1.6 Lecture 6: Cyclotomic polynomials and cyclotomic extensions

Let n be a positive integer.

- A **primitive** n**th root of unity** is an element $\omega \in \mathbb{C}$ such that $\omega^n = 1$ and if $m \in \mathbb{Z}_{>0}$ and $m < n$ then $\omega^m \neq 1$.
- The n**th cyclotomic polynomial** is

$$\Phi_n(x) = \prod_{\omega} (x - \omega), \qquad \text{where the product is over the primitive } n\text{th roots of unity in } \mathbb{C}.$$

- The **Euler** ϕ**-function** is $\phi\colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ given by

$$\phi(n) = \deg(\Phi_n(x)).$$

Since the roots of unity are the primitive dth roots of unity for the positive integers d dividing n then

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

HW: Use this formula, and induction on n, to show that $\Phi_n(x) \in \mathbb{Q}[x]$.

HW: Show that $\Phi_n(x) = m_{\omega,\mathbb{Q}}(x)$, where $\omega = e^{\frac{2\pi i}{n}}$.

HW: Let $\omega = e^{\frac{2\pi i}{n}}$. Show that $\mathbb{Q}(\omega)$ is the splitting field of $\Phi_n(x)$ over $\mathbb{Q}$.

HW: Show that $\Phi_n(x)$ is irreduciible in $\mathbb{Q}[x]$.

HW:. Let $\omega = e^{\frac{2\pi i}{n}}$. Show that $\mathbb{Q}(\omega) \supseteq \mathbb{Q}$ is a Galois extension.

HW: Let $\omega = e^{\frac{2\pi i}{n}}$. Show that $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega))| = \phi(n)$.

HW: Let $\omega = e^{\frac{2\pi i}{n}}$. Show that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$.

Theorem 1.12. *Let* $n \in \mathbb{Z}_{>0}$.

(a) $\Phi_n(x) \in \mathbb{Z}[x]$ *and* $\Phi_n(x)$ *is irreducible in* $\mathbb{Z}[x]$.

(b) $\phi(n) = \deg(\Phi_n(x)) = \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^{\times}) = ($*the number of primitive* n*th roots of unity*$)$.

Theorem 1.13. *Let* ω *be a primitive* n*th root of unity. Then*

$$\mathbb{Q}(\omega) \textit{ is the splitting field of } f(x) = x^n - 1 \textit{ over } \mathbb{Q},$$

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) \cong (\mathbb{Z}/n\mathbb{Z})^{\times} \qquad \textit{and} \qquad \mathrm{Card}((\mathbb{Z}/n\mathbb{Z})^{\times}) = \phi(n).$$