Finite Fields

Keng-Yu Chen

June 9, 2025

We show the classification of finite fields and how the operations of them work.

1 Classification

We here show that all finite fields of the same size are isomorphic to the splitting field for the polynomial $X^{p^n} - X$ over $\mathbb{Z}_p$ for some prime p and natural number n.

Lemma 1. *Every finite field has a prime subfield, generated by the unity* 1*, of cardinality a prime number* p*, which is its characteristic. The prime subfield is isomorphic to* $\mathbb{Z}_p$*.*

Theorem 1. *Every finite field has* p^n *elements for some prime* p *and natural number* n*.*

Proof. Let K be any finite field and $F = \mathbb{Z}_p$ be its prime subfield. We can view K as a vector space over the field F. Since K is finite, there exists a basis $\{b_1, \cdots, b_n\}$ of K. Every element of K can be written uniquely as

$$a_1 b_1 + \cdots + a_n b_n$$

where $a_i \in \mathbb{Z}_p$, which implies $|K| = p^n$

□

Theorem 2. *If a field* K *has* p^n *elements, then it is the splitting field for the polynomial* $f(X) = X^{p^n} - X$ *over* $\mathbb{Z}_p$

Proof. Consider the multiplicative group K^*, with $p^n - 1$ elements. By the Lagrange theorem, we know every element x of K satisfies $x^{p^n-1} - 1 = 0$. This also means $x^{p^n} - x = 0$. With 0, these are p^n roots of $f(X)$. But $f(X)$ has exactly p^n roots. Hence the field K is the set of all roots of $f(X)$. $f(X)$ splits over K, and $f(X)$ cannot split over any proper subfield.

□

With Theorem 1 and Theorem 2, we know if a field with p^n elements really exists, it is the splitting field over $\mathbb{Z}_p$. Then we show a splitting field really has p^n elements.

Lemma 2. *If a characteristic of a commutative ring* R *is a prime* p*, then the map*

$$\phi : R \to R, \quad \phi(x) = x^p$$

is an endomorphism of R*.*

Note that this implies $(x + y)^p = x^p + y^p$ in R.

Theorem 3. *The splitting field* K *for the polynomial* $f(X) = X^{p^n} - X$ *over* $\mathbb{Z}_p$ *has* p^n *elements.*

Proof. Let F be the set of all the roots of $f(X)$. By Lemma 2,

$$F = \{x \in K \mid x^{p^n} = x\} = \{x \in K \mid \phi(x)^n = x\}$$

Note that $1 \in F$ and as ϕ is an endomorphism, $\phi^n := \psi$ is also an endomorphism. So for any $a, b \in F$,

$$\psi(a + b) = \psi(a) + \psi(b) = a + b$$
$$\psi(ab) = \psi(a)\psi(b) = ab$$
$$\psi(a^{-1}) = \psi(a)^{-1} = a^{-1}$$

This says F is itself a field. This rather implies $F = K$ is the splitting field for $f(X)$. As there are p^n roots of $f(X)$, it is left to show that all roots are simple.

Given any root $a \neq 0$, we know $a^{p^n-1} = 1$ and

$$f(X) = (X^{p^n-1} - 1)X = (X^{p^n-1} - a^{p^n-1})X = (X - a)g(X)$$

for some $g(X)$. Dividing the polynomial,

$$g(X) = X^{p^n-1} + aX^{p^n-2} + \cdots + a^{p^n-2}X, \quad g(a) = (p^n - 1)a^{p^n-1} = -1$$

Hence a is a simple root.

□

With Theorem 1, Theorem 2, and Theorem 3, any finite field with cardinality p^n is a splitting field and exists for all prime p and natural number n, and they are all sorts of finite fields. Therefore, we then use $\mathbb{F}_{p^n}$ to denote any field with p^n elements. Also, by the proof of Theorem 3, $\mathbb{F}_{p^n}$ is the set of all the roots of $f(X) = X^{p^n} - X$ over $\mathbb{Z}_p$, and each root is simple.

2 Operation

Lemma 3. *For a finite field K, K^* is a cyclic group.*

Proof. Firstly, K^* is a finite Abelian group, so we may write K^* as

$$K^* = \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{k_t}}$$

for some prime powers $p_i^{k_i}$.

Suppose K^* is not a cyclic group, there exist some p_i and p_j that are not coprime, which means $p_i = p_j := p$. (If m, n are coprime, then $\mathbb{Z}_{mn} = \mathbb{Z}_m \oplus \mathbb{Z}_n$)

K^* thus have a subgroup isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$. This subgroup contains $p^2 - 1$ elements of order p, which means there are $p^2 - 1$ roots to the polynomials $X^p - 1$ over K. This contradicts the fact that $X^p - 1$ have at most p roots.

