Finite Fields: Part II

Cunsheng Ding

HKUST, Hong Kong

November 26, 2015

Contents

The Objective of this Lecture

Our objective

- Study the structure of the finite fields $\mathrm{GF}(p^m)$.
- Deal with extensions and subfields of $\mathrm{GF}(p^m)$.

Throughout this lecture, let $q = p^m$, where p is any prime and m is any positive integer.

The Group $(\mathrm{GF}(q)^*, \cdot)$ of the Finite Field $\mathrm{GF}(q)$

Our first task is to prove that the group $(\mathrm{GF}(q)^*, \cdot)$ is cyclic. To this end, we need to prove a number of auxiliary results.

Proposition 1

For any $a \in \mathrm{GF}(q)^*$, there exists a positive integer ℓ such that $a^\ell = 1$.

Proof.

Consider the following sequence of elements in $\mathrm{GF}(q)^*$:

$$a^0, a^1, a^2, \cdots.$$

Since the group $\mathrm{GF}(q)^*$ has order $q-1$, there exist two distinct $0 \le h < k$ such that $a^h = a^k$. Hence, $a^h(a^{k-h} - 1) = 0$ and $a^{k-h} = 1$. The desired conclusion then follows. $\square$

The Group $(\mathrm{GF}(q)^*, \cdot)$ of the Finite Field $\mathrm{GF}(q)$

Definition 2

The order of $a \in \mathrm{GF}(q)^*$, denoted by $\mathrm{ord}(a)$, is the least positive integer ℓ such that $a^\ell = 1$.

The following theorem was proved in the previous lecture about groups and rings.

Proposition 3 (Lagrange's Theorem)

For any $a \in \mathrm{GF}(q)^*$, $\mathrm{ord}(a)$ divides $q-1$.

The following conclusion follows from Proposition 3.

Proposition 4

Every $a \in \mathrm{GF}(q)$ satisfies $a^q = a$.

The Group $(\mathrm{GF}(q)^*, \cdot)$ of the Finite Field $\mathrm{GF}(q)$

The proof of the following proposition is left as an exercise.

Proposition 5

For any $a \in \mathrm{GF}(q)^*$, we have $\mathrm{ord}(a^i) = \mathrm{ord}(a)/\gcd(\mathrm{ord}(a), i)$.

The Group $(\mathrm{GF}(q)^*, \cdot)$ of the Finite Field $\mathrm{GF}(q)$

Proposition 6

For any $a \in \mathrm{GF}(q)^*$ and $b \in \mathrm{GF}(q)^*$, we have $\mathrm{ord}(ab) = \mathrm{ord}(a)\mathrm{ord}(b)$ if $\gcd(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$.

Proof.

Let ℓ be a positive integer such that $(ab)^\ell = 1$. Then $a^\ell = b^{-\ell}$. Hence, $a^{\ell \mathrm{ord}(b)} = (b^{\mathrm{ord}(b)})^{-\ell} = 1$. It then follows that $\mathrm{ord}(a) \mid \ell \mathrm{ord}(b)$. Since $\gcd(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, $\mathrm{ord}(a)$ divides ℓ. By symmetry, $\mathrm{ord}(b)$ divides ℓ. Consequently, $\mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$ must divide ℓ. But $\mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b)) = \mathrm{ord}(a)\mathrm{ord}(b)$, as $\gcd(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$. On the other hand, it is obvious that $(ab)^{\mathrm{ord}(a)\mathrm{ord}(b)} = 1$. The desired conclusion then follows. $\square$

The Group $(\mathrm{GF}(q)^*, \cdot)$ of the Finite Field $\mathrm{GF}(q)$

Proposition 7

If $g(x) \in \mathbb{F}[x]$ has degree n, then the equation $g(x) = 0$ has at most n solutions in $\mathbb{F}$, where $\mathbb{F}$ is any field.

Proof.

