Galois Theory for Rats - Field Extensions

Skyler Hu

February 7, 2026

Contents

1 Motivation: Galois Theory for Rats

Galois Theory, the study of fields, polynomials and solvability (if my limited understanding could be allowed to ascribe these topics to this theory), is a profoundly beautiful and revealing topic in modern algebra. In addition to impressing other math people who have not yet heard of it (my primary motivation), learning Galois Theory has the benefits of sating a mathematical appetite for symmetry and formalizing what feels intuitive, opening doors to possibilities in more advanced math and introducing stories on the history of mathematics. As such, this handout is intended to serve as an intuitive guide (rather than a completely rigorous/theoretical one) to Galois theory and field theory in general, allowing the reader to enjoy discovery without need for too much formal work.

That being said, a basic knowledge on groups, rings and fields is assumed, all that could be learned within the time of a month or two. Prior experience on polynomials over a field, irreducibility, ideals, roots of unity and the characteristic of a field would also be helpful.

Due to my incapability of formal research and literature review experience, the handout is largely based on Dummit & Foote's Abstract Algebra, 3rd edition.

Rats are small, fascinating creatures with a love for food, company and (stereotypically) cheese. Should a rat develop the motivation to study Galois Theory, it is fully welcome to consult this handout.

2 Fields and their Extensions: Introduction

We begin with the definition of a *field*, a set with the four defined operations similar to the rationals $\mathbb{Q}$. In other words, a field is a commutative (abelian) 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 2.1. (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 $F(a_1, a_2, \dots, a_n)$, where $\{a_1, a_2, \dots, a_n\}$ 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.

It is often helpful to think of fields as similar to the rationals $\mathbb{Q}$: there exists the operations 'addition' and 'multiplication' (with the exception that 'multiplication' is not necessarily commutative in a field, think: vector or matrix multiplication). With polynomials, the core object of study in Galois theory, in mind, we can also consider polynomials over a field in a similar way to polynomials with rational coefficients, i.e. polynomials over $\mathbb{Q}$.

Definition 2.2. (Polynomials over a field.) If polynomial $f(x)$ is over a field F, then $f(x)$ has all coefficients in F.

Casual conclusion that will be used a lot:

Theorem 2.1. (Polynomials over a field form a field.) The polynomials $f(x)$ over field F form a field, typically denoted by $F[x]$. Can you prove this?

Example 2.1. Some examples of field extensions and their motivations:

1. Consider the field of rationals $\mathbb{Q}$. (Can you show that the rationals form a field?) Adjoining the imaginary unit i to $\mathbb{Q}$ gives us $\mathbb{Q}(i)$, the set of complex numbers of the form $a + bi$ with $a, b \in \mathbb{Q}$. You can show that $\mathbb{Q}(i)$ is a field by considering $(a + bi) \pm (c + di)$, $(a + bi)(c + di)$ and $\frac{a+bi}{c+di}$.

2. Similarly, show that $\mathbb{Q}(\sqrt{2})$ is a field. The idea of field extensions is more widely found than generally thought, considering this is an example readers would typically have done in Algebra 2.

3. $\mathbb{R}(i) = \mathbb{C}$.

3 Degrees of Extensions and the Tower Law

The most commonly used parameter of describing field extensions is the *degree* of field extensions, which characterizes the 'dimensions' of K relative to subfield F:

Definition 3.1. (Degree of a Field Extension.) 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.

