

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] = \langle aba^{-1}b^{-1} : a, b \in G^{(i)} \rangle.$$

G is solvable if and only if $G^{(k)} = 1$ for some k.

> **Why this matters.** Abelian quotients can be refined to cyclic ones. So a solvable group is one that can be built from cyclic groups, layer by layer. In Galois theory, each cyclic layer corresponds to a radical step (adjoining an n-th root). Solvability of the Galois group is therefore exactly the condition that the polynomial's roots can be expressed by radicals.

Example 2.3 (Solvability of Small Symmetric Groups)**.**

- S_3: solvable. Chain $1 \trianglelefteq A_3 \trianglelefteq S_3$, quotients $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$.

- S_4: solvable. Chain $1 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$ where V_4 is the Klein four-group.
- S_n, $n \geq 5$: **not solvable**. Since A_n is simple and non-abelian, the derived series stalls: $S_n^{(1)} = A_n$ and $A_n^{(1)} = A_n$.

3 Rings and Fields

3.1 Rings

Definition 3.1 (Ring)**.** A **ring** is a set R with two operations, addition and multiplication, such that $(R, +)$ is an abelian group, multiplication is associative, and multiplication distributes over addition.

Key examples: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, and the polynomial ring $\mathbb{R}[x]$.

3.2 Fields

Definition 3.2 (Field)**.** A **field** is a commutative ring in which every non-zero element has a multiplicative inverse. Equivalently, $(F \setminus \{0\}, \cdot)$ is an abelian group.

Example 3.1 (Fields)**.** $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields. For a prime p, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field, written $\mathbb{F}_p$.

Definition 3.3 (Characteristic)**.** The **characteristic** of a field F is the smallest positive integer n such that $\underbrace{1 + \cdots + 1}_{n} = 0$, or 0 if no such n exists. The characteristic is always 0 or a prime. Fields like $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0.

Theorem 3.1. *Any field homomorphism $\varphi : F \to K$ is injective.*

This means fields embed cleanly into one another — there is no collapsing. It is why field extensions are well-behaved.

Definition 3.4 (Ideals and Quotient Rings)**.** An **ideal** $I \subseteq R$ is a subset closed under addition and under multiplication by any ring element. The **quotient ring** R/I consists of cosets $r + I$ with the natural addition and multiplication. When $p(x) \in F[x]$ is irreducible, $F[x]/(p(x))$ is a field.

4 Polynomials

Definition 4.1 (Polynomial Ring)**.** For a field F, the **polynomial ring** $F[x]$ consists of all expressions $a_0 + a_1 x + \cdots + a_n x^n$ with $a_i \in F$, under formal addition and multiplication.

Definition 4.2 (Irreducible Polynomial)**.** A polynomial $f \in F[x]$ of degree ≥ 1 is **irreducible over** F if it cannot be written as $f = gh$ with $g, h \in F[x]$ both of degree ≥ 1.

> **Irreducibility depends on the field.** The polynomial $x^2 + 1$ is irreducible over $\mathbb{R}$ (no real square root of -1) but factors as $(x+i)(x-i)$ over $\mathbb{C}$. This field-dependence is

the entire point: adjoining a root of an irreducible polynomial is how field extensions are built.

Theorem 4.1 (Factor Theorem). *α is a root of $f \in F[x]$ if and only if $(x-\alpha)$ divides f in $F[x]$.*

A polynomial of degree n over a field has at most n roots. A root α has **multiplicity** m if $(x-\alpha)^m \mid f$ but $(x-\alpha)^{m+1} \nmid f$.

4.1 Roots of Unity

Definition 4.3 (Root of Unity). An n-th **root of unity** is a root of $x^n - 1$. The **primitive n-th root of unity** is

$$\zeta_n = e^{2\pi i/n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

All n-th roots of unity are $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$, forming a cyclic group of order n under multiplication.

These roots will reappear as the connection between cyclic group extensions and radical (root-extraction) steps.

5 Field Extensions

5.1 Definitions and Degree

Definition 5.1 (Field Extension). A **field extension** K/F is a pair of fields with $F \subseteq K$. We call F the **base field** and K the **extension**.

