Galois Theory for Rats

Skyler Hu

September 28, 2025

Contents

0 Before we Start

0.1 Galois Theory for Rats: Definition

This is intended to be a handout for people interested in Galois Theory. It is not, in any way, meant to be a full, concise course on Galois Theory. Rather, I have tried to introduce topics and ideas in a way understandable to people new to abstract algebra.

The handout assumes basic knowledge on groups, rings and fields: readers should at least know the definition of groups, rings and fields, know some common small groups, and have some intuition on how they operate. To give an idea of this level of proficiency, a dedicated math nerd should be able to achieve the level within 1-2 months of studying algebra.

0.2 Motivation

As you may know, Galois theory is considered one of the most beautiful branches of mathematics (or at least of algebra). It addresses the longstanding, fundamental problem of solvability by radicals – why the general equation of fifth degree is not solvable by radicals, and sheds light on many hidden aspects of polynomials and roots. In addition, Galois theory is applicable to various subjects of algebra, including group theory, topology and algebraic number theory.

The story behind Galois theory is also one of legend and tragedy. It's a well known anecdote among math people that Évariste Galois, the young genius behind Galois theory, died under mysterious circumstances in a duel at the age of 20. During his lifetime, he was a revolutionary mathematician, a literal revolutionary (he was an avid Republican during the French Revolution), and an ardent, impassioned soul. Studying Galois theory might give us some insight into his short, brilliant life and mathematics.

I first encountered Galois theory in SUMaC 2025. I had been reading on mathematical history prior to the camp, and the idea of solvability through algebraic methods, as well as Galois' life, was fascinating. During this fantastic month I gained a basic understanding of Galois theory, as well as an overwhelming number of inside math jokes concerning it, and this has motivated me to share this theory, as well as the experience of learning something new, with the math community.

0.3 Structure

The structure of this handout is laid out as follows:

First, we provide a statement and outline of the solvability criterion, and address key insights or building blocks to solving the problem. We proceed to build the required theory up from the definition of a field to the solvability of polynomials of different degrees. Some asides that are not critical to proving the final theorem but are interesting to explore nonetheless (e.g. a field-theoretic proof of the Fundamental Theorem of Algebra) are included.

A short justification of why I'm doing this: the path from basic field extensions all the way up to the insolvability of equations of degree 5 or higher is extremely long, winding and sometimes counterintuitive. Starting with all the prerequisites and working up to the final theorem might be tedious or demoralizing (source: how I worked through Galois Theory). For someone with intuition on algebraic objects, starting with the theorem statement and building towards the proof may feel more logical and satisfying.

In order to make this handout more short and concise (and less disgusting to read through), some proofs have been removed and deferred to the Proofs for Goats handout alongside this one. The proofs that remain are either 1) central or 2) fun to work through.

0.4 Acknowledgements

I would like to give thanks to all the brilliant rats I met. Also bro, gang and chief, Wilbur watermelon, and whoever supplies SUMaC with all the snacks every day.

In addition: my family, friends, coffee, Buldak ramen(or Korean food in general), Dumbit and Foole, and my favorite video games.

1 The Big Theorem

1.1 Who Was Évariste Galois?

The appeal of Galois Theory to most learners began from the legend of his life: according to anecdotes told by various textbooks and professors, Galois during his lifetime was a genius and embittered revolutionary, who jotted down his research results the night before the duel that took his life. In order to do justice to the tales as well as the math, I'm including the short form of the full story that got me fascinated by Galois Theory here.

At a glance, Évariste Galois was a mercurial character as well as a mathematical genius. Tragic was his life story, it should be noted that most of his misfortunes were inflicted by himself. The memoirs he submitted for review containing his ingenious work were lost (interestingly, by other reputed mathematicians of the time including Cauchy and Fourier), and as retaliation he railed against the "established order" of the French academic scene. He devoted much time to presenting himself as the tragic genius we know today, embracing his public image by setting himself on a pyre.

