An Exploration of Finite field

Xuanang Chen
Based on GRM example class by Mr James Dougal

March 2021

Abstract

What is the possible order of a finite field? Do they all exist? Does irreducibles over $\mathbb{F}_p$ of a given degree exists? How can we count the number of them? We will prove that a finite field must have order p^k for some prime p, and there exists such fields for all p and all non-negative integer k.

1 Introduction

Q1: When must an abelian be cyclic?
A1: When the order is square-free.
Q2: How to determine a ring of order n with characteristic n?
A2: Low Tech: The expansion of $(1+1+...)(1+1+...)$ determines the multiplication; High Tech: Consider the ring homomorphism from Z to R which is a surjection. $R \cong \mathbb{Z}/n\mathbb{Z}$
Note that if the order n of a ring is square-free, then the additive abelian group must be cyclic, hence characteristic is n, hence must be isomorphic to $\mathbb{Z}/n\mathbb{Z}$.
Recall the construction of a field of order 4: $\mathbb{F}_2[X] \big/ (X^2+X+1)$. As X^2+X+1 is an irreducible, (X^2+X+1) is a maximal ideal, hence quotient is a field with $2^2 = 4$ elements.
Our plan: Find some irreducible of degree $d \pmod{p}$, so we can build a finite field with p^d elements. The following sections will show that such an irreducible exists, and will find a nice formula for the number of such fields.

2 Why

Why are we only looking for fields with p^n elements?

Lemma 1. *Let F be a finite field. Then $char(F) = p$, where p is a prime.*

Proof. $char(F)$ is finite since F is finite. If it is composite, then F is not an Integral Domain, but since F is a finite field it must be an I.D., contradiction. □

Definition 1. *A field extension is a pair of fields $K \leq L$, where K is a subring of L. We write this as L/K. We can view L as an vector space over K. The degree of L/K, written as $[L/K]$, is the degree of L as a $K-vector\ space$.*

Note: We require K to be a field rather than a ring because, a vector space must be over a field (so that the property of vector space could work).

Corollary 1. *Any finite field has p^n elements, where p is its characteristic.*

Proof. We can view a finite field F as a vector space over F_p, where p is the characteristic of F, F_p is a copy of F consisting of $\{1, 1+1, ...\}$. Then F has p^n elements for $n = [F/F_p]$ □

This answers the question at the start of this section.

Example 1. *Suppose R is an I.D. with a subring F which is a field s.t. $dim_F R < \infty$. Then R must also be a field.*

Proof. Let $n = dim_F R$. For any $r \in R/\{0\}$, $\exists c_i \in F$ s.t. $\sum_0^n c_i r^i = 0$ and c_i not all zero. If $C_0 \neq 0$, then $r(c_1 + c_2 r + ... + c_n r^{n-1})(-c_0)^{-1} = 1$. So r has an inverse. If $c_0 = 0$, since R is an I.D. and $r/ne0$, $c_1 + c_2 r + ... + c_n r^{n-1} = 0$. Repeat we are done. □

Lemma 2. *Let R be an Integral Domain with a subgring F which is a field. We can view R as an $F-$vector space as λr makes sense and satisfies the asioms. Assume R is a finite-dimensional $F-$vector space, then R must be a field.*

Proof. (c.f. to the proof that a finite I.D. must be a field) Choose $\alpha \in R/\{0\}$, consider the homomorphism

$$\begin{aligned} \phi : R &\to R \\ r &\to \alpha r \end{aligned}$$

ϕ is clearly a linear map. ϕ is injective as R is an I.D.. By rank-nullity theorem, ϕ must be surjective as well. Thus R must be a field as there's an inverse to each non-zero element. □

3 If and Only If

Clearly if f is irreducible over $\mathbb{F}_p$ of degree n, then we get a field of order p^n, i.e. $\mathbb{F}_p/(f)$. Is the converse true?