Since $F \subseteq K$ and K is a field, K is naturally a vector space over F.

Definition 5.2 (Degree). The **degree** of K/F is $[K : F] = \dim_F K$, the dimension of K as an F-vector space.

Theorem 5.1 (Tower Law). *If $F \subseteq E \subseteq K$ are fields, then*

$$[K : F] = [K : E] \cdot [E : F].$$

The tower law is the primary computational tool throughout what follows. Every argument about whether a construction is possible runs through this formula.

5.2 Simple Extensions

Definition 5.3 (Simple Extension). For $\alpha \in K$, the field $F(\alpha)$ is the smallest subfield of K containing both F and α.

Definition 5.4 (Algebraic Element). $\alpha \in K$ is **algebraic over** F if it is the root of some non-zero polynomial $f \in F[x]$. Otherwise it is **transcendental**.

Definition 5.5 (Minimal Polynomial). The **minimal polynomial** of an algebraic element α over F is the unique monic irreducible polynomial $p \in F[x]$ with $p(\alpha) = 0$.

Theorem 5.2. *If α is algebraic over F with minimal polynomial p of degree d, then*

$$[F(\alpha) : F] = d \quad \textit{and} \quad F(\alpha) \cong F[x]/(p(x)).$$

Example 5.1. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, since $\sqrt{2}$ has minimal polynomial $x^2 - 2$. Elements of $\mathbb{Q}(\sqrt{2})$ are $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

5.3 Splitting Fields

Definition 5.6 (Splitting Field)**.** The **splitting field** of $f \in F[x]$ is the smallest extension K/F over which f factors completely into linear factors:

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \quad \alpha_i \in K.$$

Theorem 5.3. *Every polynomial over a field has a splitting field, unique up to isomorphism.*

5.4 Cyclotomic Fields

Definition 5.7 (Cyclotomic Field)**.** The **n-th cyclotomic field** $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$.

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

5.5 Separable and Normal Extensions

Definition 5.8 (Separable Polynomial)**.** $f \in F[x]$ is **separable** if it has no repeated roots (in its splitting field). Over fields of characteristic 0 — such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — every irreducible polynomial is automatically separable.

Definition 5.9 (Normal Extension)**.** K/F is **normal** if it is the splitting field of some polynomial over F. Equivalently: whenever an irreducible polynomial in $F[x]$ has one root in K, it has all its roots in K.

6 Compass and Straightedge Constructions

Before introducing the full Galois group, we can already obtain a striking application of field extensions alone.

6.1 What Constructions Are Allowed

The classical Greek rules: given two points (defining a unit length), one may:

(i) draw the line through any two constructed points;

(ii) draw the circle centred at a constructed point passing through another;

(iii) mark the intersection points of constructed lines and circles.

Each such step, when expressed algebraically, amounts to solving a linear or quadratic equation — it produces an element lying in a degree-2 extension of the current field.

Theorem 6.1 (Constructibility Criterion)**.** *A real number α is constructible by compass and straightedge if and only if there is a tower of fields*

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_k$$

with $\alpha \in F_k$ and $[F_{i+1} : F_i] = 2$ for each i. By the tower law, this forces $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ to be a power of 2.

Contrapositive (the useful direction). If $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is *not* a power of 2, then α is not constructible.

6.2 Three Classical Impossibilities

Theorem 6.2 (Doubling the Cube)**.** *It is impossible to construct, by compass and straightedge, a cube with exactly twice the volume of a given unit cube.*

Proof. Doubling the unit cube requires constructing $\alpha = 2^{1/3}$. Its minimal polynomial over $\mathbb{Q}$ is $x^3 - 2$, which is irreducible (by Eisenstein with $p = 2$). Therefore $[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$, which is not a power of 2. □

Theorem 6.3 (Trisecting the Angle)**.** *It is impossible to trisect an arbitrary angle by compass and straightedge.*

