Theorem 14.5. Let U be a finite subgroup of the multiplicative group $F^* = F \setminus \{0\}$ of F. Then U is cyclic.

Proof. Let $|U| = n$. Let d be a divisor of n and set

$$O_d = \{u \in U \mid o(u) = d\},$$
$$X_d = \{u \in U \mid u^d = 1\}.$$

Clearly $O_d \subseteq X_d$ and $|X_d| \leq d$ since $x^d - 1 \in F[x]$ has at most d roots. Assume $\exists y \in O_d$. Then $y^d = 1$ and so $(y^i)^d = (y^d)^i = 1$. In particular $\langle y \rangle \subseteq X_d$. Since $o(y) = d$, the elements $1, y, y^2, \ldots, y^{d-1}$ are distinct, and so $|\langle y \rangle| = d$. Then

$$d = |\langle y \rangle| \leq |X_d| \leq d$$

implies $\langle y \rangle = X_d \cong \mathbb{Z}_d$ via the isomorphism

$$\langle y \rangle \longrightarrow \mathbb{Z}_d$$
$$y^i \longmapsto i \pmod{d}.$$

If $x \in O_d \setminus \{y\}$, then $\langle x \rangle = X_d = \langle y \rangle$. Hence O_d is the set of all generators of $\langle y \rangle$ and so by Proposition 14.4(1) we have (under our assumption that $\exists y \in O_d$) that

$$O_d = \{y^k \mid 1 \leq k \leq d, \gcd(k, d) = 1\}.$$

By Proposition 14.4(2) we conclude that if $O_d \neq \emptyset$, then $|O_d| = \varphi(d)$. Hence $|O_d| \leq \varphi(d)$. Using this and Proposition 14.4(3) we obtain

$$n = |U| = \sum_{d \mid n} |O_d| \leq \sum_{d \mid n} \varphi(d) = n,$$

and so $\sum_{d \mid n} |O_d| = \sum_{d \mid n} \varphi(d)$ which gives $|O_d| = \varphi(d)$ for every $d \mid n$. Then $O_n \neq \emptyset$ and so there exists $u \in U$ with $o(u) = n$, that is, $\langle u \rangle = U$. □

Corollary 14.6. The set $\{x \in F \mid x^n - 1 = 0\} \subseteq F$ is a cyclic group.

Proof. The set $\{x \in F \mid x^n - 1 = 0\}$ has at most n elements and is nonempty since it contains 1. Moreover, if $\alpha^n = 1$ and $\beta^n = 1$,

then $(\alpha\beta)^n = \alpha^n\beta^n = 1$. The claim follows by Theorem 14.5.

Theorem 14.7. Let $n \in \mathbb{Z}$, $n \geq 1$. Then the following are equivalent.

(1) $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) \nmid n$.

(2) there exists a field extension $F \subseteq E$ such that there exists a primitive n-th root of unity in E.

Moreover, if any of the above conditions are satisfied, there exist exactly $\varphi(n)$ primitive n-th roots of unity in E.

Proof (1) $\Rightarrow$ (2): Let $f(x) = x^n - 1 \in F[x]$. Since $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) \nmid n$, we have $f'(x) = nx^{n-1} \neq 0$. Let E be the splitting field of f over F. By Theorem 9.3 we have that the multiplicity of every root of f is 1 and so f has n roots in E. By Corollary 14.6 (applied to the field E), the set $\{r \in E \mid f(r) = 0\}$ is a cyclic group of order n. Let w be a generator of this group. Then $w^n = 1$ but $w^m \neq 1$ for $1 \leq m \leq n-1$, and so w is a primitive n-th root of unity.

(2) $\Rightarrow$ (1): Let $w \in E$ be a primitive n-th root of unity and assume to a contradiction that $\mathrm{char}(F) = p \mid n$. Then $n = mp$ for some $m < n$ since $p \geq 2$. Then

$$0 = w^n - 1 = w^{mp} - 1 = (w^m)^p - 1^p = (w^m - 1)^p \Rightarrow w^m = 1.$$

But this contradicts w being a primitive root of unity since $m < n$. Hence $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) \nmid n$.

Now assume that both (1) and (2) hold and let w be a primitive n-th root of unity. Then

$$\langle w \rangle \subseteq \{x \in E \mid x^n - 1 = 0\}$$

and

$$|\{x \in E \mid x^n - 1 = 0\}| \leq n = |\langle w \rangle|$$

imply $\langle w \rangle = \{x \in E \mid x^n - 1 = 0\}$. Then primitive n-th roots of unity are generators of the group $\{x \in E \mid x^n - 1\}$, that is generators of $\langle w \rangle = \mathbb{Z}_n$. The claim follow by Proposition 14.4(2).

Example 14.8. $\mathrm{char}(\mathbb{C}) = 0$ and $e^{2\pi i \frac{k}{n}} = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$ is a primitive root for all $1 \leq k \leq n$ with $\gcd(k, n) = 1$. As expected we have $\varphi(n)$ primitive roots of unity.

Definition 14.9. Let $n \geq 1$ be such that $\mathrm{char}(F) \nmid n$. The n-th cyclotomic polynomial is

$$\Phi_n(x) = \prod_{\substack{w \text{ primitive} \\ n\text{-th root of unity}}} (x - w)$$

Example 14.10. Let $F = \mathbb{Q}$.

