Galois Theory for Rats - Field Representation

Skyler Hu

February 7, 2026

Contents

1 Introduction & Motivation **3**

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.

2 Proof

Theorem 2.1. 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:** Let $n > 0$ be any integer and consider $x^{p^n} - x \in F_p[x]$. This polynomial is separable (it is equal to $x(x^{p^n-1}) - 1$) and therefore has p^n distinct roots.
Consider the splitting field of $x^{p^n} - x$ over $F_p[x]$. Let α, β be roots of $x^{p^n} - x$. Since $\alpha^{p^n} = \alpha$, $\beta_{p^n} = \beta$,

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta,\ \alpha^{p^n} = \alpha^{-1} \text{ and } (\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta,$$

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.
Since $\mid F \mid = p^n$, 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 $\mid F \mid = p^n$. Since the multiplicative group $F^\times$ has order $p^n - 1$,

$\alpha^{p^n-1} = 1$ 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.

Conclusion. There exists a unique field of order p^n for prime p and positive integer n. □