□

Theorem 4. *For every n, there exists an irreducible polynomial $q(X)$ over $\mathbb{Z}_p$ of degree n. Moreover,*

$$\mathbb{F}_{p^n} = \mathbb{Z}_p[X]/(q(X))$$

and that $q(X)$ divides $X^{p^n} - X$.

Proof. Let a be the generator of $\mathbb{F}_{p^n}^*$. Then $\mathbb{F}_{p^n} = \mathbb{Z}_p(a)$ since $\mathbb{F}_{p^n}$ contain $\mathbb{Z}_p$ and a, and all elements of $\mathbb{F}_{p^n}^*$ are powers of a. Now let $q(X)$ be the minimal polynomial of a over $\mathbb{Z}_p$, then

$$\deg(q(X)) = [\mathbb{Z}_p(a) : \mathbb{Z}_p] = [\mathbb{F}_{p^n} : \mathbb{Z}_p] = n$$

Moreover, by the isomorphism theorem, since $q(X)$ is irreducible,

$$\mathbb{Z}_p(a) = \mathbb{Z}_p[a] = \mathbb{Z}_p[X]/(q(X))$$

For any root b of $q(X)$ (in some algebraic closure of $\mathbb{Z}_p$). Since $q(X)$ is irreducible, $q(X)$ is also the minimal polynomial of b and thus

$$\mathbb{Z}_p[X]/(q(X)) = \mathbb{Z}_p(b) = \mathbb{F}_{p^n}$$

The field $\mathbb{F}_{p^n}$ is the set of all the roots of $f(X) = X^{p^n} - X$; as a result, b is also a root of $f(X)$. As all the roots of $q(X)$ in some algebraic closure is a root of $f(X)$, $q(X)|f(X)$.

□

Theorem 4 implies that to consider operating on the finite field $\mathbb{F}_{p^n}$, we can first find an irreducible polynomial $q(X)$ of degree n (which must exist), and then consider operating on the field $\mathbb{Z}_p[X]/(q(X))$. Moreover, by the following theorem, such $q(X)$ divides $X^{p^n} - X$.

Theorem 5. *Let $q(X)$ be an irreducible polynomial over $\mathbb{Z}_p$ of degree $d|n$, then $q(X)$ divides $X^{p^n} - X$.*

Proof. Let a be a root of $q(X)$ in some extension of $\mathbb{Z}_p$. As $q(X)$ is irreducible, $q(X)$ is the minimal polynomial of a and thus

$$[\mathbb{Z}_p(a) : \mathbb{Z}_p] = \deg(q(X)) = d$$

But this then implies $\mathbb{Z}_p(a)$ has p^d elements, $\mathbb{Z}_p(a) = \mathbb{Z}_{p^d}$, which further implies

$$a^{p^d} = a$$

But as $d|n$, $p^n = (p^d)^l$ for some l, and $a^{p^n} = (a^{p^d})^{p^d} \cdots = a$, we see a is also a root of $X^{p^n} - X$. This implies $q(X)$ divides $X^{p^n} - X$.

□

Finally, we show that all irreducible polynomials that divide $X^{p^n} - X$ can be used to construct the finite field $\mathbb{F}_{p^n}$.

Theorem 6. *$f(X) = X^{p^n} - X$ over $\mathbb{Z}_p$ is the product of all monic irreducible polynomials over $\mathbb{Z}_p$ whose degree $d|n$.*

Proof. On the one hand, from Theorem 5, we already know that any monic irreducible polynomials over $\mathbb{Z}_p$ whose degree $d|n$ divides $f(X)$. Since irreducible polynomials in $\mathbb{Z}_p[X]$ are coprime (otherwise, an element can have two minimal polynomials), we have

$$\prod_{\text{monic irr. } q\in\mathbb{Z}_p[X], \deg(q)|n} q(X) \mid f(X)$$

On the other hand, recall that

$$f(X) = \prod_{\alpha\in\mathbb{F}_{p^n}} (X - \alpha)$$

For each $\alpha \in \mathbb{F}_{p^n}$, its minimal polynomial $q_\alpha(X)$ must be of some degree $d|n$ since

$$\deg(q_\alpha(X)) = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p], \quad [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] \mid [\mathbb{F}_{p^n} : \mathbb{Z}_p] = n$$

Therefore, $X - \alpha$ divides some monic irreducible polynomial whose degree divides n. As each $X - \alpha$ is coprime,

$$f(X) = \prod_{\alpha\in\mathbb{F}_{p^n}} (X - \alpha) \mid \prod_{\text{monic irr. } q\in\mathbb{Z}_p[X], \deg(q)|n} q(X).$$

Hence,

$$f(X) = \prod_{\text{monic irr. } q\in\mathbb{Z}_p[X], \deg(q)|n} q(X)$$

□

3 Subfield

Finally, we discuss subfields of finite fields $\mathbb{F}_{p^n}$. Note that these subfields are also finite fields and have the same characteristic as the original field.

