continued

Finite Fields,

Jiang-Hua Lu

The University of Hong Kong

MATH4302, Algebra II

Monday April 14, 2025

In this file:

1. §3.2.6 : Finite fields , continued

On Thursday, April 10, 2025, we proved

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 $\mathbb{F}_{p^n}$. $x^{p^n} - x$
2. For each $n \geq 1$ and for each $d|n$, there is exactly one sub-field of $\mathbb{F}_{p^n}$ which is $\mathbb{F}_{p^d}$. $x^{p^d} - x$

Today

3. A "description" of all irreducible polynomials over $\mathbb{F}_p$ for every prime p. $x^{p^n} - x \in \mathbb{F}_p[x]$

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.

This shows 1)

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 $q | f_n$. This proves 2)
- 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 $q | f_n$. This proves 3)

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.

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

For any comm. ring R of characteristic p,

consider $\sigma : R \to R$, $\sigma(a) = a^p$

$\sigma(a+b) = \sigma(a) + \sigma(b)$ $\quad \sigma(ab) = \sigma(a)\sigma(b)$

$L = \mathbb{F}_{p^n}$ $\quad \sigma(a) = a^p \quad \sigma^2(a) = a^{p^2}$

$\sigma^n(a) = a^{p^n} = a \quad \sigma^n = Id$

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.

So $\sigma \in Aut_{\mathbb{F}_p}(L)$, ie $\sigma : L \to L$ isom

and $\sigma|_{\mathbb{F}_p} = Id_{\mathbb{F}_p}$

$(a^p = a \quad \forall a \in \mathbb{F}_p)$

$(a^{p-1} = 1 \quad \forall a \in \mathbb{F}_p \setminus \{0\})$

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 $f(t), g(t) \in \mathbb{F}_2[t]$.

$$\left(\frac{f(t)}{g(t)}\right)^p = t$$

- 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.

Question: For prime p and integer n,

let $\mathcal{I}_{p,n}$ = the set of all irred. poly ~~over~~ in $\mathbb{F}_p[x]$ of deg n.

What is $|\mathcal{I}_{p,n}| = i_{p,n}$

What structure does it have?

$\tau: \mathbb{F}_p[x] \longrightarrow \mathbb{F}_p[x]: f(x) \longmapsto f(x+1)$

If $P_1, P_2 \in \mathcal{I}_{p,n}$, $\mathbb{F}_p[x]/\langle P_1(x)\rangle \simeq \mathbb{F}_p[x]/\langle P_2(x)\rangle$