Finite Field

Yuting Fang

MATH 4581 AU 20

Instructor: Jim Cogdell

Abstract

Finite fields, also called Galois fields, are fields that contains finite number of elements. Study of finite field is essential for further study on Galois Theory, polynomial, and other topics in algebra. Finite fields also appear in many applications, including coding theory and cryptography. This document gives an introduction, including related algebraic background, important structures, and major properties. An example of how finite field ideas are applied in coding theory is presented in the end.

1. Algebraic Background

Many algebraic concepts are employed heavily in study of finite fields. Here I give a survey of critical concepts that will be used in the project.

1.1 Extension Field

A field $\boldsymbol{E}$ is an ***extension field*** of a field $\boldsymbol{F}$ if $\boldsymbol{F}$ is a **subfield** of E. The field F is called the ***base field***. Denoted by $\boldsymbol{F} \subset \boldsymbol{E}$.

$\boldsymbol{E}$ is a vector space over $\boldsymbol{F}$ of dimension $\boldsymbol{n}$, then $\boldsymbol{E}$ is a ***finite extension*** of degree $\boldsymbol{n}$ over $\boldsymbol{F}$. Indicated by $[\boldsymbol{E} : \boldsymbol{F}] = \boldsymbol{n}$.

If $\boldsymbol{F} \subset \boldsymbol{E}$ and $\boldsymbol{E} \subset \boldsymbol{K}$, then $\boldsymbol{F} \subset \boldsymbol{K}$ and $[\boldsymbol{K} : \boldsymbol{F}] = [\boldsymbol{K} : \boldsymbol{E}][\boldsymbol{E} : \boldsymbol{F}]$.

1.2 Ring Homomorphism

If R and S are rings, then a ring ***homomorphism*** is a map $\Phi: R \to S$ satisfying $\Phi(a + b) = \Phi(a) + \Phi(b)$, $\Phi(ab) = \Phi(a)\Phi(b)$, for all $a, b \in R$.

If Φ is a one-to-one and onto homomorphism, then it is an ***isomorphism*** of rings.

1.3 Splitting Field

Let $\boldsymbol{F}$ be a field and $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a non-constant polynomial in $F[x]$. An extension field $\boldsymbol{E}$ of $\boldsymbol{F}$ is a ***splitting field*** of p(x) if there exist elements $\alpha_1, \ldots, \alpha_n$ in $\boldsymbol{E}$ such that $E = F(\alpha_1, \ldots, \alpha_n)$ and $p(x) = a_n(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$.

Existence & Uniqueness: Let $p(x) \in \boldsymbol{F}[x]$ be a non-constant polynomial, then there exist a splitting field $\boldsymbol{E}$ for *p(x)*. Given two splitting fields *K* and *L* of $p(x)$, there exists an isomorphism $\Phi: K \to L$ that keeps elements in $\boldsymbol{F}$ fixed and maps roots of $p(x)$ in *K* into roots in *L*.

1.4 Algebraic Element

An element $\boldsymbol{\alpha}$ in an extension field $\boldsymbol{E}$ over $\boldsymbol{F}$ is ***algebraic*** over F, if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in \boldsymbol{F}$[x].

$\boldsymbol{E}$ is an ***algebraic extension*** of $\boldsymbol{F}$ if every element in $\boldsymbol{E}$ is algebraic over $\boldsymbol{F}$.

$\boldsymbol{E}$ is a ***simple extension*** of $\boldsymbol{F}$ if $\boldsymbol{E} = \boldsymbol{F}(\alpha)$ for some $\alpha \in \boldsymbol{E}$.

Theorem (21.13): Let $\boldsymbol{E} = \boldsymbol{F}(\alpha)$ be a simple extension of $\boldsymbol{F}$, where $\boldsymbol{\alpha} \in \boldsymbol{E}$ is algebraic over $\boldsymbol{F}$. Suppose that the degree of $\boldsymbol{\alpha}$ over F is $\boldsymbol{n}$. Then every element $\boldsymbol{\beta} \in$ E can be expressed uniquely in the form $\beta = b_0 + b_1 a + \cdots + b_{n-1}\alpha^{n-1}$.