A good way of thinking about degrees of field extensions is borrowing the idea of basis from linear algebra (in fact, abstract algebra and linear algebra are related more closely that you might think!): the degree of extension K/F is the *minimum number of distinct elements* $\{a_0, a_1, a_2, \ldots, a_n\}$ required to express all elements in K as a linear combination of elements in F, with coefficients $\{a_0, a_1, a_2, \ldots, a_n\}$:

$$k \in K,\ k = a_0m_0 + a_1m_1 + \ldots + a_nm_n \text{ where } m_0,\ m_1,\ \ldots m_n \in F.$$

For example, consider the extension $\mathbb{Q}(\sqrt{2})$, the set of number of the form $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. 2 elements, 1 and $\sqrt{2}$, are used in expressing elements from $\mathbb{Q}(\sqrt{2})$ as a linear combination of elements in $\mathbb{Q}$ (a and b), so the degree of the extension $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

The following result is integral to the study of field extensions and will be used a lot in later arguments. It's also very neat-looking and the proof is fun to walk through!

Theorem 3.1. (Tower Law.) Let K be a field extension over L and L be a field extension over F. Then

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

The Tower Law is very intuitive with a basic understanding of how vector spaces work. A proof of the Tower Law is included in the Proofs section. (Hint: manipulate the basis.)

Example 3.1. (Using the Tower Law.) What happens when we adjoin $\sqrt[3]{2}$ to $\mathbb{Q}(\sqrt{2})$? We showed previously that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and we can show similarly that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (consider elements of the form $a+b\sqrt[3]{2}+c\sqrt[3]{4}$.) By the Tower Law, this implies $[\mathbb{Q}(\sqrt{2},\, \sqrt[3]{2}) : \mathbb{Q}] = 6$. Considering elements of the form

$$a_0 + a_1 \cdot \sqrt{2} + a_2 \cdot \sqrt[3]{2} + a_3 \cdot \sqrt[3]{4} + a_4 \cdot 2^{\frac{5}{6}} + a_5 \cdot 2^{\frac{5}{3}},$$

we see that this is true.

4 Fields and Polynomials : Some Fundamental Results

In this section we use a few sample theorems to illustrate the relationship between fields and polynomials, with a (possibiliy inaccurate) explanation of their significance in building our logic. We start with one that may seem trivial:

Theorem 4.1. (Field extension containing root exists.) 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 field of polynomials over F quotiented by the ideal generated by $p(x)$.

Note. A polynomial $p(x) \in F[x]$ is irreducible when $p(x)$ has no roots in F.
A Brief Note on $F[x]/(p(x))$. The concepts of polynomial rings quotiented by ideals generated by a polynomial is more common in ring theory, but right now it's safe to say that $F[x]/(p(x))$ is precisely the field of 'remainder' polynomials when $f(x) \in F[x]$ is divided by $p(x)$. e.g. Over the field $\mathbb{F}_2$ (the integers modulo 2), $\mathbb{F}_2/(x^2 + 1)$ is

$$\{0,\, 1,\, x,\, x + 1\}.$$

There are some more detailed arguments here. We haven't explicitly shown that $F[x]/(p(x))$ is a field, and precisely what is an ideal and how do we use it is a big part of ring theory, specficially a structure called *Euclidean domains*, but right now rest assured that I've done the hard math for you and this is all you need to know.

Example 4.1. We can illustrate with an example on why **Theorem 4.1** is true. Again, consider the polynomial $p(x) = x^2 + 1 \in \mathbb{F}_2[x]$. $p(x)$ has roots $\pm i$, so the field extension containing the roots of $p(x)$ is given by $\mathbb{F}_2(i)$, which is

$$\{0,\, 1,\, i,\, 1+i\},$$

with isomorphism to $\mathbb{F}_2[x]/(p(x)) = \{0,\, 1,\, x,\, x+1\}$ given by $i \mapsto x$. The complete proof of **Theorem 4.1**, including the proof of the trivial(?) statement that a field extension containing a root exists, is given in the Proofs section.

