Finite Fields

Jiang-Hua Lu

The University of Hong Kong

MATH4302, Algebra II

Thursday April 10, 2025

In this file:

What we already know about finite fields:

- Most basic example: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number.
- $|\mathbb{F}_p| = p$.
- Every finite field F is an extension of $\mathbb{F}_p$, where $p = \mathrm{char}(F)$.
- If F is a finite field and $\mathrm{char}(F) = p$, then

  $$F \cong \mathbb{F}_p^n = \{(a_1, \ldots, a_n) : a_j \in \mathbb{F}_p\} \quad \text{as a vector space over } \mathbb{F}_p,$$

  where $n = [F : \mathbb{F}_p]$. In particular, $|F| = p^n$.
- There ~~there~~ are no fields with 35 elements.

Lemma. If $|F| = p^n$ and $K \subset F$ a sub-field, then $|K| = p^d$ for some $1 \leq d \leq n$ and $d|n$.

Proof. Being a sub-field of F, K also has characteristic p. Let $d = [K : \mathbb{F}_p]$. Then

$$n = [F : \mathbb{F}_p] = [F : K][K : \mathbb{F}_p] = d[F : K].$$

$\diamond$

Example. If $|F| = 7^6$, then possible cardinalities of sub-fields of F are

$$7,\ 7^2,\ 7^3,\ 7^6.$$

Question. If $|F| = 7^6$, are there sub-fields of F with 7^2 or 7^3 elements?

Theorems to be proved: Let p be a prime number.

1. For any $n \geq 1$, there is one field, and only one up to isomorphism, with p^n elements, which is denoted as $\mathbb{F}_{p^n}$.
2. For each $n \geq 1$ and for each $d|n$, there is exactly one sub-field of $\mathbb{F}_{p^n}$ which is $\mathbb{F}_{p^d}$.
3. A description of all irreducible polynomials over $\mathbb{F}_p$ for every prime p.

Main tools:

1. The quotient $\mathbb{F}_p[x]/\langle f \rangle$ for irreducible $f \in \mathbb{F}_p[x]$.
2. Splitting fields.

$|F| = p^2, p^3$

Recall the quotient construction:

If $f(x) \in \mathbb{F}_p[x]$ is irreducible and has degree n, then $\mathbb{F}_p[x]/\langle f \rangle$ is a field with p^n elements.

Easy for small n and p:

4, 8

Example. There are exactly 4 quadratic polynomials in $\mathbb{F}_2[x]$: $f(x) = x^2 + ax + b$ with $a, b \in \mathbb{F}_2$:

$$x^2, \quad x^2 + 1, \quad x^2 + x, \quad x^2 + x + 1.$$

The only irreducible one is $f(x) = x^2 + x + 1$, and

$$\mathbb{F}_2[x]/\langle f \rangle = \mathbb{F}_4 = \{0, 1, a, a + 1\}.$$

Multiplication table:

Exercise: There are exactly two cubic irreducible polynomials in $\mathbb{F}_2[x]$:

$$f = x^3 + x + 1 \quad \text{and} \quad g = x^3 + x^2 + 1.$$

Write down the addition and multiplication tables of

$$\mathbb{F}_8 = \mathbb{F}_2[x]/\langle f \rangle \quad \text{and} \quad \mathbb{F}_8' = \mathbb{F}_2[x]/\langle f \rangle$$

and show that $\mathbb{F}_8 \cong \mathbb{F}_8'$.

A fundamental fact about characteristic p (Every student's dream)

Lemma. If F is a field with $\mathrm{char}(F) = p > 0$, then

$$(a+b)^p = a^p + b^p, \qquad \forall a, b \in F.$$

Lemma. If F is a finite field of order q, then every element $a \in F$ satisfies

$$x^q - x = 0.$$

Proof.

- If $a = 0$, ok.
- Assume that $a \neq 0$. Then $a \in F \backslash \{0\}$ which is an abelian group with $q - 1$ elements.
- By Lagrange's Theorem, $a^{q-1} = 1$, so $a^q = a$.

$\diamond$

We fix a prime number p throughout. Let $n \geq 1$ be an integer.

Theorem

A finite field F has order p^n if and only if it is isomorphic to the splitting field over $\mathbb{F}_p$ of

$$f(x) = x^{p^n} - x \in \mathbb{F}_p[x].$$

Proof. Assume first that F is a field of order p^n.

- The prime field of F is $\mathbb{F}_p$, so F is an extension of $\mathbb{F}_p$;
- By previous lemma, every $\alpha \in F$ is a root of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$;
- f can have at most p^n roots in F, so $F = R_f$, the set of all roots of f in F;
- Thus f completely splits in $F[x]$, and $F = \mathbb{F}_p(R_f)$ is a splitting field of f over $\mathbb{F}_p$.

Proof Cont'd:

Conversely, let F be a splitting field of $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$. Let R be the set of all roots of f on F.