Aside from a failed scholar (at least during his lifetime), Galois was also a failed revolutionary. An ardent Republican, he was imprisoned once for publicly issuing death threats to the king of France, again for inciting unrest on Bastille day. It seems that to him, the world was cut cleanly into the right and the wrong, and he would die before crossing his principles for avoiding self-destruction. It also seems that he considers himself always in the right.

Common sense dictates that a soul burning with such passion would not burn for long. In May 1832, he was challenged to a duel under mysterious circumstances. The eve of the duel he wrote a long letter to his friend Auguste Chevalier, summarizing (although not explaining in detail like in the myth surrounding him) his research findings and praying that someone would come along and decode this mess. He died the next day, scarcely 21 years old, brave and confident till the end.

The point of the story is not to dissuade mathematicians from fighting in duels. (Although if you're a mathematician reading this, please don't fight in duels.) By catching a glimpse into Galois's life held to the highest of High Romanticism, we might get an idea of the origin of the beautiful Galois Theory, the mind behind it, and the vibrant era of academia that cast it.

1.2 Core of Galois Theory Explained

As mentioned in the introduction, we start by stating the central theorem to the solvability problem:

Theorem 1.1 ((Solvability Criteria.)). The polynomial $f(x)$ can be solved by radicals if and only if its Galois group is a solvable group.

The core intuition of Galois Theory is linking polynomials to fields. In order to prove the solvability criterion, we may start with a graph depicting the connection between groups (solvable groups as stated in Theorem 1.1) and fields (representing polynomials):

We fill in the boxes with a step-by-step approach. Representing polynomials using fields and their properties are established in Sections /*insert section number here*/, characterizing field extensions and their relationship to polynomials. In Section /* insert section number here*/ we begin introducing Galois groups, filling the group side of Galois Theory. Section /*insert section number here*/ proves the Fundamental Theorem of Galois Theory, the essential link between groups and fields. The last sections /*insert section number here*/ provides the cornerstone of our proof, building from elements depicted in Figure 1.1 to the final proof of solvability criteria.

The broader idea behind the group theory, field theory and connection part:

1. The **group theory** side uses primarily the idea of *Galois groups*, groups that are formed from permuting roots of polynomials. The polynomial is solvable if and only if the chain of Galois groups (constructed in a specific manner, as we will see in Sections /*insert section number here*/) are solvable in each step (we will shortly define the notion of a *solvable group*).

2. The **field theory** side requires the definition of *splitting field extensions*, which are formed by adjoining roots of polynomials to a base field comprising the coefficients of the polynomial. In short, the splitting field of a polynomial is the smallest field extension that contains all the roots of polynomial $f(x)$, and we shall see that they can be constructed in a way symmetric to solvable Galois groups.

3. The correlation between groups and fields formed from the polynomial relies on the Fundamental Theorem of Galois Theory, stating that there exists a bijection between towers of field extensions and corresponding groups formed by permuting elements of the field (field automorphisms). Such a correspondence is called a *Galois Correspondence*, and forms the cornerstone of many proofs building up to solvability criteria. It also gives some intuition on why we formed groups and fields out of polynomials.

2 Basic Theory of Field Extensions

2.1 Field and Characteristics

We begin by refreshing our memory of the definition of a field.

Definition 2.1. (Field.) A field satisfies the following field axioms:

1. Elements of a field form an abelian (commutative) group under addition (or any operation resembling addition);
2. Elements of a field form a group under multiplication (or any operation resembling multiplication);
3. Addition and multiplication satisfy the distributive law.

Examples of fields include the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, and the cyclic groups of prime order (e.g. F_2, F_5). See if you can prove that these examples are fields. (When we prove something is a field, we can simply check all the field axioms.)

