Note for Finite Field

Date: May 21 Made by Eric

Goal

Theorem 1. ***(List of All finite field)*** *Every finite field are of prime power order, and conversely, for all prime power $x = p^n$, there exists exactly one field of order x.*

The theorem above is short and powerful, but it is no way simple. We partition the theorem into:

Part (A) Every field is of order of prime power.

Part (B) For all prime power $x = p^n$, there exists a field of order x.

Part (C) For all prime power $x = p^n$, there is only one finite field of order x.

Part (A)

Theorem 2. *Every finite field $\mathbb{F}$ is of prime characteristic.*

Proof. Because $\mathbb{F}$ is finite, we know the characteristic is non-zero. Then we assume the characteristic of $\mathbb{F}$ is mn where m, n are greater than 1. Let $u = n \cdot 1 \neq 0$ and observe that $m \cdot (u) = (mn) \cdot 1 = 0$ CaC ∎

Theorem 3. *Every finite field $\mathbb{F}$ is of prime power order.*

Proof. Let p be the characteristic of $\mathbb{F}$, and observe that $\{m \cdot 1 | m \in \mathbb{Z}\}$ is a sub-field of $\mathbb{F}$ of order p. By Theorem of Lagarange, we know p divides the order of $\mathbb{F}$, so we wish to show that no other prime q divides the order of $\mathbb{F}$. Assume there exists some other prime q divides the order of $\mathbb{F}$. Notice that $\langle \mathbb{F}, + \rangle$ is a group of some order divided by q, so by First Sylow Theorem, we know there exists an element α of order q in group $\langle \mathbb{F}, + \rangle$. In other word, $q \cdot \alpha = 0$. Do division algorithm to q with p, to have $q = np + r$ where $0 \leq r < p$. Here, $0 < r$ because q is a prime, not divided by p. Then we see $0 = q \cdot \alpha = (np) \cdot \alpha + r \cdot \alpha = r \cdot \alpha$ CaC to p is the characteristic of $\mathbb{F}$.

∎

Part (B): Existence

Lemma 4. *Every finite field $\mathbb{F}$ of power p^n contain a sub-field isomorphic to $\mathbb{Z}_p$, thus $\mathbb{F}$ is isomorphic to a sub-field of $\overline{\mathbb{Z}_p}$*

Proof. Check that $\{m \cdot 1 | m \in \mathbb{Z}\}$ is a sub-field and is isomorphic to $\mathbb{Z}_p$. ∎

Lemma 5. *There are p^n amount of distinct zeros in $\overline{\mathbb{Z}_p}$ of the polynomial $x^{p^n} - x \in \mathbb{Z}_p[x]$*

Proof. Let $f(x) = x^{p^n} - x \in \overline{\mathbb{Z}_p}$. We wish to show that every zero α of $f(x)$ are of multiplicity 1.

It is obvious that 0 is a zero of $f(x)$ of multiplicity 1. Assume $\alpha \neq 0$ and $\alpha \in \overline{\mathbb{Z}_p}$ is a zero of $f(x)$ of multiplicity greater than 1. Observe

$$x^{p^n} - x = x(x^{p^n-1} - 1) \tag{1}$$

Because $\alpha \neq 0$, we know $\alpha^{p^n-1} - 1 = 0$. In other words, $\alpha^{p^{n-1}} = 1$. Then

$$f(x) = x^{p^n} - x = x(x^{p^{n-1}} - 1) = x(x^{p^{n-1}} - \alpha^{p^{n-1}}) \tag{2}$$

$$= x(x-\alpha)(x^{p^n-2} + \alpha x^{p^n-3} + \alpha^2 x^{p^n-4} + \cdots + \alpha^{p^n-2}) \tag{3}$$

Because α is of multiplicity greater than 1, we should see $g(x) := x(x^{p^n-2} + \alpha x^{p^n-3} + \alpha^2 x^{p^n-4} + \cdots + \alpha^{p^n-2}) = \frac{f(x)}{(x-\alpha)}$, satisfy $g(\alpha) = 0$. Yet, if we actually calculate $g(\alpha) = (p^n - 1) \cdot \alpha(\alpha^{p^n-2}) = (p^n - 1) = \alpha^{p^n-1} = (p^n - 1) \cdot 1 = -1$, we will see CaC.

■

Theorem 6. *The zeros in $\overline{\mathbb{Z}_p}$ of the polynomial $x^{p^n} - x \in \mathbb{Z}_p[x]$ constitute a field of order p^n*

Proof.

$$K := \{x \in \overline{\mathbb{Z}_p} | x^{p^n} - x = 0\} \tag{4}$$

By Lemma 5, we know $|K| = p^n$, so it only remains to show that K is a sub-field.

