6.11 Finite fields

Theorem 6.21.

(a) The function

$$\begin{array}{ccc} \{\textit{finite fields}\} & \longrightarrow & \{p^k \mid p \in \mathbb{Z}_{>0} \textit{ is prime, } k \in \mathbb{Z}_{>0}\} \\ \mathbb{F} & \longmapsto & \mathrm{Card}(\mathbb{F}) \end{array} \qquad \textit{is a bijection.}$$

(b) The finite field $\mathbb{F}_{p^k}$ with p^k elements is given by

$$\mathbb{F}_{p^k} \textit{ is the extension of } \mathbb{F}_p \textit{ of degree } k, \qquad \mathbb{F}_{p^k} = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^k} - \alpha = 0\}, \qquad \mathbb{F}_{p^k} = (\overline{\mathbb{F}_p})^{F^k},$$

where $F\colon \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ is the Frobenius map.

6.12 Cyclotomic polynomials

Let n be a positive integer.

- A **primitive nth 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 $\omega^m = 1$.
- The **nth 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

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

Theorem 6.22. *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 nth roots of unity).

Theorem 6.23. *Let ω be a primitive nth root of unity. Then $\mathbb{Q}(\omega)$ is the splitting field of $\{x^n - 1\}$,*

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