

Galois Theory for Rats - Field Representation

Skyler Hu

February 11, 2026

Contents

1	Introduction & Motivation	3
2	Prerequisites & Definitions	3
3	Proof	5
4	Proofs	6
4.1	Derivatives...in field theory?	6
4.2	Theorem 2.2: Freshman's Dream	7
4.3	Proposition 2.1: Irreducibility & Separability	7

1 Introduction & Motivation

In this handout on *Field Representation*, we will introduce and prove a single result: there exists exactly 1 field of order p^n for any prime p and any positive integer n .

There are some reasons to why this result is important. First, it's simplicity: readers familiar with group theory will know that one of the most (and arguably *the* most) important topics when working with groups is *Representation Theory*, describing the types of groups of given order. Representation Theory is still an active area of research today, and its core project – the classification of all finite simple groups – is recognized as one of the most prodigious and monumental efforts in modern mathematics. However, the mirror idea when it comes to fields – classifying all the fields – takes the length of this handout and a lunch break.

The insight this comparison provides is profound. In comparing different algebraic structures, fields has only 5 (6?) more structural constraints than groups, but these couple additional axioms scale down the difficulty of the same question by an unimaginable extent. In general, it's safe to consider that the simplicity of a task increases with more constraints (contrary to intuition): a linear equation with two variables has infinite solutions, but two linear equations with two variables only have one (or occasionally zero); there are hundreds of thousands of people named Skyler, but there is only one Skyler who wrote this handout.

This handout includes some prerequisites to prove the theorem and the proof, as well as some other interesting field theory tidbits not extremely relevant to our holy grail (solvability). Intuitive guidance on some of the harder to understand parts is also included.

2 Prerequisites & Definitions

Aside from the theorems of field extensions in the first handout: Fields and Extensions, there exists a number of different properties of fields, many concerning polynomial properties. Some of them are essential to proving the theorem:

Theorem 2.1. (Field Representation.) There exists a unique field of order p^n for any prime p and positive integer n .

We begin with the defintion of *separability*. Although this terminology is new, readers should have encountered this idea in high school algebra: separability describes whether or not a polynomial has multiple roots.

Definition 2.1. (Separable Polynomials.) A polynomial over F is *separable* if it has no multiple roots (i.e. all roots are distinct). Otherwise, a polynomial is *inseparable*.

In determining whether or not a polynomial is separable, we can make use of the following rule. This will come in useful in proving **Theorem 2.1**, and the proof is included in the Proofs section.

Proposition 2.1. (When is a Polynomial Separable?) Every irreducible polynomial over a finite field F is separable. A polynomial $f(x) \in F[x]$ is separable if and only if it is a product of distinct irreducible polynomials in $F[x]$.

Proposition 2.1 connects irreducibility (existence of factors) to separability (existence of multiple roots). Meanwhile to help us better understand fields of finite characteristic, we introduce another important component of the proof, which is a delightful notion one might have entertained since they first learned factoring in middle school.

Theorem 2.2. (Freshman's Dream) Let F be a field of characteristic p . Then for $a, b \in F$,

$$(a + b)^p = a^p + b^p, (ab)^p = a^p b^p.$$

The proof of Freshman's Dream is in the Proofs section. It is remarkably easy and uses another elementary result (the Binomial Theorem), so try to prove it on your own!

A Word on Characteristics. An intuitive idea of the characteristic of a field is what represents ‘zero’ in a field; for example, F_5 , the field of integers modulo 5, has characteristic 5, which corresponds to treating 5 and its multiples as ‘zero’ when working mod 5. For infinite fields such as \mathbb{Q} and \mathbb{R} , there doesn’t exist another element other than the number 0 that is ‘zero’ in this sense, so the characteristic for these fields is defined to be infinite.

3 Proof

Theorem 3.1. There exists a field of order p^n for all prime p and positive integer n . This field is unique up to isomorphism.

