Galois Theory for Rats: TL;DR Version

Skyler Hu

February 4, 2026

Contents

1 Fields and Extensions

This handout assumes basic knowledge on groups, rings and fields, i.e. types of such algebraic structures, their properties and how they operate. Knowledge on polynomials over a field, irreducibility, ideals, roots of unity and the characteristic of a field would also be helpful.

Note. It is often helpful to view isomorphic fields, groups, etc. as a single group or field, since they are algebraically equivalent by the definition of an isomorphism. For example, if a is in a field isomorphic to F, then it is conventional to say that $a \in F$.

A field is a set that has the four defined operations similar to the rationals $\mathbb{Q}$. In other words, a field is a commutative group under addition, a group under multiplication and the two operations satisfy the distributive law. Forming fields from base fields give us *field extensions*:

Definition 1.1. (Field Extension.) If K is a field containing a subfield F, then call K a *field extension* of F, denoted K/F.

Field extensions are commonly expressed using the notation $F(a_1, a_2, \ldots, a_n)$, where $\{a_1, a_2, \ldots, a_n\}$ are the elements adjoined (added) to F to obtain a new field. An extension is defined to be *simple* if it is generated by a single element α over F.

There are two important theorems concerning field extensions and roots of polynomials, which are the primary objects of study in Galois Theory:

Theorem 1.1. Let $p(x) \in F[x]$ be an irreducible polynomial over F. Then there exists a field extension K/F containing a root of $p(x)$. If α is this root of $p(x)$ in $K = F(\alpha)$, then $F(\alpha) \cong F[x]/(p(x))$, the polynomials over F quotiented by the ideal generated by $p(x)$.

Theorem 1.2. (Roots of $p(x)$ are algebraically equivalent.) Let $p(x) \in F[x]$ be an irreducible polynomial over F. If $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ are the roots of $p(x)$, then $F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_n)$ are all isomorphic, i.e. the roots of $p(x)$ are algebraically equivalent when adjoined to F.

Theorem 1.2 follows naturally from Theorem 1.1, since $F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_n)$ are all isomorphic to $F[x]/(p(x))$. Theorem 1.2 also gives us that if one root of $p(x)$ is in a field extension of F, then all roots of $p(x)$ are in this field extension of F, an important idea we'll come back to when discussing splitting fields.

The *degree* of a field extension K/F, denoted $[K : F]$, is defined as the dimension of K as a vector space over F, i.e. the size of the basis for K over F. An important result concerning the degree of field extensions is the Tower Law:

Theorem 1.3. (Tower Law.) Let K be a field extension over L and L be a field extension over F. Then

$$[K : F] = [K : L][L : F].$$

2 Algebraic, Solvable, Composite Extensions

Galois Theory is primarily concerned with the roots of polynomials, so it follows to define a specific property as being a root of a polynomial over a field. This is given by the definition of algebraic extensions:

Definition 2.1. (Algebraic Extensions.) An element $\alpha \in K$ over F is said to be *algebraic* if it is a root of a nonzero polynomial $p(x) \in F[x]$. Otherwise, the element is said to be *transcendental* over F. An extension K/F is algebraic if every element $\alpha \in K$ is algebraic over F.

Algebraic extensions have a few important properties:

1. An extension of an algebraic element over F is a finite extension, i.e. $F(\alpha)/F$ has finite degree if α is algebraic over F.

2. If α is algebraic over F, there exists a unique monic irreducible polynomial over F, $m(x)$, having *alpha* as a root. This polynomial is called the *minimal polynomial* of α over F.

Another way of forming new fields from given fields is the *composition* of fields, its definition given below:

Definition 2.2. (Composite Fields.) Given two subfields K_1, K_2 of K, the *composite field* K_1K_2 is the smallest subfield of K that contains both K_1 and K_2.

In Galois Theory, the type of fields most often discussed is the *splitting field*, a field extension containing all the roots of a polynomial. More specifically:

Definition 2.3. (Splitting Field.) For any field F, if $f(x) \in F[x]$ then there exists a unique field extension K/F such that $f(x)$ splits completely into linear factors over K and doesn't split completely into linear factors for any smaller $F_0 \subset K$. This field extension K is defined as the *splitting field* of $f(x)$ over F, and it has at most degree $n!$ for $f(x)$ of degree n.

The following definition, originating from multiplicity of roots in elementary algebra, is also widely used:

Definition 2.4. (Separable Polynomials & Extensions.) A polynomial $f(x) \in F[x]$ is said to be *separable* if it has no multiple roots. Otherwise, $f(x)$ is *inseparable.*
A field extension K/F is said to be *separable* if every element in K is a root of some separable polynomial over F.

3 Fundamental Theorem of Galois Theory

In this section we explore the Fundamental Theorem of Galois Theory (FTGT), which describes in detail the relation of field extensions and groups concerning polynomials.

Definition 3.1. (Automorphism.) An autormorphism σ of field K is an isomorphism from the field to itself. The collection of automorphisms is denoted $Aut(K)$. If $\alpha \in K$ and $sigma \in Aut(K)$, we can write $sigma(\alpha)$ as $\sigma\alpha$ to denote the mapping of α to another element of k.