Proof. It suffices to show that $60°$ cannot be trisected, i.e. that $20°$ is not constructible. Using the identity $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$ with $\theta = 20°$:

$$4\cos^3(20°) - 3\cos(20°) = \cos(60°) = \frac{1}{2}.$$

Setting $c = \cos(20°)$, we get $8c^3 - 6c - 1 = 0$. This polynomial is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(c) : \mathbb{Q}] = 3$, which is not a power of 2. □

Theorem 6.4 (Squaring the Circle)**.** *It is impossible to construct a square with the same area as a given unit circle.*

Proof. The required length is $\sqrt{\pi}$. Since π is transcendental (Lindemann, 1882), $\sqrt{\pi}$ is also transcendental. Transcendental numbers are not algebraic, hence not constructible. □

Summary.

Problem	Required number	Obstruction
Doubling the cube	$2^{1/3}$	$[\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$
Trisecting $60°$	$\cos(20°)$	$[\mathbb{Q}(\cos 20°) : \mathbb{Q}] = 3$
Squaring the circle	$\sqrt{\pi}$	π transcendental

7 The Galois Group

7.1 Automorphisms of Field Extensions

Definition 7.1 (F-Automorphism)**.** Let K/F be a field extension. An **F-automorphism** of K is a field isomorphism $\sigma : K \to K$ that fixes F pointwise: $\sigma(a) = a$ for all $a \in F$.

Definition 7.2 (Galois Group)**.** The **Galois group** of K/F is

$$\mathrm{Gal}(K/F) = \{\sigma : K \xrightarrow{\sim} K : \sigma(a) = a \ \forall a \in F\},$$

the group of all F-automorphisms of K, under composition.

7.2 How the Galois Group Acts on Roots

If $f \in F[x]$ and $\sigma \in \mathrm{Gal}(K/F)$, then for any root α of f:

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

So σ maps roots of f to roots of f. If f has roots $\alpha_1, \ldots, \alpha_n$ in K, this gives an embedding

$$\mathrm{Gal}(K/F) \hookrightarrow S_n.$$

The orbit of α_i under this action is the set of conjugates of α_i over F — exactly the other roots of α_i's minimal polynomial.

7.3 Galois Extensions and Fixed Fields

Definition 7.3 (Galois Extension)**.** K/F is a **Galois extension** if it is both normal and separable. In this case,

$$|\mathrm{Gal}(K/F)| = [K : F].$$

Definition 7.4 (Fixed Field)**.** For a subgroup $H \leq \mathrm{Gal}(K/F)$, the **fixed field** is

$$K^H = \{x \in K : \sigma(x) = x \ \text{ for all } \sigma \in H\}.$$

Example 7.1 (Cyclotomic Galois Group)**.** The cyclotomic field $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois. Each automorphism is determined by its value on ζ_n, and must send ζ_n to another primitive n-th root of unity ζ_n^k with $\gcd(k, n) = 1$. This gives:

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

This group is abelian, so all cyclotomic extensions are solvable — consistent with the fact that roots of unity are radical expressions.

8 The Fundamental Theorem of Galois Theory

The central result of the theory establishes a perfect dictionary between subgroups of the Galois group and intermediate fields of the extension.

Theorem 8.1 (Fundamental Theorem of Galois Theory)**.** *Let K/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/F)$. There is an order-reversing bijection:*

$$\{\textit{subgroups } H \leq G\} \ \longleftrightarrow \ \{\textit{intermediate fields } F \subseteq E \subseteq K\}$$

given by $H \mapsto K^H$ and $E \mapsto \mathrm{Gal}(K/E)$, with inverse maps to each other.

Moreover:

(i) $[K : K^H] = |H|$ *and* $[K^H : F] = [G : H]$;

(ii) $H \trianglelefteq G$ *if and only if* K^H/F *is a Galois extension;*

(iii) When $H \trianglelefteq G$: $\mathrm{Gal}(K^H/F) \cong G/H$.

Intuition. Larger subgroups fix fewer elements, giving smaller intermediate fields. The correspondence inverts inclusion. Normal subgroups correspond to extensions that are themselves Galois — the quotient group is then the Galois group of that sub-extension.