Proof. **1. Existence:** We use a constructive argument to obtain a field of order p^n .

Let $n > 0$ be any integer and consider $x^{p^n} - x \in F_p[x]$, where F_p is a field of characteristic p . Since $x^{p^n} = x(x^{p^n-1} - 1)$ and $x, x^{p^n-1} - 1$ are both irreducible over F_p , $x^{p^n} - x$ is separable by **Proposition 2.1**. Therefore $x^{p^n} - x$ has p^n distinct roots.

Consider the splitting field of $x^{p^n} - x$ over $F_p[x]$. Let α, β be roots of $x^{p^n} - x$. Then $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$, and

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta, \quad \alpha^{p^n-2} = \alpha^{-1} \text{ and } (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta, \quad (\text{Freshman's Dream})$$

so the set F containing all the roots of $x^{p^n} - x$ is closed under addition, multiplication and inverse, and F is a field. Since F is a subfield of the splitting field of $x^{p^n} - x$, F is the splitting field by the minimality of the splitting field.

Since $|F| = p^n$, there exists finite fields of order p^n for any prime p and integer n . We can obtain a field of order p^n by finding the splitting field of the polynomial $x^{p^n} - x$ over F_p .

In addition, since $[F : F_p] = n$, there exists finite fields of degree n over F_p for any $n > 0$.

2. Uniqueness: Let F be a field of characteristic p . If $[F : F_p] = n$ where F_p is the prime subfield of F , then $|F| = p^n$. Since the multiplicative group F^\times has order $p^n - 1$ (excluding the additive identity 0), $\alpha^{p^n-1} = 1$ for any $\alpha \in F^\times$, giving $\alpha^{p^n} = \alpha$. Then α is an element in the splitting field of $x^{p^n} - x$ over F_p , which has precisely order p^n . Then F is a splitting field of $x^{p^n} - x$, and is unique up to isomorphism by the properties of splitting fields.

(Note: if you didn't see it, the argument for uniqueness essentially reverse-engineers the argument for existence, which is a very common method when proving uniqueness.)

Conclusion. There exists a unique field of order p^n for prime p and positive integer n . Wasn't that satisfying? □

4 Proofs

Note: every statement in this handout is closely interconnected with a bunch of others, so this section gives the full view from defining separability to proving relevant theorems. As such, you're free to skip some parts if you only want an intuitive understanding, but reading the Proofs section top to bottom may help you appreciate the structure of fields and polynomials. Also, it is always better to read a proof than skip it (given you're not an engineering student).

We start with the definition of the *derivative* over a field, which is similar to the definition of a derivative in calculus:

Definition 4.1. (Derivative of Polynomial.) The derivative of the polynomial $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in F[x]$ is

$$D_x f(x) = a_n nx^{n-1} + a_{n-1}(n-1)x^{n-2} + \dots + 2a_2x + a_1 \in F[x].$$

The derivative rules we learned in calculus (addition & subtraction, chain rule) also applies. Can you prove this?

Derivatives could be used to indicate separability in polynomials:

4.1 Derivatives... in field theory?

Proposition 4.1. (Separability & Derivatives) A polynomial $f(x)$ is separable if and only if it has no common factors with its derivative other than 1, i.e. $f(x)$ is coprime with $D_x f(x)$.

Proof. ‘If’: We prove the contrapositive: If $f(x)$ and $D_x f(x)$ has a common root α , then $f(x)$ is not separable.

Write $f(x) = (x - \alpha)h(x)$. Take the derivative using the chain rule:

$$D_x f(x) = (x - \alpha)D_x h(x) + h(x).$$

Since $(x - \alpha)$ is a factor of $D_x f(x)$, $(x - \alpha)$ is a factor of $h(x)$, and the root α has at least multiplicity 2 in $f(x)$, making it inseparable.

‘Only If’: We also prove the contrapositive: if $f(x)$ has a multiple root (i.e. inseparable), then $f(x)$ and $D_x f(x)$ have a common factor.