Arbitrarily pick $\alpha, \beta \in K$, and observe

$$(\alpha+\beta)^p = \alpha^p + \binom{p}{1} \cdot \alpha^{p-1}\beta + \cdots + \binom{p}{1} \cdot \alpha\beta^{p-1} + \beta^p \tag{5}$$

Notice that the $\overline{\mathbb{Z}_p}$ is an extension of $\mathbb{Z}_p$, which means, the 1 in $\overline{\mathbb{Z}_p}$ is exactly the 1 in $\mathbb{Z}_p$. The enable us to deduce that $\overline{\mathbb{Z}_p}$ is of characteristic p by observing $p \cdot 1 = 0 \in \overline{\mathbb{Z}_p}$. Notice that $\forall 1 \leq x < p, p | \binom{p}{x}$, so we deduce

$$(\alpha+\beta)^p = \alpha^p + \beta^p \tag{6}$$

We now use induction to show that $\alpha + \beta \in K$. Suppose $(\alpha+\beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$, which is true when $m = 1$. Observe

$$(\alpha+\beta)^{p^{m+1}} = [(\alpha+\beta)^{p^m}]^p = (\alpha^{p^m} + \beta^{p^m})^p \tag{7}$$

$$= \alpha^{p^{m+1}} + \binom{p}{1} \cdot (\alpha^{p^m})^{p-1}\beta^{p^m} + \cdots + \binom{p}{1} \cdot \alpha^{p^m}(\beta^{p^m})^{p-1} + \beta^{p^{m+1}} = \alpha^{p^{m+1}} + \beta^{p^{m+1}} \tag{8}$$

■

and observe

$$(\alpha+\beta)^{p^n}-(\alpha+\beta)=\alpha^{p^n}-\alpha+\beta^{p^n}-\beta=0 \text{ (done)} \tag{9}$$

Notice that because $\alpha,\beta\in K$, so we know $\alpha^{p^n}=\alpha$ and $\beta^{p^n}=\beta$. Then $(\alpha\beta)^{p^n}-\alpha\beta=\alpha^{p^n}\beta^{p^n}-\alpha\beta=\alpha\beta-\alpha\beta=0$. In other words, $\alpha\beta\in K$. It remains to show $-\alpha\in K$ and $\alpha^{-1}\in K$. Observe

$$(-\alpha)^{p^n}-(-\alpha)=-(\alpha^{p^n}-\alpha)=0 \text{ if } p>2 \tag{10}$$

$$(-\alpha)^{2^n}-(-\alpha)=\alpha^{2^n}+\alpha \underset{\alpha}{\overset{2^n}{=}} -\alpha=0 \text{ because } \overline{\mathbb{Z}_2} \text{ is of characteristic } 2 \tag{11}$$

(done)

$$\alpha^{p^n}=\alpha \implies \alpha^{-p^n}-\alpha^{-1} \implies (\alpha^{-1})^{p^n}-\alpha^{-1}=0 \text{ (done)} \tag{12}$$

Part (C): Uniqueness

Theorem 7. *For all prime power $x=p^n$, there is only one finite field of order x.*

Proof. Suppose $\mathbb{E},\mathbb{F}$ are two field of order p^n. Here, we denote $\mathbb{E}'=\{m\cdot 1_{\mathbb{E}}|m\in\mathbb{Z}\}$ and $\mathbb{F}'=\{m\cdot 1_{\mathbb{F}}|m\in\mathbb{Z}\}$, where $1_{\mathbb{E}}$ and $1_{\mathbb{F}}$ stands for the unity of $\mathbb{E}$ and $\mathbb{F}$.

Because $\langle\mathbb{E}^*,*\rangle$ and $\langle\mathbb{F}^*,*\rangle$ are cyclic, we know there exists $\alpha\in\mathbb{E}^*,\beta\in\mathbb{F}^*$, such that $\langle\mathbb{E}^*,*\rangle=\langle\alpha\rangle$ and $\langle\mathbb{F}^*,*\rangle=\langle\beta\rangle$. This enable us to deduce $\mathbb{E}=\mathbb{E}'(\alpha)$ and $\mathbb{F}=\mathbb{F}'(\beta)$. Denote $\text{irr}\langle\alpha,\mathbb{E}'\rangle$ by $f(x)\in\mathbb{E}'[x]$, and denote $\text{irr}\langle\beta,\mathbb{F}'\rangle$ by $g(x)\in\mathbb{F}'[x]$. We will complete the proof by showing

$$\mathbb{E}=\mathbb{E}'(\alpha)\simeq\mathbb{E}'[x]/\langle f(x)\rangle\simeq\mathbb{F}'[x]/\langle g(x)\rangle\simeq\mathbb{F}'(\beta)=\mathbb{F} \tag{13}$$

