Intro to Algebra 2 W5-2

fat

March 22, 2024

Definition 1. A field F is said to be **perfect** if every irreducible polynomial in $F[x]$ is separable.

Example 1. If char $F = 0$ or $|F| < \infty$, then F is perfect.

Theorem 1. Let p be a prime. For each positive integer $n, \exists$ a finite field of p^n elements. It is unique up to isomorphism. More precisely, if we let

$$\mathbb{F} := \{\text{roots of } x^{p^n} - x \in \mathbb{F}_p[x] \text{ in } \overline{\mathbb{F}_p}\}$$

Then $\mathbb{F}$ is a field of p^n elements.

Proof.

We first prove that $|\mathbb{F}| = p^n$, i.e. the polynomial $x^{p^n} - x$ has no repeated roots.(i.e. $x^{p^n} - x$ is separble.) We have

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

$\Rightarrow (x^{p^n} - x, \mathrm{D}(x^{p^n} - x)) = 1$. By Prop 33, $x^{p^n} - x$ has no repeated roots (separable). We now show that $\mathbb{F}$ is a field. It suffices to show that

(1) $\forall \alpha, \beta \in \mathbb{F}, \alpha - \beta \in \mathbb{F}$.

(2) $\forall \alpha, \beta \in \mathbb{F}, \beta \neq 0, \alpha/\beta \in \mathbb{F}$.

Suppose $\alpha, \beta \in \mathbb{F}$,

$$(\alpha - \beta)^{p^n} - (\alpha - \beta) = (\alpha^p - \beta^p)^{p^{n-1}} - (\alpha - \beta) = \cdots = \alpha^{p^n} - \beta^{p^n} - (\alpha - \beta)$$

$$= (\alpha^{p^n} - \alpha) - (\beta^{p^n} - \beta) = 0$$

since $\alpha, \beta \in \mathbb{F}$ are roots of $x^{p^n} - x$. Also, if $\alpha, \beta \neq 0 \in \mathbb{F}$, then

$$\left(\frac{\alpha}{\beta}\right)^{p^n} - \frac{\alpha}{\beta} = \frac{\alpha^{p^n}}{\beta^{p^n}} - \frac{\alpha}{\beta} = \frac{\alpha}{\beta} - \frac{\alpha}{\beta} = 0$$

$\Rightarrow \alpha/\beta \in \mathbb{F}$.

Now suppose that E is another field of p^n elements. Since $|E^\times| = p^n - 1$, we have $\alpha^{p^n-1} = 1 \ \forall \alpha \in E^\times$. $\forall \alpha \in E, \alpha^{p^n} - \alpha = \alpha(\alpha^{p^n-1} - 1) = 0$. i.e. every element of E is a root of $x^{p^n} - x$. Since $|E| = p^n = \deg(x^{p^n} - x)$, we find $x^{p^n} - x$ splits completely in $E[x]$. Therefore E is a splitting field for $x^{p^n} - x$, since $E, \mathbb{F}$ are both splitting fields for $x^{p^n} - x$. By Corollary 28, $E \simeq \mathbb{F}$. $\square$

Notation: We let $\mathbb{F}_{p^n}$ denote the field of p^n elements.

Proposition 1 (Proposition 38)**.** Let $p(x)$ be an irreducible polynomial over a field of char p. Then $\exists$ a unique integer $k \geq 0$ and a unique separable irreducible polynomial $p_{\text{sep}}(x) \in F[x]$ such that

$$p(x) = p_{\text{sep}}(x^{p^k})$$

Proof.

If $p(x)$ is separable, we let $k = 0$ and $p_{\text{sep}} = p$. If not, by a corollary earlier, $p(x) = p_1(x^p)$ for some $p_1(x) \in F[x]$. It's clear that p_1 is irreducible in $F[x]$. If p_1 is separable, we let $k = 1, p_{\text{sep}} = p_1$ and we are done. If not, then $p_1(x) = p_2(x^p)$ for some $p_2(x) \in F[x]$ and hence $p(x) = p_2(x^{p^2})$. Continuing this way, we see that $\exists k \geq 0, p_{\text{sep}}(x) \in F[x]$ such that $p(x) = p_{\text{sep}}(x^{p^n})$. $\square$

Remark 1. Let $p(x), k, p_{\text{sep}}(x)$ be given as in Prop 38. Then the number of distinct roots of $p(x) = \#$ of roots of $p_{\text{sep}}(x) = \deg p_{\text{sep}}(x)$. To see this, say $\alpha_1, ..., \alpha_d$ are the roots of $p_{\text{sep}}(x)$ in $\bar{F}$, where $d = \deg p_{\text{sep}}(x)$

$$\Rightarrow p_{\text{sep}}(x) = (x - \alpha_1) \cdots (x - \alpha_d)$$

$$\Rightarrow p(x) = (x^{p^k} - \alpha_1) \cdots (x^{p^k} - \alpha_d)$$

Let $\beta_j \in \bar{F}$ be elements such tthat $\beta_j^{p^k} = \alpha_j$. Then

$$p(x) = (x^{p^k} - \beta_1^{p^k}) \cdots (x^{p^k} - \beta_d^{p^k})$$

$$= (x - \beta_1)^{p^k} \cdots (x - \beta_d)^{p^k}$$

$\Rightarrow$ The number of distinct roots of $p(x)$ in $\bar{F}$ is $d = \deg p_{\text{sep}}(x)$.