The proof is by induction on n. If $n = 1$, the equation is of the form $ax + b = 0$, which obviously has only the solution $x = -b/a$. If $n \geq 2$ and $g(x) = 0$ has no solution, then we are done. Otherwise, $g(\alpha) = 0$ for some $\alpha \in \mathbb{F}$, and apply the Division Algorithm to divide $g(x)$ by $x - \alpha$. Then we have

$$g(x) = q(x)(x - \alpha) + g(\alpha) = q(x)(x - \alpha).$$

Now $\deg(q(x)) = n - 1$. By induction, $q(x) = 0$ has at most $n - 1$ solutions. Whence, $g(x) = 0$ has at most n solutions.

□

The Group $(\mathrm{GF}(q)^*, \cdot)$ of the Finite Field $\mathrm{GF}(q)$

Theorem 8

The multiplicative group $\mathrm{GF}(q)^*$ *is cyclic.*

Proof.

We assume that $q \geq 3$. Let $h := q - 1 = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ be the canonical factorization of $q - 1$. For every i with $1 \leq i \leq n$, by Proposition 7, the polynomial $x^{h/p_i} - 1$ has at most h/p_i roots in $\mathrm{GF}(q)$. Since $h/p_i < h$, it follows that there are nonzero elements in $\mathrm{GF}(q)$ that are not roots of this polynomial.

Let a_i be such an element, and set $b_i = a_i^{h/p_i^{r_i}}$.

By Proposition 3, $b_i^{p_i^{r_i}} = a_i^h = a_i^{q-1} = 1$. Hence, $\mathrm{ord}(b_i) = p_i^{s_i}$, where $0 \leq s_i \leq r_i$. On the other hand, $b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1$. It follows that $\mathrm{ord}(b_i) = p_i^{r_i}$.

By Proposition 6, we have

$$\mathrm{ord}(b_1 b_2 \cdots b_n) = \mathrm{ord}(b_1)\mathrm{ord}(b_2) \cdots \mathrm{ord}(b_n) = h = q - 1.$$

$\square$

The Group $(\mathrm{GF}(q)^*, \cdot)$ of the Finite Field $\mathrm{GF}(q)$

Definition 9

Any element in $\mathrm{GF}(q)^*$ with order $q-1$ is called a generator of $\mathrm{GF}(q)^*$ and a primitive element of $\mathrm{GF}(q)$.

Theorem 10

$\mathrm{GF}(q)$ *has* $\phi(q-1)$ *primitive elements.*

Proof.

By Theorem 8, $\mathrm{GF}(q)$ has a primitive element α. Hence, every element $\beta \in \mathrm{GF}(q)^*$ can be expressed as $\beta = \alpha^k$ for some k. By Proposition 5, β is a primitive element if and only if $\gcd(k, q-1) = 1$. The desired conclusion then follows. $\square$

The Group $(\mathrm{GF}(q)^*, \cdot)$ of the Finite Field $\mathrm{GF}(q)$

Remark

Let p be any prime. Then a primitive element of $\mathrm{GF}(p)$ is called the primitive root of p or modulo p.

Example 11

It is easily verified that 3 is a primitive element of $\mathrm{GF}(7)$. Note that $\phi(6) = 2$. $\mathrm{GF}(7)$ has only two primitive elements: 3 and $3^5 \bmod 7 = 5$.

Uniqueness of Finite Fields

Definition 12

Two fields $\mathbb{F}_1$ and $\mathbb{F}_2$ are said to be <u>isomorphic</u> if there is a bijection σ from $\mathbb{F}_1$ to $\mathbb{F}_2$ satisfying the following:

1. $\sigma(a+b) = \sigma(a) + \sigma(b)$ for all $a, b \in \mathbb{F}_1$.
2. $\sigma(ab) = \sigma(a)\sigma(b)$ for all $a, b \in \mathbb{F}_1$.
3. $\sigma(1_{\mathbb{F}_1}) = 1_{\mathbb{F}_2}$, where $1_{\mathbb{F}_1}$ and $1_{\mathbb{F}_2}$ are the identities of $\mathbb{F}_1$ and $\mathbb{F}_2$, respectively.

Remarks

- Two isomorphic fields have the same properties, and thus can be viewed as identical.
- In an assignment problem, you will be asked to prove that two finite fields are isomorphic.

