Lecture 19: Cyclotomic Fields and Applications

\( \mathbb{Q}(\zeta_n) \) with \( \zeta_n = e^{2\pi i/n} \); \( \mu_n = \{ z \in \mathbb{C} \mid z^n = 1 \} \)

\( \Phi_n(x) = \prod_{d \mid n} (x - \zeta_d) \). Then \( x^n - 1 = \prod_{d \mid n} \Phi_d(x) \) for any primitive \( n \).

---

Thm: For any \( n \), \( \Phi_n(x) \) is in \( \mathbb{Z}[x] \) and is irreducible.
Hence \([\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\mu_n^{\text{primitive}}| = \phi(n)\).

Pf that \( \Phi_n(x) \in \mathbb{Z}[x] \): We induct on \( n \).

Set \( f(x) = \prod_{d \mid n} \Phi_d(x) \), so then \( x^n - 1 = f(x) \Phi_n(x) \) in \( \mathbb{Q}[x] \) by induction.

In \( \mathbb{Q}[x] \) have \( x^n - 1 = q(x)f(x) + r(x) \) with \( \deg r < \deg f \). Then in \( \mathbb{C}[x] \) have

\[ \Phi_n(x)f(x) = \Phi_n(x)q(x)f(x) + \Phi_n(x)r(x) \Rightarrow (\Phi_n(x) - q(x))f(x) = r(x) \]

\( \Rightarrow r(x) = 0 \) as \( \deg r < \deg f \). So \( \Phi_n(x) = q(x) \) and \( \Phi_n(x) \in \mathbb{Q}[x] \) and by Gauss in \( \mathbb{Z}[x] \) as well.
Proof of Irreducibility: Suppose $\Phi_n = f \cdot g$ for $f, g \in \mathbb{Z}[x]$ with $f$ irreducible.

Claim: Suppose $S$ is a root of $f$. If $p$ is a prime not dividing $n$, then $S^p$ is also a root of $f$.

Assuming this, let $S$ be a fixed root of $f$. Then any primitive $n$th root is $S^m$ where $m = p_1 p_2 \cdots p_k$ and all $p_i \nmid n$. As $S^m = (((S^{p_1})^{p_2})^{p_3} \cdots )^{p_k}$ repeatedly applying the claim gives $S^m$ is a root of $f$. So $f(x) = \Phi_n(x)$ and so $\Phi_n(x)$ is irreducible.

Proof of Claim: Suppose instead $g(S^p) = 0$. Thus $S$ is a root of $g(x^p) \Rightarrow g(x^p) = f(x) \cdot h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Let's look in $\mathbb{F}_p[x]$:

1. $x^n - 1$ is separable as $nx^{n-1} \not\equiv 0$ in $\mathbb{F}_p[x]$. So $\Phi_n(x)$ has distinct roots.
(2) The Frobenius map $\overline{F}_p : \overline{F}_p \to \overline{F}_p$ is the identity, since $a^p = a$ for all $a \in \overline{F}_p$ as discussed last time. Hence $\overline{g}(x^p) = (\overline{g}(x))^p$ for all $\overline{g} \in \overline{F}_p[x]$.

(3) As $\overline{g}(x)^p = \overline{f}(x)\overline{h}(x)$, we see $\overline{g}$ and $\overline{h}$ have a common root.

But then by (3) the poly $\overline{\Phi}_n = \overline{g}^{\frac{1}{p}}$ has a multiple root, a contradiction.

---

**Thm:** $m \in \mathbb{Z}_{>0}$. There are infinitely many primes $p \equiv 1 \mod m$, i.e. $p = cm + 1$.

[Special case of Dirichlet's Thm on Primes in Arithmetic Progressions.]

**Proof:** Consider $\Phi_m(a)$ for $a \in \mathbb{Z}_{>0}$. Then

1. There are infinitely many primes which divide some $\Phi_m(a)$.

2. Any $p \mid \Phi_m(a)$ with $p \nmid m$ has $p \equiv 1 \mod m$. 
(1) is true for all monic polys in \( \mathbb{Z}[x] \), so will focus on (2).

In \( \mathbb{F}_p \), have \( a^m - 1 = \prod_{d \mid m, d < m} \Phi_d(a) = 0 \)

Claim: \( a \) has order \( m \) in \( \mathbb{F}_p^x \).

Pf of Claim: Suppose \( a^d = 1 \) for \( d < m \). Now \( d \mid m \) and so \( a \) is a root of some \( \Phi_d \) for \( d \mid d \). But then \( x^m - 1 \) has a multiple root, a contradiction as \( m x^{m-1} \neq 0 \) in \( \mathbb{F}_p[x] \). So \( a \) has order \( m \) in \( \mathbb{F}_p^x \).

Pf of (2): As \( a \) has order \( m \), we have \( m \mid |\mathbb{F}_p^x| = p - 1 \) \( \Rightarrow p = cm + 1 \), as needed.

Pf of (1): More gen, let \( f(x) \in \mathbb{Z}[x] \) be monic.
Suppose \( \{ f(a) \mid a \in \mathbb{N} \} \) have only finitely many prime divisors \( p_1, \ldots, p_k \). Choose a \( \alpha \) so that \( f(\alpha) = c \neq 0 \).
Consider
\[ g(x) = C^{-1} f(a + C p_1 \cdots p_k x) \]
\[ n = \deg f \]
\[ = C^{-1} \left( f(a) + f'(a) cy + \frac{f''(a)}{2} c^2 y^2 + \cdots + \frac{f^{(n)}(a)}{n!} c^n y^n \right) \]
\[ = 1 + f'(a)y + \frac{f''(a)}{2} c^2 y^2 + \cdots + \frac{f^{(n)}(a)}{n!} c^n y^n \]
which is in \( \mathbb{Z}[x] \).

For any \( b \), have \( g(b) \equiv 1 \mod p_1 \cdots p_k \).

Pick \( b \) large enough so that \( |g(b)| > 1 \).

Let \( p \) be any prime factor of \( g(b) \).

Then \( p \neq p_i \) for all \( i \) and \( p | f(a + C p_1 \cdots p_k b) \).