Theorem 4.1 allows us to gain a basic understanding of what field extensions with roots are like, an important idea in Galois theory. Also it's always good to have something isomorphic to something else (see: the entirety of Representation Theory), so keep this theorem in mind. Note how we haven't explicitly stated the root adjoined to F, and the reason is the following statement:

Corollary 4.1. (Roots fo $p(x)$ are algebraically equivalent.) Let $p(x) \in F[x]$ be an irreducible polynomial over F. If $\{\alpha_1,\, \alpha_2,\, \dots,\, \alpha_n\}$ are the roots of $p(x)$, then $F(\alpha_1),\, F(\alpha_2),\, \dots,\, F(\alpha_n)$ are all isomorphic, i.e. the roots of $p(x)$ are algebraically equivalent when adjoined to F.

Proof. This follows naturally from **Theorem 4.1**, since $F(\alpha_1),\, F(\alpha_2),\, \dots,\, F(\alpha_n)$ are all isomorphic to $F[x]/(p(x))$. The rigorous proof involves some manipulation of ideals and is included in the Proofs section. □

Corollary 4.1 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. In a way, this simplifies a myriad of arguments when working with roots: instead of considering roots of a polynomial, we only need to think of *a root*, singular, cutting down 50% of proof complexity.

Also an unexpected application of this corollary is the *Fundamental Theorem of Algebra.* Readers may or may not be familiar with the analysis proof of FTA, but not many are aware that an algebraic proof exists, is a lot more fun than the analysis proof (at least as per the author, you are welcome to argue) and lies at the heart of Galois Theory. A key argument in the algebraic proof of the FTA stems from **Corollay 4.1**, stating that if a polynomial has a complex root, then it has all its roots in the complex number field $\mathbb{C}$. There is a separate handout in this series on the algebraic proof of FTA.

5 Proofs

It's encouraged, with this handout as well as with other mathematical material, to work through the proofs on your own before reading the full solution. Though that's not how the author initially learned it, so feel free to consult this section upon first read. Be warned, however: unlike the body of the handout, each handout's Proofs section is not written with the intention to be lenient on your thinking machine.

5.1 Theorem 3.1: Tower Law

Proof. (Theorem 3.1: Tower Law) *Theorem Statement.* Let K be a field extension over L and L be a field extension over F. Then $[K : F] = [K : L][L : F]$.
The proof is divided into two cases: whether or not the field extension is finite.
Case 1: Finite Extensions. Suppose that $[L : K] = m$ and $[K : F] = n$ are finite.
Let α_1, α_2, …, α_m be a basis of L over K and let β_1, β_2, …, β_n be a basis of K over F. Then every element of L can be written as

$$a_1\alpha_1 + a_2\alpha_2 + \ldots + a_m\alpha_m \text{ where } a_i \in K.$$

Therefore $a_i = b_{i1}\beta_1 + b_{i2}\beta_2 + \ldots + b_{in}\beta_n$, $i = 1, 2, \ldots, m$, $b_{ij} \in F$. Substituting in a_i gives us the general form of elements in L:

$$\sum_{1\leq i\leq m,\, 1\leq j\leq n} b_{ij}\alpha_i\beta_j \in L.$$

Therefore the mn elements of the form $\alpha_i\beta_j$ (with coefficient in F) span L as a vector space over F. In order to show that $[L : F] = mn$, we only need to show that there is no *smaller* span of L over F, i.e. elements of the form $\alpha_i\beta_j$ are linearly independent.
Since α_1, …, α_m for a basis of L over K, they are linearly independent, so

$$\sum_{1\leq i\leq m,\, 1\leq j\leq n} b_{ij}\alpha_i\beta_j = 0$$

if and only if the coefficients $b_{ij}\beta_j$ are all 0. Equivalently, β_1, …, β_n form a basis of K over F, so the sum is only 0 when all coefficients $b_{ij}\alpha_i$ are all 0. Therefore the only solution to

$$\sum_{1\leq i\leq m,\, 1\leq j\leq n} b_{ij}\alpha_i = 0$$

is $b_{ij} = 0$ for all possible i, j, so $\alpha_i\beta_j$ are linearly independent, and form a basis of L over F. Therefore $[L : F] = [L : K][K : F]$, as claimed. □

Summary. We show that for α_i, thebasis of K over F, and for β_j, the basis of L over K, all possible products $\alpha_i\beta_j$ form a basis of L over F. To do this, we first showed that $\alpha_i\beta_j$ spans L over F, then show that this span is minimal (i.e. a basis).