An important attribute of a field is its *characteristic*. Before defining the characteristic, we introduce a claim that makes the definition more intuitive:

Proposition 2.1. There exists a homomorphism $\phi : \mathbb{Z} \mapsto F$ for any field F defined as

$$\phi(m) = m \cdot 1_F, m \in F.$$

Proof. $\phi(mn) = (mn) \cdot 1_F = (m \cdot 1_F)(n \cdot 1_F) = \phi(m)\phi(n)$. □

Definition 2.2. (Characteristic of Field.) The *characteristic* of a field F, denoted $ch(F)$, is the smallest positive integer p such that

$$p \cdot 1_F = 0_F, \text{where multiplication is defined as } 1_F^p \text{ under addition.}$$

if such p exists. $ch(F)$ is defined to be 0 otherwise.

We can see that the characteristic of a field resembles 0 in some sense. Note that $ch(F)$ is defined as an integer rather than a field element: the field element corresponding to $ch(F)$ would be 0_F to ensure that F has no zero divisors.

There are only a few options for the characteristic of a field:

Proposition 2.2. The characteristic of a field is either 0 or a prime p.

Proof. It's easy to list some fields with characteristic 0: $\mathbb{Q}$ and $\mathbb{R}$ are two such fields. We only need to prove that fields with characteristics other than 0 can only have prime characteristics. *Proof by Contradiction.* By the definition have a field, if m, n are positive integers, we have

$$m \cdot 1_F + n \cdot 1_F = (m + n) \cdot 1_F \text{ and } (m \cdot 1_F)(n \cdot 1_F) = (mn) \cdot 1_F.$$

Now suppose that $ch(F) = n$ is composite. Then $n = ab$ for $a, b \neq 1$, so since $n \cdot 1_F = 0_F$:

$$(ab) \cdot 1_F = (a \cdot 1_F)(b \cdot 1_F) = 0_F.$$

So either $a \cdot 1_F$ or $b \cdot 1_F = 0_F$, so there exists an integer smaller than n satisfying characteristic conditions, contradicting the minimality of characteristics. Therefore $ch(F) = n$ must be a prime if not 0. □

Note how Proposition 4.1 clarifies the definition of a characteristic: the proposition defines a map from an integer multiple of 1_F to a field element, which corresponds to mapping $p \cdot 1_F$ to 0_F in the definition of $ch(F)$.

2.2 Field Extensions and Roots

2.2.1 Introduction

Field theory and Galois theory are primarily concerned about forming new fields from known fields, otherwise known as field extensions. In group theory, you may have studied the effect of addiing an element to a group, which often requires the addition of many further elements in order for the result to also be a group. A field extension is similar: new fields are formed from a base field by adjoining 1 or more elements to the base field. Field extensions, combined with the roots of polynomials, have some interesting results and applications. By studying field extensions, we not only make significant progress towards our goal of solvability, but also gain a new perspective on previously known structures, such as the rationals $\mathbb{Q}$, square roots of integers and the complex numbers $\mathbb{C}$.

2.2.2 Field Extension: Definition and Examples

Definition 2.3. (Field Extension.) If K is a field containing a subfield F, then call K a *field extension* of F, denoted K/F.

An important attribute of the field extension is its degree, in other words, the dimension of field extension K over its base field F:

Definition 2.4. (Degree of Field Extension.)
The degree of field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F. In other words, if the set $S = \{a_1, a_2, \cdots, a_n\}$ form a basis for K over F (i.e. a_i are linearly independent and every element in K can be written as a linear combination of a_i, then $[K : F] =\mid S \mid .$)

Note. There is a common notation used for representing field extensions: if F is the base field of the extension, then $F(\alpha)$ denotes the field extension obtained by adjoining (adding) element α to F.
We can denote field extensions adjoining multiple elements similarly: let F be a base field. Then $F(a_1, a_2, \cdots, a_n)$ denotes the field extension obtained by adjoining $\{a_1, a_2, \cdots, a_n\}$ to F.

Example 2.1. (Common Field Extensions.)