- Since $f'(x) = p^n x^{p^n - 1} - 1 = -1$ has no roots in F, f has no repeated roots in F.
- Since $\deg(f) = p^n$, f has exactly p^n roots in F, i.e., $|R| = p^n$.
- For any $a, b \in R$,

  $$(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b, \qquad (ab)^{p^n} = a^{p^n} b^{p^n} = ab,$$

  and if $b \neq 0$, then $(1/b)^{p^n} = 1/b$. Thus R is a sub-field of F.
- Moreover, $\mathbb{F}_p \subset R$. Thus $F = \mathbb{F}_p(R) = R$. Conclude that

  $$|F| = |R| = p^n.$$

Q.E.D.

<u>Question</u>: Is there another $g(x) \in \mathbb{F}_p[x]$ with $\deg g < p^n$ s.t. the splitting field of g has order p^n?

Corollary

For any prime number p and any integer $n \geq 1$,

1. *there exist fields with p^n elements;*
2. *any two fields with p^n elements are isomorphic.*

Proof. Statements follow directly from existence and uniqueness of splitting fields.

We turn to sub-fields of $\mathbb{F}_{p^n}$, p a prime number. Recall

Easy Fact: If F is a field with p^n elements, where $n \geq 1$, then every sub-field of K is F has order p^d for some $1 \leq d \leq n$ and $d|n$.

Fact: For any prime p and integers $d, n \geq 1$ such that $d|n$, one has

$$(x^{p^d} - x)|(x^{p^n} - x). \quad \text{in } \mathbb{Z}[x]$$

Proof: For positive integers a, b, we have the identity

$$z^{ab} - 1 = (z^a - 1)((z^a)^{b-1} + \cdots + z^a + 1).$$

- Since $d|n$, we have $(p^d - 1)|(p^n - 1)$.
- Using the identity again, we have $(x^{p^d - 1} - 1)|(x^{p^n - 1} - 1)$.
- It follows that $(x^{p^d} - x)|(x^{p^n} - x)$.

Q.E.D.

Theorem

For each $d \in \mathbb{Z}_{\geq 1}$ such that $d|n$, there is one and exactly one sub-field of $\mathbb{F}_{p^n}$ with p^d elements. These are all sub-fields of $\mathbb{F}_{p^n}$.

Proof. We already know that a sub-field of $\mathbb{F}_{p^n}$ necessarily has order p^d for some $d|n$.

- Fix d such that $d|n$. Remains to show that there is one and exactly one sub-field of $\mathbb{F}_{p^n}$ with p^d elements.
- Let $f_n = x^{p^n} - x \in \mathbb{F}_p[x]$ and $f_d = x^{p^d} - x \in \mathbb{F}_p[x]$.
- We have proved that $\mathbb{F}_{p^n}$ is a splitting field of f_n; all elements of $\mathbb{F}_{p^n}$ are roots of f_n, and no one is repeated. $f_n = (x - \alpha_1) \cdots (x - \alpha_{p^n})$
- One has $f_d | f_n$ by previous Lemma, so f_d completely splits in $\mathbb{F}_{p^n}$.

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

$$(a+b)^p = a^p + b^p$$

Proof cont'd:

- Using Every Student's Dream, we see again that the set R_{f_d} of all roots of f_d in $\mathbb{F}_{p^n}$ is a sub-field with p^d elements.
- Suppose that K is a sub-field of $\mathbb{F}_{p^n}$ with p^d elements.
- Then every $\alpha \in K$ satisfies $\alpha^{p^d} - \alpha = 0$.
- So $K \subset R_{f_d}$, and thus $K = R_{f_d}$.
- Thus so R_{f_d} is the unique sub-field of $\mathbb{F}_{p^n}$ with p^d elements.

Q.E.D.

Another basic fact about finite fields. Let K be any field.

Theorem

Any finite subgroup G of the multiplicative group $K^\star = K \backslash \{0\}$ is cyclic. In particular, $K^\star$ is cyclic if K is finite.

Proof. Let $|G| = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$, $p_1, \ldots, p_l$ distinct prime numbers.

- By the Classification Theorem on Finite Abelian Groups, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$$G = G(p_1) \times G(p_2) \times \cdots \times G(p_l),$$

  where for each $i = 1, \ldots, l$ there exist positive integers k_i and $n_{i,1}, \ldots, n_{i,k_i}$ such that $n_i = n_{i,1} + \cdots + n_{i,k_k}$, and $\simeq \mathbb{Z}/6\mathbb{Z}$

$$|G(p_i)| = p_i^{n_i} \qquad G(p_i) \cong (\mathbb{Z}/p_i^{n_{i,1}}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_i^{n_{i,k_i}}\mathbb{Z}). \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

- By the Chinese Reminder Theorem, enough to show that each $k_i = 1$ for each $i = 1, \ldots, l$, so $G(p_i)$ is cyclic. $\cancel{\not\cong}$ $\mathbb{Z}/4\mathbb{Z}$

If $k_i > 1$, then $r < n_i$ s.t every elt $a \in G(p_i)$ satisfies $a^{p^r} = 1$

Proof cont'd:

- Assume that there exists j such that $k_j > 1$ ~~is not~~ cyclic.
- Then there exists $r < n_j$ such that every $a \in G(p_j)$ satisfies $a^{p_j^r} = 1$.
- Now $G(p_j)$ has $p_j^{n_j}$ elements;
- The equation $x^{p_j^r} = 1$ can have at most p^r solutions, so this is a contradiction.
- Hence every $G(p_j)$ is cyclic and that G is cyclic.