Theorem (21.15): Every finite extension field $\boldsymbol{E}$ of a field $\boldsymbol{F}$ is an algebraic extension.

1.5 Characteristic of Field

A field $\boldsymbol{F}$ has characteristic $\boldsymbol{p}$ if $\boldsymbol{p}$ is the smallest positive integer such that for every nonzero element $\boldsymbol{\alpha}$ in $\boldsymbol{F}$, $\boldsymbol{p\alpha} = 0$. If no such integer exists, then F has characteristic 0.

Theorem (16.19): The characteristic of an integral domain is either prime or 0.

Furthermore, a finite field (ex: $\mathbb{Z}/p$) has prime characteristic, but an infinite field has either has 0 (ex: $\mathbb{Q}$) or prime characteristic (ex: field of rational functions over F_p).

2. Definition and Basic Structure

The field of integers modulo a prime number may be the first finite field we study. Many of its properties can be extended to arbitrary finite fields. Why "finite" elements and prime characteristic make these fields special will be the focus.

Definition: ***Finite field*** is a field that contains a finite number of elements.

Recall the ***field*** is a set F with two operations, addition (+) and multiplication (·), satisfying:

1) (F, +) is an abelian group with identity element 0.
2) (F\{0}, ·) is an abelian group with identity element 1.
3) For all $a \in F$, $0 \cdot a = a \cdot 0 = 0$
4) Distributivity combines (+) and (·).

A finite field of order $\boldsymbol{q}$ is denoted by $\boldsymbol{F_q}$ or ***GF(q).***

Finite field is also called Galois field (*GF*), named after Évariste Galois (French, 1811–1832), who begin the general study of finite field theory.

With fact that every finite fields have prime characteristic; we can first study the order of finite fields and establish its relation with characteristic.

Proposition 2.1 [Order to Characteristic] Let $\boldsymbol{p}$ be ***characteristic*** of a finite field $\boldsymbol{F}$ with $\boldsymbol{n}$ elements, then $\boldsymbol{p}$ is a prime dividing $\boldsymbol{n}$.

Proposition 2.2 [Characteristic to Order] If $\boldsymbol{F}$ is a finite field of characteristic $\boldsymbol{p}$, then the order of $\boldsymbol{F}$ is $\boldsymbol{p^n}$ for some $\boldsymbol{n} \in \mathbb{N}$.

In 2.1, since *n* is order and *p* is characteristic, then $n\alpha = p\alpha = 0$ for α in F. Also $p \leq n$. Thus, $\boldsymbol{p}$ must divide $\boldsymbol{n}$. In 2.2, to get the order, we consider how many different elements $\boldsymbol{F}$ can have. With homomorphism $\boldsymbol{\varphi}$: $\mathbb{Z} \to \boldsymbol{F}$, $\varphi(n) = n \cdot 1$, we can build a field $\varphi(\mathbb{Z})$, over which $\boldsymbol{F}$ is an algebraic extension. Then elements in $\boldsymbol{F}$ $a = a_1\alpha_1 + \cdots + a_n\alpha_n$, where $a_i \in \varphi(\mathbb{Z})$. There are p^n possible linear combinations of the α_i's, and then p^n distinct elements in $\boldsymbol{F}$.

These propositions reveal an important structure of finite fields: **every finite field is of prime-power order**.

Further we can study subfields of a finite field and structure of the lattice.

Theorem 2.3 [Subfield Criterion]: Let $\boldsymbol{F}$ be a finite field of order p^n. Then every subfield of subfield of $\boldsymbol{F}$ has order p^m, where *m* is a positive divisor of *n*. Conversely, if *m* is a positive divisor of *n*, then there exists exactly one subfield of $\boldsymbol{F}$ with p^m elements.

A subfield $\boldsymbol{E}$ of $\boldsymbol{F}$ must be a field extension of the prime field $\boldsymbol{K}$, which is isomorphic to $\mathbb{Z}_p$.

Then [F : K] = [F : E][E : K], *m* divides *n*. The existence and uniqueness of the finite field will be presented in next section.

From this criterion, we can determine subfields of the finite field $\boldsymbol{F_{p^n}}$ by **listing all divisors of $\boldsymbol{n}$**.