Lemma 3. *If F is a finite field, then the group $F^\times$ (under multiplication) must be cyclic.*

Proof. Since F is a field, $X^n - 1$ has no larger than n roots.
By classification of finite abelian groups, the multiplication group $G \cong C_{n_1} \times ... \times C_{n_k}$. If there's a repeated factor $C_m \times C_m$, then there are m^2 solutions to $X^m - 1$, which is a contradiction. Hence G is cyclic. □

Proposition 1. *A field of order p^n exists if and only if a degree n irreducible polynomial exists over $\mathbb{F}_p$.*

Proof. ($\Rightarrow$) We have $\mathbb{F}_p/F$. By lemma 3, we can choose $\beta \in F$ s.t. all powers of β cover $F^\times$. Consider

$$\begin{aligned} \psi : \mathbb{F}_p[X] &\to F \\ f(X) &\to f(\beta) \end{aligned}$$

It is clearly a surjective homomorphism. Moreover, $ker(\psi) = (f)$ for the minimal polynomial f. Thus $\mathbb{F}_p[X]/(f) \cong F$ is a field. So (f) is maximal hence f is irreducible. Since $p^{deg(f)} = |F| = p^n$, we know that f has degree n.
($\Leftarrow$) Trivial. $\mathbb{F}_p/(f)$. □

This answers the question at the start of this section.

4 The Theorem that Kills It

Consider the equation $X^{p^n} - X$. This polynomial has no repeated roots since it exactly covers all roots—if we assume a field with p^n elements exists. But of course we cannot assume this condition. How can we proceed?

Lemma 4. *f is a polynomial with a repeated root r if and only if $f(r) = f'(r) = 0$.*

Proof. ($\Rightarrow$)It's trivial if we write $f(x) = (x-r)^2 h(x)$.
($\Leftarrow$) Also trivial. □

Now note that $X^{p^n} - X$ has derivative -1 over $\mathbb{F}_p$. So it has no double roots.
It's time for our big theorem to show up.

Theorem 1. *Given a field F and a polynomial $f(X) \in F[X]$, there exists a larger field (field extension) where f has all its roots.*

Note: the smallest such field is called the splitting field. Indeed, one can further show that the splitting field is unique up to isomorphism. This is not included in this article, and to show this, you'd better take a course in Galois Theory.

Proof. Set $L = F$.
1. If a root α of f is in L, replace f by $f/(x - \alpha)$
2. Let g be an irreducible factor of f. Replace L by $L[X]/g$. Turn to step 1.
Now step 2 ensures step 1 can proceed, and when the degree of f decreases to zero we get a splitting field. □

It looks good— we can prove what we want now.

Theorem 2. *The finite field of order p^k exists, for all prime p and all non-negative integer k.*

Proof. This is a direct corollary of the previous theorem. By Theorem 1, there exists a field K where $X^{p^n} - X$ has all its roots over $\mathbb{F}_p$. Let $F = \{\beta : \beta^{p^n} - \beta = 0\}$. Then F is a field with p^n elements. □

Thus we also have the irreducible polynomial over $\mathbb{F}_p$ exists for any degree.
Hooray!

5 Counting

How can we count the number of irreducible polynomials in $\mathbb{F}_p[X]$ of given degree?

Lemma 5. *$F_{p^d} \leq F_{p^n}$ if and only if $d|n$, where we write F_{p^n} to be a field of p^n elements.*

Proof. Note that $X^{p^d} - X | X^{p^n} - X$ if and only if $d|n$, and the elements in F_{p^n} are precisely the roots of $X^{p^n} - X$. □

It might sound a bit confusing, but we have:

Proposition 2. *f is a (monic degree one) irreducible factor of $X^{p^n} - X$ over F_{p^n} if and only if f is a monic irreducible polynomial whose degree divides n over F_p.*

Proof. ($\Leftarrow$) If f is an irreducible factor of $X^{p^n} - X$ over F_{p^n}, its splitting field $\mathbb{F}_p[X]/(f)$ is contained in F_{p^n}. (Consider this in the construction of splitting field). So $d|n$.
($\Rightarrow$) If f is a monic irreducible polynomial whose degree divides n over F_p, then the splitting field of f must be contained in F_{p^n} by lemma 5. The result follows. □

Thus we have:

Corollary 2. *$X^{p^n} - X$ is the product of all irreducibles of degree d s.t. $d|n$. i.e.*

$$X^{p^n} - X = \prod_{d|n,\ f \text{ monic irreducible of degree } d} f$$

Write C_d for the number of monic irreducibles of degree d over $\mathbb{F}_p$. We have

$$p^n = deg(X^{p^n} - X) = deg(\prod_{d|n} f) = \sum_{d|n} dC_d$$

We can solve this by using Mobius Inversion Formula, given that lower degree C_d is derived.

Example 2. *Calculate C_d for $d = 2$ over $\mathbb{F}_2$:*
List all quadratics mod p: $X^2 + bX + C$. Write down all $(X - r)(X - s)$, eleminates from the list.