MATH4302, Algebra II, 2022

Jiang-Hua Lu

The University of Hong Kong

Monday April 11, 2022

Today

1. §2.2.6 : Finite fields, II (leftover from last time)
2. §2.2.7: Separable polynomials and perfect fields
3. §2.2.8: Separable extensions and the Primitive Element Theorem
4. §3.1.1: Automorphism groups and roots of polynomials

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

Lemma. For any $n \geq 1$,

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

Proof.

$\mathbb{F}_{p^n} \setminus \{0\}$ is a cyclic group, has a generator α

- 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.

So (1) ✓

If F is any finite field with m elts, then $\forall\ \alpha \in F$, $\alpha^m = \alpha$

$\alpha^{m-1} = 1$ when $\alpha \neq 0$

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 $= m$ elements;
- The element $a = \bar{x} \in L$ satisfies $f_n(a) = 0$, so $q | f_n$. $a^{p^n} = a$ so 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 $q|f_n$.

By ②

Q.E.D.

Consider the factorization

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

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 $d_j = \deg(q_j)$, $j = 1, 2, \cdots, l$.
- 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 $\boxed{\mathbb{F}_p(a)}$ is a subfield of $\mathbb{F}_{p^n}$ with p^{d_j} elements;
- By results on subfields of $\mathbb{F}_{p^n}$, must have $d_j | n$.

$\mathbb{F}_p(a) \cong \mathbb{F}_p[x]/\langle q_j \rangle$

We have thus proved the following Theorem on the polynomial

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

p prime
$n \geq 1$

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 irreducible polynomial appears exactly once in the prime factorization of $f_n(x)$.

$N_{p,n}$ = # of monic irred. poly. in $\mathbb{F}_p[x]$ of deg n

Examples. In $\mathbb{F}_2[x]$, one has $p=2$

$$x^2 - x = x(x-1),$$
$$x^4 - x = x(x-1)(x^2+x+1),$$
$$x^8 - x = x(x-1)(x^3+x+1)(x^3+x^2+1),$$
$$x^{16} - x = x(x-1)(x^2+x+1)(x^4+x+1)$$
$$(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

$n=4$
$d \in \{1,2,4\}$

$N_{2,4} = 3$
$N_{2,1} = 2$
$N_{2,2} = 1$

The Frobenius homomorphism:

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

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

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

Pf: $\sigma(a+b) = \sigma(a) + \sigma(b)$: $(a+b)^p = a^p + b^p$

$\sigma(ab) = \sigma(a)\sigma(b)$: $(ab)^p = a^p b^p$

//

$\mathrm{char}(L) = p > 0$

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

Pf: Since $\sigma: L \to L$ is injective

$|\sigma(L)| = |L|$, $\boxed{\sigma(L) \subset L}$

so $\sigma(L) = L$

ie σ is surjective.

Thus σ is an isomorphism, ie an automorphism

Thus every $\alpha \in L$ is of the form β^p for some $b \in L$.

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

Eg: In $\mathbb{F}_{29}$, $27 = \alpha^{29}$ for some $\alpha \in \mathbb{F}_{29}$

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

$\mathbb{F}_p(t)$

$\|$

$\left\{ \frac{f(t)}{g(t)} : f, g \in \mathbb{F}_p[t] \right\}$

$t \in \mathbb{F}_p(t)$

$\exists ?\ \alpha = \frac{f(t)}{g(t)} \in L$ s.t.

$\alpha^p = \frac{f(t)^p}{g(t)^p} \overset{?}{=} t$

$\iff f(t)^p = t\, g(t)^p \quad (*)$

let $m = \deg f$, $n = \deg g$

Answer: No.

$(*) \Rightarrow mp = 1 + np$ not possible

§2.2.7: Separable polynomials and perfect fields

Definition. For a field K, a polynomial $f(x) \in K[x]$ is said to be separable over K if it has no repeated roots in its splitting field over K.

Example. $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ is separable over $\mathbb{Q}$, but not when regarded as a polynomial over $\mathbb{F}_3$:

$$f(x) = (x-2)^3 \in \mathbb{F}_3[x].$$

Example. $K = \mathbb{F}_2(t)$ and $f(x) = x^2 - t \in K[x]$. The splitting field of $L = K(\sqrt{t})$ of f over K has degree 2 over K, but

$$f(x) = x^2 - t = (x - \sqrt{t})^2 \in L[x],$$

so f is not separable. over $K = \mathbb{F}_2(t)$.