Definition 2. We define the **separable degree** of p to be $\deg p_{\text{sep}}(x)$ and is denoted by $\deg_s p(x)$. The integer p^k is called the **inseparable degree** of $p(x)$ and is denoted by $\deg_i p(x)$.

Definition 3. An algebraic extension K/F is said to be **separable** if $\forall \alpha \in K, m_{\alpha,F}(x)$ is separable.

Remark 2. If F is perfect, then every algebraic extension of F is separable.

13.6 Cyclomotic Polynomials and Extensions

Notation: Let $\zeta_n = e^{2\pi i/n}$ and $\mu_n = \{n\text{th roots of unity}\} = \{1, \zeta_n, ...\zeta_n^{n-1}\}$.

Definition 4. We say $\zeta \in \mu_n$ is **primitive** if $\langle \tau \rangle = \mu_n$, i.e. if $\zeta = \zeta_n^k$ where $(k, n) = 1$.

Definition 5. The nth **cycclotomic polynomial** $\Phi_n(x)$ is defined to be

$$\Phi_n(x) := \prod_{\zeta \in \mu_n, \zeta \text{ primitive}} (x - \zeta) = \prod_{k=1,(k,n)=1}^{n} (x - \zeta_n^k)$$

Lemma 1 (Lemma 40)**.** $\Phi_n(x) \in \mathbb{Z}[x]$ and is monic.

Proof.

Note that

$$x^n - 1 = \prod_{\zeta \in \mu_n} (x - \zeta)$$

Since $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$,

$$= \prod_{d|n} \prod_{\zeta \in \mu_n \text{ has order } d} (x - \zeta) = \prod_{d|n} \Phi_d(x)$$

We now prove by induction on n.

$$n - 1 \Rightarrow \Phi_1(x) = x - 1$$

Assume the statement holds until $n-1$. Now

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)} \in \mathbb{Z}[x]$$

where the above fraction polynomial is in $\mathbb{Z}[x]$ because both the numerator and the denominator are monic. $\square$

Theorem 2 (Theorem 41)**.** $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ and $\deg \Phi_n(x) = \varphi(n)$ where $\varphi(n)$ is the Euler phi function.

Proof.

Let $f(x) = m_{\zeta_n, \mathbb{Q}}(x)$. Then $f(x)|\Phi_n(x)$. We'll show that $f(x) = \Phi_n(x)$. This implies $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. Proving "$f(x) = \Phi_n(x)$" $\Leftrightarrow$ "$\forall k$ such that $(k,n) = 1$, $f(\zeta_n^k) = 0$". So it suffices to show that $\forall k, (k,n) = 1$, $f(\zeta_n^k) = 0$. ($\forall$ primitive nth roots ζ of unity, $f(\zeta) = 0$.)

We first prove the case $k = p$ is a prime. Write $\Phi_n(x) = f(x)g(x)$. (By Gauss's lemma, $f, g \in \mathbb{Z}[x]$.) We have

$$\Phi_n(\zeta_n^p) = 0$$

Suppose that $f(\zeta_n^p) \neq 0$, then $g(\zeta_n^p) = 0$. $\Rightarrow \zeta_n$ is a root of $g(x^p)$. $\Rightarrow f(x)|g(x^p)$. Say $g(x^p) = f(x)h(x)$. Now consider the reduction modulo p. Say $g(x) = a_m x^m + \cdots + a_n$. Since $\overline{a_m}^p = \overline{a_m}$ $\forall a_m \in \mathbb{Z}$.($\overline{a_n}$ = residue class of a_n modulo p.) We have

$$\overline{g(x^p)} = \overline{a_m} x^{pm} + \cdots + \overline{a_0}$$

$$= \overline{a_m} x^{pm} + \cdots \overline{a_0}^p$$

$$= (\overline{a_m} x^m + \cdots + \overline{a_0})^p = \overline{g(x)}^p$$

Therefore

$$\overline{g(x)}^p = \overline{f(x)h(x)}$$

Since $(\mathbb{Z}/p\mathbb{Z})[x]$ is a UFD, this implies that $GCD(\overline{f(x)}, \overline{g(x)}) \neq 1$. $\Rightarrow \overline{\Phi_n(x)} = \overline{f(x)g(x)}$ has a repeated root. However we can show that $\overline{\Phi_n(x)}$ has no repeated roots (which will be proved below). This yields a contradiction. Thus we must have $f(\zeta_n^p) = 0$.

We will now show the claim. We'll show that $\overline{x^n - 1}$ has no repeated roots. Then since $\overline{\Phi_n(x)} | \overline{x_n - 1}, \overline{\Phi_n(x)}$ does not have a repeated root either. Here $\mathrm{D}(\overline{x^n - 1}) = \overline{nx^{n-1}}$. Since $p \not| n, \bar{n} \neq \bar{0}$. We have

$$\overline{x^n - 1} = (\overline{n^{-1}x})\mathrm{D}(\overline{x^n - 1}) - 1$$

$$\Rightarrow (\overline{x^n - 1}, \mathrm{D}(\overline{x^n - 1})) = 1$$

$\Rightarrow \overline{\Phi_n(x)}$ has no repeated roots. $\square$