Q.E.D.

这个定理确实是换成finite integral domain**也成立的，**
但这是trivial**的，**因为finite integral domain**等价于**finite field

Corollary

Any finite extension of a finite field is simple.

Proof. Let F be a finite extension of a finite field K.

- Since $F \backslash \{0\}$ is a cyclic group, there exists $a \in F \backslash \{0\}$ such that every $b \in F \backslash \{0\}$ is a power of a.
- Thus $F = K(a)$.

Q.E.D.

continue on
Monday, April 14
2025

We turn to Irreducible polynomials over $\mathbb{F}_p$, where p is a prime number.

Lemma. For any $n \geq 1$,

1. irreducible polynomials over $\mathbb{F}_p$ of degree n exist;
2. every monic irreducible polynomial of degree n is a factor of
$$f_n(x) = x^{p^n} - x.$$
3. every monic irreducible polynomial of degree $d|n$ is a factor of f_n.

Proof.

- We proved that $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_{p^n}$.
- the minimal polynomial of α over $\mathbb{F}_p$ is irreducible and has degree n.

Proof cont'd:

- Let $q \in \mathbb{F}_p[x]$ be any irreducible monic with degree n.
- Then the field $L = \mathbb{F}_p[x]/\langle q \rangle$ has p^n elements;
- The element $a = \bar{x} \in L$ satisfies $f_n(a) = 0$, so $q | f_n$.
- Assume now that $q \in \mathbb{F}_p[x]$ is irreducible monic with degree $d | n$.
- Then $q | f_d$. Since $f_d | f_n$, we have $q | f_n$.

Q.E.D.

Consider the factorization

$$f_n = q_1^{k_1} q_2^{k_2} \cdots q_l^{k_l} \in \mathbb{F}_p[x]$$

into irreducible factors, where the q_j's are pairwise distinct and monic.

First some observations:

- Since f_n splits completely in $\mathbb{F}_{p^n}$ with no repeated roots, must have $k_1 = \cdots = k_l = 1$.
- Consider the factor q_j and let $d_j = \deg(q_j)$.
- q_j splits completely in $\mathbb{F}_{p^n}$ with no repeated roots;
- Let $a \in \mathbb{F}_{p^n}$ be a root of q_j.
- Then $\mathbb{F}_p(a)$ is a sub-field of $\mathbb{F}_{p^n}$ with p^{d_j} elements;
- By results on sub-fields of $\mathbb{F}_{p^n}$, must have $d_j | n$.

We have thus proved the following Theorem on the polynomial

$$f_n(x) = x^{p^n} - x \in \mathbb{F}_p[x]$$

Theorem: For any prime number p and any $n \geq 1$,

1. the irreducible factors of $f_n(x)$ in $\mathbb{F}_p[x]$ are precisely all the monic irreducible polynomials in $\mathbb{F}_p[x]$ with degrees $d|n$;
2. each such polynomial appears exactly once in the prime factorization of $f_n(x)$.

Examples. In $\mathbb{F}_2[x]$, one has

$$\begin{aligned}
x^2 - x &= x(x-1), \\
x^4 - x &= x(x-1)(x^2+x+1), \\
x^8 - x &= x(x-1)(x^3+x+1)(x^3+x^2+1), \\
x^{16} - x &= x(x-1)(x^2+x+1)(x^4+x+1) \\
&\qquad (x^4+x^3+1)(x^4+x^3+x^2+x+1).
\end{aligned}$$

The Frobenius homomorphism:

Lemma-Definition. For a field L of characteristic $p > 0$, the map

$$\sigma : \quad L \longrightarrow L, \qquad \sigma(a) = a^p,$$

is an injective ring homomorphism, called the Frobenius homomorphism of L.

Lemma. If L is a finite field, the Frobenius morphism is an isomorphism.

Proof. The Frobenius morphism $\sigma : L \to L$ is injective, so $\sigma(L)$ is a subset of L, and $|\sigma(L)| = |L|$. Thus $\sigma(L) = L$, i.e., σ is surjective.

Example. The Frobenius morphism on $L = \mathbb{F}_p(t)$ is not surjective: $t \in \mathbb{F}_p(t)$ is not in the image σ.

Proof. We prove by contradiction.

- Suppose that $\alpha = \frac{f(t)}{g(t)} \in L$ satisfies $\sigma(\alpha) = t$, where $f(t), g(t) \in \mathbb{F}_2[t]$.
- Then $\alpha^p = t$, so $f(t)^p = tg(t)^p$.
- Let $m = \deg(f)$ and $n = \deg(g)$. Then $mp = 1 + np$, not possible.
- Thus $t \in L$ is not in image of σ.

Q.E.D.