Uniqueness of Finite Fields

The following theorem can be found in Chapter 2 of Lidl and Niederreiter.

Theorem 13

Any finite field with p^m elements is isomorphic to $\mathrm{GF}(p^m)$, constructd with a fixed monic irreducible polynomial $\pi(x) \in \mathrm{GF}(p)[x]$ with degree m.

Remark

Due to this theorem, we do not need to specify the monic irreducible polynomial $\pi(x)$ over $\mathrm{GF}(p)$ with degree m when we mention $\mathrm{GF}(p^m)$.

Extensions and Subfields of Finite Fields

Definition 14

Let $\mathbb{F}$ be a field. A subset $\mathbb{K}$ of $\mathbb{F}$ that is itself a field under the operations of $\mathbb{F}$ will be called a subfield of $\mathbb{F}$. In this context, $\mathbb{F}$ is called an extension field of $\mathbb{K}$. If $\mathbb{K} \neq \mathbb{F}$, we say that $\mathbb{K}$ is a proper subfield of $\mathbb{F}$.
A field containing no proper subfields is called a prime field. Examples of prime fields are $\mathrm{GF}(p)$, where p is any prime.

Example 15

$\mathrm{GF}(p^m)$ is an extension field of $\mathrm{GF}(p)$, and $\mathrm{GF}(p)$ is a subfield of $\mathrm{GF}(p^m)$.

Existence of Subfields of Finite Fields

Theorem 16

If $\mathrm{GF}(p^k)$ *is a subfield of* $\mathrm{GF}(p^m)$*, then* $k \mid m$*.*

Proof.

Every $b \in \mathrm{GF}(p^m)$ must be a root of $x^{p^m} = x$. Every $a \in \mathrm{GF}(p^k)$ must be a root of $x^{p^k} = x$. Since $\mathrm{GF}(p^k) \subseteq \mathrm{GF}(p^m)$, every $a \in \mathrm{GF}(p^k)$ is also a root of $x^{p^m} = x$. Thus, $(x^{p^k} - x) \mid (x^{p^m} - x)$, and $(x^{p^k-1} - 1) \mid (x^{p^m-1} - 1)$. It then follows that

$$x^{p^k-1} - 1 = \gcd(x^{p^k-1} - 1, x^{p^m-1} - 1).$$

But, we have

$$\gcd(x^{p^k-1} - 1, x^{p^m-1} - 1) = x^{\gcd(p^k-1, p^m-1)} - 1 = x^{p^{\gcd(k,m)}-1} - 1. \tag{1}$$

Hence, $k \mid m$. $\square$

Existence of Subfields of Finite Fields

Theorem 17

Let $k \mid m$. Then $\mathrm{GF}(p^m)$ has a subfield with p^k elements.

Proof.

Since $k \mid m$, it follows from (1) that $(x^{p^k} - x) \mid (x^{p^m} - x)$. Note that all the elements of $\mathrm{GF}(p^m)$ are the roots of $x^{p^m} - x = 0$. It then follows that the set

$$\mathbb{K} = \{a \in \mathrm{GF}(p^m) \mid a^{p^k} = a\}$$

has cardinality p^k.
Let $a, b \in \mathbb{K}$. Then

$$(a+b)^{p^k} = a^{p^k} + b^{p^k} = a+b, \ (ab)^{p^k} = a^{p^k} b^{p^k} = ab, \ (a^{-1})^{p^k} = (a^{p^k})^{-1} = a^{-1}.$$

Hence, $\mathbb{K}$ is a subfield with p^k elements. $\square$

Existence of Subfields of Finite Fields

Theorem 18

Let $k \mid m$ and let $\mathrm{GF}(p^k)$ denote the subfield of $\mathrm{GF}(p^m)$. Let α be a generator of $\mathrm{GF}(p^m)^*$, and let $\beta = \alpha^{(p^m-1)/(p^k-1)}$. Then β is a generator of $\mathrm{GF}(p^k)^*$.

Proof.