We first show that if $d \mid n$, we have a subfield $\mathbb{F}_{p^d}$.

Theorem 7. *Let $d \mid n$. The set*

$$L := \{x \in \mathbb{F}_{p^n} \mid x^{p^d} = x\}$$

is a subfield of $\mathbb{F}_{p^n}$ and $|L| = p^d$.

Proof. By Lemma 2 and the proof of Theorem 3, we know that $\phi(x) = x^p$ over $\mathbb{Z}_p$ is an endomorphism and thus $\psi := \phi^d$ is also an endomorphism. This implies L is a field in $\mathbb{F}_{p^n}$. But since each element in $\mathbb{F}_{p^n}$ is distinct, $|L| = \#\{\text{roots of } X^{p^d} - X\} = p^d$.

□

Next, we show that if $\mathbb{F}_{p^d}$ is a subfield, $d \mid n$.

Theorem 8. *Let L be a subfield of $\mathbb{F}_{p^n}$. Then $|L| = p^d$ for some $d \mid n$.*

Proof. Since L is a subfield of $\mathbb{F}_{p^n}$, its characteristic is p, and thus $|L| = p^d$ for some natural number d. Suppose $d \nmid n$, all elements of L are solutions to both equations

$$X^{p^d} - X = 0 \quad \text{and} \quad X^{p^n} - X = 0$$

Let $a \in L$, and let $n = dq + r$ for some $r < d$, then

$$\alpha = \alpha^{p^n} = (\alpha^{p^d})^{p^{n-d}} = \alpha^{p^{n-d}} = \cdots = \alpha^{p^r}$$

Hence, α is also a root of the polynomial of $X^{p^r} - X$. There are at most p^r roots of this polynomial, but there are $|L| = p^d > p^r$ elements in L. Since we have shown in previous theorems that the roots of the polynomial $X^{p^d} - X$ are all simple, this fact leads to a contradiction.

$\square$

Theorem 7 and Theorem 8 show that every divisor d of n corresponds to a unique subfield $\mathbb{F}_{p^d}$ of $\mathbb{F}_{p^n}$.

We can now view $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ as subfields of $\mathbb{F}_{p^{mn}}$. This implies the following theorem.

Theorem 9. *The set*

$$\bar{\mathbb{Z}}_p := \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$$

is a field. Moreover, it is the algebraic closure of $\mathbb{Z}_p$.

Proof.

$\bar{\mathbb{Z}}_p$ is a field

Given any $a \neq 0, b \in \bar{\mathbb{Z}}_p$, there are some natural numbers m, n such that $a \in \mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$. Since both fields are subfields of $\mathbb{F}_{p^{mn}}$, $a, b \in \mathbb{F}_{p^{mn}}$, and thus $a \pm b, ab, a^{-1}b$ are all in $\mathbb{F}_{p^{mn}} \subset \bar{\mathbb{Z}}_p$.

$\bar{\mathbb{Z}}_p$ is algebraically closed.

Given any polynomial $f(X) = \sum_{i=1}^{m} a_i X^i$ over $\bar{\mathbb{Z}}_p$, where $a_i \in \mathbb{F}_{p^{n_i}}$, we can view it as a polynomial over $\mathbb{F}_{p^M}$, where $M = l.c.m(\{n_i\})$. Let $g(X)$ be an irreducible polynomial that divides $f(X)$. Such $g(X)$ must exist since $f(X) \in \bar{\mathbb{Z}}_p[X]$, a principal ideal domain.

Consider the ring $K = \mathbb{Z}_{p^M}[X]/(g(X))$. Note that it is an extension of $\mathbb{Z}_{p^M}$, and $g(X)$ has a root in K since

$$g(X + (g(X))) = g(X) + (g(X)) = 0$$

Moreover, K is finite and contains $(p^M)^{\deg(g(X))}$ elements. All finite fields are of size q^N for some prime number q and natural number N, where q is its characteristic. Hence, $q = p$ and $K = \mathbb{F}_{p^{M\deg(g(X))}}$. We thus show that $g(X)$ has a root in $\mathbb{F}_{p^{M\deg(g(X))}} \subset \bar{\mathbb{Z}}_p$, which implies $f(X)$ also has a root in $\bar{\mathbb{Z}}_p$.

$\bar{\mathbb{Z}}_p$ is an algebraic extension of $\mathbb{Z}_p$.

Given any $a \in \bar{\mathbb{Z}}_p$, there is some natural numbers n such that $a \in \mathbb{F}_{p^n}$, which implies that a is a root of the polynomial $X^{p^n} - X$ over $\mathbb{Z}_p$.

$\square$