The containment relation can also be determined by divisibility relations among divisors.

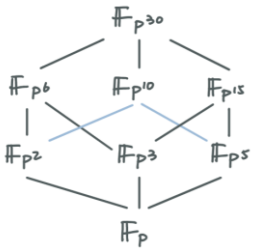

Figure: Lattice of Subfields of $F_{p^{30}}$

3. Existence and Uniqueness

Exploring from characteristic and order of finite fields, we can show existence and uniqueness of finite fields. Every finite field is of prime-power order. Conversely, for every prime power there exists a finite field whose order is the number. Furthermore, finite fields with same order are isomorphic, and then can be identified.

To prove the existence, we will apply concept and criterion of separable extension:
Definition: A polynomial $f(x) \in F[x]$ of degree *n* is ***separable*** if it has ***n*** distinct roots in the splitting field of $f(x)$. An extension ***E*** of ***F*** is a ***separable extension*** of ***F*** if every element in ***E*** is the root of a separable polynomial in $F[x]$.
Lemma 2.5 [Separability Criterion] Let F be a field and $f(x) \in F[x]$. Then $f(x)$ is separable if and only if $\boldsymbol{f(x)}$ and its derivative $\boldsymbol{f'(x)}$ are relatively prime.

[Existence] For every prime p, positive integer n, there exists a finite field ***F*** with p^n elements.

The basic idea behind is to consider ***F*** as the ***splitting field*** of $f(x)$, where $f(x) = \boldsymbol{x^{p^n} - x}$.
First, $f(x)$ is separable and has p^n distinct zeros in ***F***, by taking derivative and separability criterion. Further, ***F*** is formed by these p^n distinct zeros of $f(x)$, because $f(x)$ splits in ***F*** and roots of $f(x)$ form a subfield of ***F***.
This process also provides a method for constructing finite fields.

[Uniqueness] Any field of order p^n is isomorphic to the splitting field of $\boldsymbol{x^{p^n}}-x$ over $\mathbb{Z}_p$.

Following the idea of existence, field of order p^n can be considered as the splitting field of $f(x) = x^{p^n} - x$. Then the uniqueness of finite field is a direct consequence of uniqueness of splitting field.
With uniqueness of finite field, it is justified to say ***the*** finite field or ***the*** Galois field of order ***q***.

4. Important Property

Recall: **Fundamental Theorem of Finite Abelian Groups**
Every finite abelian group G is isomorphic to a direct product of cyclic groups of the form $\mathbb{Z}_{p_1^{\alpha_1}} \times ... \times \mathbb{Z}_{p_n^{\alpha_n}}$, where the p_i's are primes.

From the Fundamental Theorem of Finite Abelian Groups, we can get another important property about the multiplicative group of nonzero elements of a finite field:

Theorem (22.10): Let ***F*** be any finite field. If ***G*** is a finite subgroup of ***F****, the multiplicative group of nonzero elements of ***F***, then ***G*** is ***cyclic***.
The idea behind is that, the ***least common multiple*** of $p_1^{e_1},\ldots,p_k^{e_k}$ is the order of ***G***, where $p_1, \ldots, p_k$ are primes such that $n = p_1^{e_1}\ldots p_k^{e_k}$, $G \cong \mathbb{Z}_{p_1^{e_1}} \times ... \times \mathbb{Z}_{p_k^{e_k}}$. Then G must contain elements of order ***n***.

Definition: Let ***F*** be any finite field. A generator of cyclic group ***F**** is a ***primitive element*** of ***F.***
The existence of primitive elements is further used to show that, every finite field can be thought as a simple algebraic extension of its prime subfield.

Considering prime characteristic, a useful property of commutative rings is the following:
Lemma 2.3 [Prime Characteristic Equation] Let p be prime and D be an integral domain of characteristic p. Then for all positive integers n, $a^{p^n} + b^{p^n} = (a + b)^{p^n}$.

At first look is equation is unreasonable. According to binomial formula: $(a + b)^p = \sum_{k=0}^{p} \binom{P}{k} a^k b^{p-k}$**.** But since ***p*** is a prime and also the characteristic, $\binom{P}{k}$ must be divisible by ***p*** for $0 < \boldsymbol{k} < p$, and then all terms of $0 < \boldsymbol{k} < p$ are zero.
This lemma plays an important role in study of irreducible polynomials related to finite fields.