By definition, $\beta^{p^k} = \beta$. It then follows from the proof of heorem 17 that $\beta \in \mathrm{GF}(p^k)$. By Proposition 5,

$$\mathrm{ord}(\beta) = \frac{\mathrm{ord}(\alpha)}{\gcd\left(\mathrm{ord}(\alpha), \frac{p^m-1}{p^k-1}\right)} = \frac{p^m-1}{\gcd\left(p^m-1, \frac{p^m-1}{p^k-1}\right)} = p^k - 1.$$

The desired conclusion then follows. □

Minimal Polynomials over $\mathrm{GF}(r)$ of Elements in $\mathrm{GF}(r^\ell)$

Let r be a power of p in the following.

Definition 19

Let $\ell \geq 1$ be an integer. For any $a \in \mathrm{GF}(r^\ell)^*$, the monic polynomial $P_a(x) \in \mathrm{GF}(r)[x]$ with the least degree such that $P_a(a) = 0$ is called the minimal polynomial over $\mathrm{GF}(r)$ of a.

Remarks

- The existence of the minimal polynomial is guaranteed by Proposition 4 (i.e., $a^{r^\ell - 1} - 1 = 0$).
- By definition, $P_a(x)$ is irreducible over $\mathrm{GF}(r)$.
- It follows from Proposition 4 that $P_a(x)$ divides $x^{r^\ell - 1} - 1$.

Minimal Polynomials over $\mathrm{GF}(r)$ of Elements in $\mathrm{GF}(r^\ell)$

Proposition 20

Let $a \in \mathrm{GF}(r^\ell)^*$. Then the minimal polynomial $P_a(x)$ of a over $\mathrm{GF}(r)$ has degree at most ℓ.

Proof.

Note that $a^{r^\ell} = a$ for any $a \in \mathrm{GF}(r^\ell)^*$. The set $\{a^{r^i} : i = 0, 1, 2, \ell - 1\}$ has at most ℓ elements. Let e be the smallest positive integer such that $a^{r^e} = a$. Then $e \leq \ell$. Define

$$g(x) = \prod_{i=0}^{e-1} (x - a^{r^i}).$$

Since $g(x)^r = g(x^r)$, g is a polynomial over $\mathrm{GF}(r)$. On the other hand, $g(a) = 0$ and $\deg(g) = e$. The desired conclusion then follows.

□

Minimal Polynomials over $\mathrm{GF}(r)$ of Elements in $\mathrm{GF}(r^\ell)$

Proposition 21

If α is a generator of $\mathrm{GF}(r^\ell)^*$, the minimal polynomial $P_\alpha(x)$ has degree ℓ.

Proof.

Let α is a generator of $\mathrm{GF}(r^\ell)^*$. Suppose that the minimal polynomial $P_\alpha(x)$ has degree $e < \ell$. Let

$$P_\alpha(x) = x^e + a_{e-1}x^{e-1} + a_{e-2}x^{e-2} + \cdots + e_1 x + e_0.$$

Then each α^i can be expressed as $\sum_{k=0}^{e-1} b_k \alpha^k$, where all $b_i \in \mathrm{GF}(r)$. Then we have

$$|\{0, \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{r^\ell - 2}\}| \leq r^e < r^\ell.$$

This is contrary to the assumption that α is a generator of $\mathrm{GF}(r^\ell)^*$. The desired conclusion then follows from Proposition 20. □

The Finite Field $\mathrm{GF}(2^3)$

Example 22

Let α be a generator of $\mathrm{GF}(2^3)^*$ with minimal polynomial $P_\alpha(x) = x^3 + x + 1$. Then the minimal polynomials of all the elements over $\mathrm{GF}(2)$ are:

$$\begin{array}{ll}
0 & x, \\
\alpha^0 & x - 1, \\
\alpha^1 & x^3 + x + 1, \\
\alpha^2 & x^3 + x + 1, \\
\alpha^3 & x^3 + x^2 + 1, \\
\alpha^4 & x^3 + x + 1, \\
\alpha^5 & x^3 + x^2 + 1, \\
\alpha^6 & x^3 + x^2 + 1.
\end{array}$$

Note that the canonical factorization of $x^{2^3-1} - 1$ over $\mathrm{GF}(2)$ is given by

$$x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1).$$