9 Solvability by Radicals

9.1 Radical Extensions

Definition 9.1 (Radical Extension)**.** An extension K/F is a **radical extension** if there is a tower

$$F = F_0 \subset F_1 \subset \cdots \subset F_k = K$$

where each $F_{i+1} = F_i(\alpha_i)$ with $\alpha_i^{n_i} \in F_i$ for some integer n_i.

In other words: K is built from F by successively adjoining n-th roots. This is precisely what it means to express something "by radicals."

Definition 9.2 (Solvable by Radicals)**.** A polynomial $f \in F[x]$ is **solvable by radicals** if its roots lie in some radical extension of F.

9.2 Cyclic Extensions

Each step $F_i \subset F_{i+1}$ in a radical tower, when the appropriate roots of unity are present, is a **cyclic extension**: a Galois extension whose Galois group is cyclic. This is because adjoining α with $\alpha^n \in F$ (when F contains the n-th roots of unity) gives an extension with $\mathrm{Gal}(F(\alpha)/F) \cong \mathbb{Z}/n\mathbb{Z}$.

9.3 The Main Theorem

Theorem 9.1 (Galois)**.** *Let* F *have characteristic* 0 *and* $f \in F[x]$. *Let* K *be the splitting field of* f *over* F. *Then:*

$$f \text{ is solvable by radicals} \iff \mathrm{Gal}(K/F) \text{ is a solvable group.}$$

The proof proceeds in two directions. If the Galois group is solvable, one uses its abelian quotients to build a sequence of cyclic (radical) extensions reaching K. Conversely, if f is solvable by radicals, the radical tower produces a solvable group containing $\mathrm{Gal}(K/F)$ as a subgroup (and subgroups of solvable groups are solvable).

9.4 The General Quintic Has No Radical Solution

Theorem 9.2. *For $n \geq 5$, there is no formula expressing the roots of a general degree-n polynomial in terms of its coefficients using only field operations and radicals.*

Proof outline. It suffices to exhibit a single polynomial of degree 5 whose Galois group is S_5.

Consider $f(x) = x^5 - x - 1 \in \mathbb{Q}[x]$. One can verify (by computing its Galois group directly, using reduction modulo primes and the discriminant) that $\mathrm{Gal}(f) \cong S_5$.

Now, S_5 is not solvable: its derived series is

$$S_5 \supset A_5 \supset A_5 \supset \cdots$$

which never reaches $\{e\}$, because A_5 is simple and non-abelian (it has no non-trivial normal subgroups). By Galois's theorem, f is not solvable by radicals.

Since a *general* formula would in particular apply to this f, no general formula can exist. □

Important contrast with lower degrees.

Degree	Galois group (generic)	Solvable?
2	$\mathbb{Z}/2\mathbb{Z}$	Yes — quadratic formula
3	S_3	Yes — Cardano's formula
4	S_4	Yes — Ferrari's method
5	S_5	**No**
$n \geq 5$	S_n	**No**

The solvability of S_3 and S_4 is what makes the classical formulas work. The jump to S_5 breaks solvability because A_5 is simple — there is no further normal subgroup to quotient by, and the derived series cannot terminate.

10 Conclusion: The Full Picture

We close by placing both results in their common framework.

Two impossibility results, one theory.

Question	**Criterion**	**Tool**
Is α constructible?	$[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2	Tower law
Is f solvable by radicals?	$\mathrm{Gal}(f)$ is a solvable group	Fundamental theorem

The logical chain that makes everything work is:

$$\text{Symmetries of roots} \longrightarrow \text{Galois group} \longrightarrow \text{Subgroup structure} \longrightarrow \text{Solvability}$$

Galois theory answers not just the general question ("is there a formula for degree n?") but the specific question ("can *this* polynomial be solved by radicals?"): compute the Galois group of the given polynomial and check whether it is solvable. The abstract machinery of groups, fields, and extensions is not decoration — it is the precise instrument that converts a question about arithmetic into a question about symmetry, and symmetry into a question with a definitive answer.