Suppose α is a multiple root of $f(x)$. Over a splitting field of $f(x)$, $f(x) = (x - \alpha)^n g(x)$ for some $n \geq 2$ and $g(x)$. Taking the derivative of $f(x)$ gives us

$$D_x f(x) = n(x - \alpha)^{n-1}g(x) + (x - \alpha)^n D_x g(x)$$

which has $(x - \alpha)$ as a factor. □

Note: it helps to think of this in terms of differentiation. We know that if a polynomial $f(x)$ has a multiple root x_0 , then the graph of $f(x)$ does not cross the x-axis at $x = x_0$, making x_0 a critical point (or stationary point, depending on which curriculum you took in high school). Then $f'(x_0) = 0$, so the derivative of f also has x_0 as a root. Field theory and calculus/analysis have more intersections than you might think (see: algebraic proof of FTA) since the complex numbers \mathbb{C} form a field (we'll see this later).

4.2 Theorem 2.2: Freshman's Dream

You might've heard about this name in a number theory class. Then again, number theory essentially studies \mathbb{Z}_n , so some parts of this handout may seem particularly familiar.

Proof. **1. Additive:** $(a + b)^p = a^p + b^p$. Expand with the Binomial Theorem:

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \dots + \binom{p}{p-1} a b^{p-1} + b^p.$$

All of $\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$ are multiples of p , so they are identical to 0 in F with characteristic p . Therefore $(a + b)^p = a^p + b^p$.

2. Multiplicative: $(ab)^p = a^p b^p$. This follows naturally from the field axiom that multiplication is commutative. \square

Note on Freshman's Dream. The etymology behind this theorem is unclear, though it could be attributed to a sinister little poem *Dark and Bloody Ground* published in 1938. There also exists a *Sophomore's Dream* theorem in calculus, which, unlike its more junior counterpart, always holds.

4.3 Proposition 2.1: Irreducibility & Separability

Theorem Statement. Every irreducible polynomial over a finite field F is separable. A polynomial in $F[x]$ is separable if and only if it is a product of distinct irreducible polynomials in $F[x]$.

We first realize some important results: first, every element in F with characteristic p is a p th power in F .

Definition 4.2. (Frobenius Endomorphism.) The map $\varphi : F \Rightarrow F$ for F of characteristic p defined by

$$\varphi(a) = a^p$$

is an injective homomorphism. This homomorphism is called the Frobenius Endomorphism of F .

Note. To see that the Frobenius Endomorphism is a homomorphism, consider Freshman's Dream. An *endomorphism* is defined as a homomorphism of an object onto itself. If this homomorphism is an isomorphism, then it is an *automorphism*, which we will see quite a lot later on in Galois theory. There is also the notion of a *morphism* (no prefixes) in algebraic geometry, but you do not need to worry about that yet.

The Frobenius Endomorphism shows us that every element in F is also a p th power in F (since the endomorphism obtained by taking the p th power maps the field to itself).

Proof. The first statement is proven by contradiction. Suppose $p(x) \in F[x]$ is an inseparable irreducible polynomial. Then by **Proposition 4.1**, $p(x) = q(x^p)$ for some $q(x) \in F[x]$. Let

$$q(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0.$$

Then

$$p(x) = a_m x^{pm} + a_{m-1} x^{p(m-1)} + \dots + a_1 x^p + a_0.$$

By **Definition 4.1**, each coefficient a_0, \dots, a_m is a power of p in F . Let $a_i = b_i^p$. Then

$$\begin{aligned} p(x) &= (b_m x^m)^p + (b_{m-1} x^{m-1})^p + \dots + (b_1 x)^p + b_0^p \\ &= (b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0)^p, \quad \text{Freshman's Dream} \end{aligned}$$

contradicting the irreducibility of $p(x)$. Therefore $p(x)$ is separable, and every irreducible polynomial over F is separable in F .

The second statement follows directly from the first. Think about it! □