An automorphism $\sigma \in Aut(K)$ *fixes* an element $\alpha \in K$ if $\sigma\alpha = \alpha$. If $F \subset K$, then *sigma* is said to *fix* F if it fixes every element of F. The collection of such automorphisms is denoted $Aut(K/F)$.

Some things named after Galois:

Definition 3.2. (Galois Extensions & Galois Group of Extension.) A field extension K/F is said to be *Galois* if $\mid Aut(K/F) \mid = [K : F]$. If K/F is Galois, the automorphism group $Aut(K/F)$ is the *Galois group* of K/F, denoted $Gal(K/F)$.

Definition 3.3. (Galois Group of Polynomial.) If $f(x)$ is a separable polynomial over F, then the *Galois group* of $f(x)$ over F is the group of automorphisms of the splittign field of $f(x)$ over F.

Such ideas are central to the Fundamental Theorem of Galois Theory:

Theorem 3.1. (Fundamental Theorem of Galois Theory.) Let K/F be a Galois extension and set $G = GalK/F$. Then there is a bijection:

$$\{K - E_1 - E_2 - \ldots - E_k - F \text{ (subfields } E \text{ of } K \text{ containing } F)\}$$

$$\mid$$

$$\{1 - H_1 - H_2 - \ldots - H_k - F \text{ (subgroups } H \text{ of } G)\}$$

given by

$$E_k \to \{\text{elements of } G \text{ fixing } E\}$$

and

$$\{\text{fixed field of } H_k\} \leftarrow H.$$

Under this correspondence:

1. This correspondence is inclusion-reversing, i.e if $E_1 \to H_1, E_2 \to H_2$, then $E_1 \subseteq E_2 \Leftrightarrow H_2 \leq H_1$.
2. $[K : E_k] = H_k$ and $[E_k : F] =\mid G : H_k \mid$

3. K/E_k, the intermediate fields over F, is always Galois, with $Gal(K/E_k) = H_k$.

4. E_k/F is Galois if and only if $H_k \leq G$ is a normal subgroup.

5. If E_1, E_2 correspond to H_1, H_2, then $E_1 \bigcap E_2$ corresponds to $\rangle H_1, H_2 \langle$ and the composite field E_1E_2 corresponds to $H_1 \bigcap H_2$.

Intuitiively, when we consider F the base field and K the splitting field of a separable polynomial $f(x)$ over F, this theorem derives a bijection between the subfields of the splitting field and the subgroups of the Galois groups of $f(x)$. This allows us to identify attributes of field extensions with properties of groups, e.g. normality and solvability. We'll see how these come into play in the proceeding content.

Theorem 3.2. (Galois groups & Symmetric groups.) There exists an injective homomorphism

$$Gal(K/F) \hookrightarrow S_n$$

from the Galois group of the splitting field K of $deg(f_x) = n$ over F into the symmetric group (permutation group) of order n. In particular, if this homomorphism is an isomorphism, then $f(x)$ is called the *general polynomial* of degree n.

4 Solvability

In this section we look at solvability. There are a few key algebraic tools for connecting fields and groups to solvability; but first, we must define what is a solvable polynomial.

Definition 4.1. (Solvability by Radicals.) An element α which is algebraic over F can be *expressed by radicals* or *solved for in terms of radicals* if α is an element of a field K which can be constructed from F through a series of extensions of the form $F_i(\sqrt[n_i]{a_i})$, where $a_i \in F_i$.

Some key algebraic definitions for the fine details of the proofs:

Definition 4.2. (Discriminant of Polynomial.) The *discriminant* D of $x_1, x_2, \ldots, x_n$ is given by

$$D = \prod_{i<j} (x_i - x_j)^2.$$

The discriminant of a polynomials is defined to be the discriminant of its roots.

Definition 4.3. (Lagrange Resolvent.) Let K be any cyclic extension of degree n over F of characteristic not dividing F. F contains the nth roots of unity. Let σ be a generator for cyclic $Gal(K/F)$.
For $\alpha \in K$ and any nth root of unity ζ, define the *Lagrange Resolvent* (α, ζ) by

$$(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha).$$

Definition 4.4. (Elementary Symmetric Functions.) For $x_1, x_2, \ldots, x_n$, the *elementary symmetric functions* $s_1, s_2, \ldots, s_n$ are defined by

$$\begin{aligned} s_1 &= x_1 + x_2 + \ldots + x_n, \\ s_2 &= x_1x_2 + x_1x_3 + \ldots + x_2x_3 + \ldots + x_{n-1}x_n, \\ &\ldots \\ s_n &= x_1x_2 \ldots x_n. \end{aligned}$$

These definitions, as well as manipulation with field theory, prove the general solvability theorem, which is often considered the core of Galois Theory:

Theorem 4.1. (Solvability Criteria.) The polynomial $f(x)$ can be solved by radicals if and only if its Galois group is a solvable group.

Lemma 4.1. (Symmetric Groups & Solvable Groups.) The symmetric group S_n is not solvable (i.e. has no proper normal subgroups) for $n > 5$.

Which arrives at the final theorem:

Corollary 4.1. (Insolvability of Quintic & Above) The general polynomial of degree greater than 5 is not solvable by radicals.