1. $[F : F] = 1$ for any field F. The basis of F over F is $\{1_F\}$.
2. The field extension $\mathbb{Q}(\sqrt{2})$ over the rationals $\mathbb{Q}$ has degree 2. Since $\mathbb{Q}(\sqrt{2})$ comprises real numbers of the form $a + b\sqrt{2}, a, b \in \mathbb{Q}$, the basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is $\{1, \sqrt{2}\}$.
3. Consider the field extension $\mathbb{Q}(\sqrt[3]{2})$ obtained by adjoining $\sqrt[3]{2}$ to the rationals. It has degree 3 over the rationals: the basis of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is $\{1, \sqrt[3]{2}\}, \sqrt[3]{4}$.

4. At first glance, $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$ might not be that obvious. We ensure that all possible products and quotients of $\sqrt{2}, \sqrt[3]{2}$ are represented: the basis is

$$\sqrt[6]{2}, (\sqrt[6]{2})^2 = \sqrt[3]{2}, (\sqrt[6]{2})^3 = \sqrt{2}, (\sqrt[6]{2})^4 = \sqrt[3]{4}, (\sqrt[6]{2})^5 = \sqrt[6]{32}, 1.$$

i.e. $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.

2.2.3 Root Extensions & Quotient Fields

The primary object of study in Galois Theory is field extensions formed by roots of polynomials, i.e. $F(\alpha)$ for α a root of $p(x) \in F[x]$. There is an important theorem that we can derive:

Definition 2.5. (Simple Extensions.) An extension K/F is simple if it can be obtained by adjoining a single element, i.e. $K = F(\alpha)$ for some α.

Note that simple extensions might not look simple at first glance: Consider *Example* 2.1.4.

Theorem 2.1. (Simple Extension Isomorphism.) Let $p(x)$ be an irreducible polynomial over F, and *alpha* be a root of $p(x)$. Then

$$F(\alpha) \cong F[x]/(p(x)),$$

i.e. the field extension formed by adjoining α to F is isomorphic to $F[x]$ quotiented by the ideal generated by $p(x)$.

This is used to derive the following:

Theorem 2.2. (Roots of $p(x)$ are algebraically equivalent.) Let α, β be roots of $p(x)$ as defined above. There exists an isomorphism:

$$\phi : F(\alpha) \xrightarrow{\sim} F(\beta)$$

that fixes F and maps α to β. In other words, roots of $p(x)$ are algebraically equivalent in a field-theoretic view.

The significance of Theorem 2.2 is that when we describe root extensions, we no longer need to specify a root. If a root of $p(x)$ is in K/F, then all of the roots are in K/F, so we only consider a "general" root of $p(x)$, in some sense.

2.3 Degrees, Algebraic Extensions, and the Tower Law

2.3.1 Algebraic Extensions and Properties

Now that we have a basic understanding of field extensions (what they are, how are they formed, field extensions with roots), we can start looking at how field extensions are classified. A basic (and relatively broad) way to classify field extensions is through the definition of *algebraic extensions*:

Definition 2.6. (Algebraic Extension.) 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.

In the last section, we have reduced "Roots of $p(x)$" to "a root of $p(x)$" using Theorem 2.2. With algebraic extension, we can reduce this expression further:

Definition 2.7. (Minimal Polynomial.) 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. When α is a root of $p(x)$, then we can say $m(x)$ is the minimal polynomial of $p(x)$ over $f(x)$.

The minimal polynomial often serves as a reduced version of our choice of $p(x)$, as seen in the following simplification of Theorem 2.1:

Theorem 2.3. (Simple Extension Isomorphism, but with Minimal Polynomial) Let $p(x)$ be an irreducible polynomial over F, and *alpha* be a root of $p(x)$. Let $m(x)$ be the minimal polynomial of $p(x)$ over F. Then

$$F(\alpha) \cong F[x]/(m(x)).$$

Example 2.2. (Minimal Polynomial.) The minimal polynomial of an element α often shares a degree with the field extension of α, as illustrate in the following examples:

1. The minimal polynomial for $\sqrt{2}$ over *mathbbQ* is $x^2 - 2$, which has degree 2. The extension