Let $\phi:\mathbb{E}'[x]/\langle f(x)\rangle\to\mathbb{E}'(\alpha)$ be defined by $\langle f(x)\rangle+p(x)\mapsto p(\alpha)$. We first show ϕ is an isomorphism. Then the symmetric part of proof about $\mathbb{F}$ can be done in exactly same fashion. For abbreviation, we denote $\langle f(x)\rangle+p(x)$ by $[p(x)]$, and so forth. The following two equations finish the work of showing ϕ is a homomorphism.

$$\phi([p(x)])+\phi([q(x)])=p(\alpha)+q(\alpha)=(p+q)(\alpha)=\phi([(p+q)(x)]) \tag{14}$$

$$\phi([p(x)])\phi([q(x)])=p(\alpha)q(\alpha)=(pq)(\alpha)=\phi([(pq)(x)]) \tag{15}$$

ϕ is onto, since every element y in $\mathbb{E}'(\alpha)$ is an output of a polynomial $r(x)\in\mathbb{E}'[x]$ with input α, so we know $\phi([r(x)])=y$.

To see ϕ is one-to-one, observe

$$\phi([p(x)])=\phi([q(x)]) \implies (p-q)(\alpha)=0 \tag{16}$$

Because $f(x)=\text{irr}\langle\alpha,\mathbb{E}'\rangle$ is the smallest polynomial in $\mathbb{E}'[x]$ that send α to 0, we know $f(x)|(p-q)(x)$. This indicates $(p-q)(x)\in\langle f(x)\rangle$, which shows

$\langle f(x)\rangle + p(x) = \langle f(x)\rangle + q(x)$. (done)

Notice that because $\mathbb{E}' \simeq \mathbb{F}'$, one can easily deduce $\mathbb{E}'[x] \simeq \mathbb{F}'[x]$. Let $\psi : \mathbb{E}'[x]/\langle f(x)\rangle \to \mathbb{F}'[x]/\langle g(x)\rangle$ be defined by $\langle f(x)\rangle + p(x) \mapsto \langle g(x)\rangle + \mu(p)(x)$ where μ is an isomorphism from $\mathbb{E}'[x]$ to $\mathbb{F}'[x]$. We now show ψ is an isomorphism. Again we use $[p(x)]$ to denote $\langle f(x)\rangle + p(x)$ and use $[r(x)]_{\mathbb{F}}$ to denote $\langle g(x)\rangle + r(x)$

$$\psi([p(x)]) + \psi([q(x)]) = [(\mu(p))(x)]_{\mathbb{F}} + [(\mu(q)(x))]_{\mathbb{F}} \tag{17}$$
$$= [(\mu(p) + \mu(q))(x)]_{\mathbb{F}} = [\mu(p+q)(x)]_{\mathbb{F}} \tag{18}$$
$$= \psi([(p+q)(x)]) = \psi([p(x)] + [q(x)]) \tag{19}$$
$$\psi([p(x)])\psi([q(x)]) = [(\mu(p))(x)]_{\mathbb{F}}[(\mu(q)(x))]_{\mathbb{F}} \tag{20}$$
$$= [(\mu(p)\mu(q))(x)]_{\mathbb{F}} = [\mu(pq)(x)]_{\mathbb{F}} \tag{21}$$
$$= \psi([(pq)(x)]) = \psi([p(x)][q(x)]) \tag{22}$$

The above two equations show that ψ is a homomorphism. Notice that we have known $\mathbb{E}'[x]/\langle f(x)\rangle \simeq \mathbb{E}$ and $\mathbb{F}'[x]/\langle g(x)\rangle \simeq \mathbb{F}$, where $\mathbb{E}$ and $\mathbb{F}$ are of the same order, so to show ψ is an isomorphism, it only remains to show that ψ is onto.

This is actually obvious if we strips off layers of isomorphism. For all $\langle g(x)\rangle + r(x) \in \mathbb{F}'[x]/\langle g(x)\rangle$, because $r(x) \in \mathbb{F}'[x]$ and μ is an isomorphism from $\mathbb{E}'[x]$ to $\mathbb{F}'[x]$, we know there exists $d(x) \in \mathbb{E}'[x]$ such that $\mu(d(x)) = r(x)$. Then we can simply pick $\psi(\langle f(x)\rangle + d(x)) = \langle g(x)\rangle + (\mu(d))(x) = \langle g(x)\rangle + r(x)$. (done)

■