(1) $\Phi_1(x) = x - 1$.

(2) If $p \geq 2$ is prime, then $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$.

(3) $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$.

(4) Let $n = 6$ and let $w \in \mathbb{C}$ a 6-th primitive root of unity. Then the only solutions to the system

$$1 \leq k \leq 6$$

$$\gcd(k, 6) = 1$$

are $k = 1, k = 5$. Then w, w^5 are the 6-th primitive roots of unity and $\Phi_6(x) = (x - w)(x - w^5) = x^2 - (w + w^5)x + 1$. By Example 14.6 we have $w = \frac{1}{2} + \frac{\sqrt{3}}{2} i$, $w^5 = \frac{1}{2} - \frac{\sqrt{3}}{2} i \Rightarrow w + w^5 = 1$ and so $\Phi_6(x) = x^2 - x + 1$.

In general it is hard to compute $\Phi_n(x)$.

Theorem 14.11. The cyclotomic polynomial $\Phi_n(x) \in \mathbb{C}[x]$ is an irreducible polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Proof. We start with showing $\Phi_n(x) \in \mathbb{Q}[x]$. Let E be the splitting field of $x^n - 1$ over $\mathbb{Q}$. Then $\mathbb{Q} \subseteq E$ is Galois by Example 12.4(3). By FTGT(1) we have $\mathbb{Q} = E_{G(E/\mathbb{Q})}$. If $\sigma \in G(E/\mathbb{Q})$ and w is a primitive n-th root of unity, then $\sigma(w)^m = \sigma(w^m)$ implies that $\sigma(w)$ is also a primitive n-th root of unity. Let $\Omega_n = \{w \in E \mid w \text{ is a primitive } n\text{-th root of unity}\}$. Since σ is injective and $\sigma(w) \in \Omega_n$ $\forall w \in \Omega_n$, the map $\sigma|_{\Omega_n} : \Omega_n \to \Omega_n$ is bijective. Then the ring morphism

$$\sigma^* : E[x] \longrightarrow E[x]$$
$$\Downarrow$$
$$a_0 + a_1 x + \cdots + a_m x^m \longmapsto \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_m)x^m$$

satisfies

$$\sigma^*(\Phi_n(x)) = \sigma^*\left(\prod_{w \in \Omega_n}(x-w)\right) = \prod_{w \in \Omega_n}\sigma^*(x-w) = \prod_{w \in \Omega_n}(x-\sigma(w)) \overset{\sigma|_\Omega \text{ bijection}}{=\!=} \prod_{w \in \Omega_n}(x-w) = \Phi_n(x).$$

Hence all the coefficients of $\Phi_n(x)$ are in $E_{G(E/\mathbb{Q})} = \mathbb{Q}$ and $\Phi_n(x) \in \mathbb{Q}[x]$.

Now we show that $\Phi_n(x) \in \mathbb{Z}[x]$. Since $\Phi_n(x) \mid x^n - 1$, we have

$$x^n - 1 = \Phi_n(x)\, h(x)$$

for some $h(x) \in \mathbb{Q}[x]$. Since $x^n - 1$ and $\Phi_n(x)$ are monic, $h(x)$ is also monic. We may factor out all denominators of the coefficients of $h(x)$ as well as the gcd of the numerators to obtain $h(x) = r\overline{h(x)}$ where $\overline{h(x)} \in \mathbb{Z}[x]$ is primitive and $r \in \mathbb{Q}$. Similarly we have $\Phi_n(x) = s\,\overline{\Phi_n(x)}$ where $\overline{\Phi_n(x)} \in \mathbb{Z}[x]$ is primitive and $s \in \mathbb{Q}$. Then

$$x^n - 1 = rs\,\overline{\Phi_n(x)}\,\overline{h(x)} \Rightarrow \frac{1}{rs}(x^n - 1) = \overline{\Phi_n(x)}\,\overline{h(x)}$$

Then by Gauss' Lemma we have that $\overline{\Phi_n(x)}\,\overline{h(x)} = \frac{1}{rs}(x^n - 1)$ is primitive. Hence $\frac{1}{rs} = \pm 1$. On the other hand, $h(x)$ is monic so the coefficient of the highest degree term of $\overline{h(x)}$ is $\frac{1}{r}$ since $h(x) = r\overline{h(x)}$. Hence $\frac{1}{r} \in \mathbb{Z}$ and similarly $\frac{1}{s} \in \mathbb{Z}$. Since $\frac{1}{r}, \frac{1}{s} \in \mathbb{Z}$ and $\frac{1}{r}\cdot\frac{1}{s} = \pm 1$, we conclude that $\frac{1}{r} = \pm 1$ and $\frac{1}{s} = \pm 1$. Hence $s = \pm 1$ and $\Phi_n(x) = \pm\overline{\Phi_n(x)} \in \mathbb{Z}[x]$.

By Theorem 14.7 there exist exactly $\varphi(n)$ primitive n-th roots of unity in $\mathbb{C}$ and so $\deg(\Phi_n) = \varphi(n)$.

Proof continued next time!