Theorem 2.4 If ***f*** is an irreducible polynomial in $\boldsymbol{F_p}[\boldsymbol{x}]$ of degree *m*, then ***f*** has a root $\boldsymbol{\alpha}$ in $\boldsymbol{F_{p^m}}$.
All the roots of ***f*** are simple and are given by the *m* distinct of $\alpha, \alpha^p, \ \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}$ of $\boldsymbol{F_{p^m}}$**.**
Corollary 2.5 Let ***f*** be an irreducible polynomial in $\boldsymbol{F_p}[\boldsymbol{x}]$ of degree *m*, then the splitting field of ***f*** over $\boldsymbol{F_p}$ is given by $\boldsymbol{F_{p^m}}$.

The idea behind 2.4 is that $\boldsymbol{\alpha}$ is a root of ***f*** in splitting field of ***f*** over $\boldsymbol{F_p}$, then $\left[\boldsymbol{F_p}(\boldsymbol{\alpha}): \boldsymbol{F_p}\right] = \boldsymbol{m}$**.**
We can get $\boldsymbol{F_p}(\boldsymbol{\alpha}) = \boldsymbol{F_{p^m}}$. Also, if β in $\boldsymbol{F_{p^m}}$ is a root of ***f***, then β^p is also a root of ***f***.
With this theorem we can find further relation 2.5 between $\boldsymbol{F_p}$ and $\boldsymbol{F_{p^m}}$ with the connection of irreducible polynomial, which provides a method for finite fields constructing. This also leads to **interpretations of finite fields as splitting fields of irreducible polynomials**. Furthermore, we can conclude that **every map from a finite field to itself can be expressed as a polynomial**.

5. Application

Finite fields are fundamental concepts for many applications of algebra, including number theory, cryptography, and coding theory. I am particularly interested in its application in **coding theory**.

Coding Theory

Coding theory, applied in areas of communications, aims to provide codes that can transmit information tolerating a small probability of **error**. The two main part to coding theory is ***error-detecting*** and ***error-correcting*** codes. Applying ***redundancy bits*** to realize these functions, we also want we use as less as redundancy bits as possible.

For an (n, k)- block code, there is a one-to-one ***encoding*** function $E: \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ and a ***decoding*** function $D: \mathbb{Z}_2^n \to \mathbb{Z}_2^k$. The code is error-correcting if *D* is onto.

Basic Mechanism of Polynomial Codes

Finite fields operations provide approaches to construct codes algebraically based on polynomials over finite fields. Following is one example:

Any binary *n*-tuple $(a_0, a_1, \dots, a_{n-1})$ can be interpreted as a polynomial in $\mathbb{Z}_2[x]$, corresponds to the polynomial $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$. Conversely, with any polynomial $f(x) \in \mathbb{Z}_2[x]$, with deg $f(x) < n$ we can associate a binary *n*-tuple.

Let $p(x)$ be a fixed nonconstant polynomial in $\mathbb{Z}_2[x]$ of degree $n - k$. $(a_0, a_1, \dots, a_{k-1})$ is a k-tuple to be encoded. We can get the corresponding polynomial $f(x)$. To encode $f(x)$, multiply it by $p(x)$. Then there is an (n, k)- code *C*. The codewords in C will be polynomials in $\mathbb{Z}_2[x]$ of degree less than *n* that are divisible by $p(x)$. In this way, we can generate polynomial codes.

6. Conclusion

Finite field is involved in many different threads of algebra development. In both theory and application, study of finite field is essential to development of modern algebra. This document gives an introduction on Finite Field, including related algebraic background, important structures, lattice of subfields, existence & uniqueness, as well as several major properties including its cyclic multiplicative of nonzero elements, and interpretations as splitting fields of irreducible polynomials. In the end, there is a brief description about how finite field ideas are applied in coding theory and polynomial codes. There are still many interesting perspectives waiting to be explored.

Reference

Abstract Algebra Theory and Applications (2020), Thomas W. Judson, http://abstract.ups.edu/index.html.