## 1 Cyclotomic Polynomials

**Theorem 1.1.** For prime p, we have  $x^p - 1 = (x - 1)(x^{p-1} + \dots + 1)$  and  $\mu_{\varepsilon_p}^{\mathbb{Q}} = x^{p-1} + \dots + 1$ .

**Definition 1**  $(n^{\text{th}} \text{ cyclotomic polynomial}).$ 

$$\Phi_n(x) = \prod_{\substack{\varepsilon \in \sqrt[n]{1} \\ |\varepsilon| = n}} (x - \varepsilon) = \frac{x^n - 1}{\prod_{\substack{d \mid n, d < n}} \Phi_d(x)}$$

**Theorem 1.2.**  $\Phi_n$  is irreducible over  $\mathbb{Q}$ .

Corollary 1. (a)  $[\mathbb{Q}(\exp(\frac{2\pi i}{n})):\mathbb{Q}] = \varphi(n)$  (where  $\varphi$  is Euler's totient function);

- (b)  $\left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right):\mathbb{Q}\right]=\frac{1}{2}\varphi(n)$ . Furthermore, all algebraic conjugates of  $\cos\frac{2\pi}{n}$  are  $\cos\frac{2\pi k}{n}$  for  $\gcd(k,n)=1$ .
- (c) Let  $c = \frac{a+bi}{a-bi} \in \sqrt[\infty]{1}$ , where  $a,b \in \mathbb{Z}$ . Then  $c \in \{\pm i,\pm 1\}$

**Lemma 1.3.** Let  $\mathbb{F}$  be a finite field. Then  $\mathbb{F}^{\times} = \mathbb{F} \setminus \{0\}$  is a cyclic group.