5.2 Theorem 4.1.1: Field extension containing root exists

Proof. (Theorem 4.1.1: Field extension containing root exists.) *Theorem Statement.* 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 field of polynomials over F quotiented by the ideal generated by $p(x)$.

We can directly find this field extension K/F and prove that it contains a root of $p(x)$. Consider $K = F[x]/(p(x))$. Since $p(x)$ is irreducible, K is a field (i.e. K satisfies the multiplicative inverse law). In order to show that K is in fact a field extension of F, we need to show that K contains an isomorphic copy of F. To do this, we consider the map series:

$$F \hookrightarrow F[x] \to F[x]/(p(x)) = K.$$

This is an *injective ring homomorphism*, showing that K does contain an isomorphic copy of F. We can the show that K contains a root of $p(x)$:

Let φ denote the isomorphism $F \mapsto F' \subset K = F[x]/(p(x))$. Then $p(\varphi(x)) = \varphi(p(x)) = p(x) \pmod{p}(x) = 0$ by definition of $F[x]/(p(x))$, so $p(x)$ has a root in K. □

Proof. (Theorem 4.1.2: $F(a) \cong F[x]/(p(x))$.) Consider the map $\varphi : F[x]/(p(x)) \to F(a)$ with

$$\varphi(c_0 + c_1x + c_2x^2 + \ldots + c_nx^n) \to c_0 + c_1a + \ldots + c_na^n,$$

where $c_0, c_1, \ldots, c_n \in F$. We can show that φ is a bijective homomorphism:
1. φ is a homomorphism. Simply note that

$$\varphi(f_1(x)f_2(x)) = f_1(a)f_2(a) = \varphi(f_1(x))\varphi(f_2(x)).$$

1. φ is a bijection. Both $F[x]/(p(x))$ and $F(a)$ are fields, and φ is not the 0 map, so it is necessarily injective. All elements in $F(a)$ can be written in the form $c_0 + c_1a + \ldots + c_na^n$ where $n = [F(a) : F]$, so φ is also surjective. Therefore the proposed φ is an isomorphism: $F(a) \to F[x]/(p(x))$. □

5.3 Corollary 4.1: Roots of $p(x)$ are algebraically equivalent

Proof. (Corollary 4.1: Roots of $p(x)$ are algebraically equivalent.) *Theorem Statement.* 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 $F(\alpha_1)$, $F(\alpha_2)$, $\dots$, $F(\alpha_n)$ are all isomorphic, i.e. the roots of $p(x)$ are algebraically equivalent when adjoined to F.

Let $\varphi : F \to F'$ be a field isomorphism. Define $p(x) \in F[x]$ as previously given, and let the polynomial obtained by applying φ to the coefficients of $p(x)$ be $p'(x) \in F'[x]$. Let α be a root of $p(x)$ in an extension of F and let β be a root of $p'(x)$ in an extension F'. Then there exists an isomorphism $\sigma : F(\alpha) \to F'(\beta)$ that maps α to β and fixes φ.

There exists a natural isomorphism $F[x] \cong F'[x]$ obtained by applying φ to all the coefficients of polynomials in $F[x]$. Since this isomorphism maps the maximal ideal $(p(x))$ to $(p'(x))$, $(p'(x))$ is also the maximal ideal, and $p'(x)$ is irreducible over $F'[x]$.

We can therefore take the quotients of the maximal ideals:

$$F[x]/(p(x)) \to F'[x]/(p'(x)).$$

Now $F[x]/(p(x) \cong F(\alpha))$ and $F'[x]/(p'(x)) \cong F(\beta)$, so $F(\alpha) \cong F(\beta)$. □