13.6

Cyclotomic Polynomials AND Extensions

$$\begin{pmatrix} 4a & b \\ b & c \end{pmatrix}$$

Discriterminant

Cyclotomic Polynomials & Extensions

※ Purpose of the section: prove the cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ generated by the nth roots of unity is of degree $\varphi(n)$.

Def. Let μ_n denote the group of nth roots of unity over $\mathbb{Q}$.

※ Some properties of μ_n:

① If $d|n$ & ζ is a dth root of unity, then ζ is also an nth root of unity. Hence $\mu_d \subseteq \mu_n$ for $d|n$.

② Conversely, if ζ is an nth root of unity which is also a dth root of unity, then $d|n$.

Def. (cyclotomic polynomials)

The nth cyclotomic polynomial $\Phi_n(x)$ is the polynomial whose roots are the primitive nth roots of unity:

$$\Phi_n(x) = \prod_{\substack{\zeta \in \mu_n \\ \zeta \text{ is primitive}}} (x-\zeta)$$

※ Properties of $\Phi_n(x)$.

$\boxed{\text{Derivation}}$ The roots of the polynomial x^n-1 are precisely the nth roots of unity:

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

If we group the nth roots of unity by their orders (e.g. $|\zeta| = d$ if and only if ζ is a primitive dth root of unity), we get

$$x^n-1 = \prod_{d|n} \prod_{\substack{\zeta^d=1, \\ \zeta \text{ primitive}}} (x-\zeta).$$

The inner product is $\Phi_d(x)$, so

$$x^n-1 = \prod_{d|n} \Phi_d(x).$$

Comparing degrees gives us $n = \sum_{d|n} \varphi(d)$. This allows us to compute $\Phi_n(x)$

for any n recursively.

#1 Lemma (Properties of $\Phi_n(x)$)

The cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Proof. It is clear that $\Phi_n(x)$ is monic and of degree $\varphi(n)$. We only need to show that the coefficients of Φ_n lie in $\mathbb{Z}$.

(Induction)

① Base case: the statement is true for $n=1$ since $\Phi_1(x) = x-1$.

② Inductive Hypothesis: Suppose that the statement is true for $1 \le d < n$. Then $x^n - 1 = f(x)\,\Phi_n(x)$ where $f(x) = \prod_{\substack{d|n,\\ d<n}} \Phi_d(x) \in \mathbb{Z}[x]$. There's some algebra additions here, but it should be pretty easy to see that $\Phi_n(x) \in \mathbb{Z}[x]$.

#1 Th. The cyclotomic polynomial $\Phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Proof. We only need to show that $\Phi_n(x)$ is irreducible over $\mathbb{Z}$.

Suppose $\Phi_n(x) = f(x)g(x)$ with $f(x), g(x)$ monic in $\mathbb{Z}[x]$. Let ζ be any root of $\Phi_n(x)$ and $f(x)$ is the minimal polynomial of ζ over $\mathbb{Z}$. Let p be a prime not dividing n. Then ζ^p is a primitive nth root of unity, and therefore is a root of either $f(x)$ or $g(x)$.

$\boxed{\text{Case \#1}}$ $g(\zeta^p)=0$. Then ζ is a root of $g(x^p)$. Since $f(x)$ is the minimal polynomial of ζ, $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$:

$$g(x^p) = f(x)\,h(x) \quad \text{for some } h(x) \in \mathbb{Z}[x].$$

Reduce this equation mod p: $\bar{g}(x^p) = \bar{f}(x)\,\bar{h}(x)$ in $\mathbb{F}_p$.

Since $\bar{g}(x^p) = (\bar{g}(x))^p$ (as seen in 13.5),

$$(\bar{g}(x))^p = \bar{f}(x)\,\bar{h}(x) \quad \text{in } \mathbb{F}_p.$$

Therefore $\bar{g}(x)$ and $\bar{f}(x)$ have a factor in common in $\mathbb{F}_p[x]$.

Return to $\Phi_n(x) = f(x)g(x)$ and reduce the equation mod p:

$$\bar{\Phi}_n(x) = \bar{f}(x)\,\bar{g}(x) \quad \text{in } \mathbb{F}_p[x]$$

Now $\bar{f}(x)$ and $\bar{g}(x)$ shares a factor in $\mathbb{F}_p[x]$, so $\bar{\Phi}_n(x)$ has a multiple root in $\mathbb{F}_p[x]$, contradicting the separability of $x^n - 1$.

$\Rightarrow$ This case is invalid.

$\boxed{\text{Case \#2.}}$ $f(\zeta^p) = 0$. Since this applies to every root ζ of $f(x)$, it is clear that every primitive nth root of unity is a root of $f(x)$, so $\Phi_n(x) = f(x)$.

#1 Cor. (Degree of extension over $\mathbb{Q}$)

The degree over $\mathbb{Q}$ of the cyclotomic field of nth roots of unity is $\varphi(n)$:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

Proof: The minimal polynomial of any primitive nth root of unity is $\Phi_n(x)$ with degree $\varphi(n)$. Since the primitive nth roots of unity generate the nth roots of unity, $\mathbb{Q}$ adjoined the primitive nth roots of unity is $\mathbb{Q}$ adjoined all the nth roots of unity.