Goal: $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \mathbb{Z}/n\mathbb{Z}^{\times}$

$\zeta = \zeta_n$, primitive n^{th} root of 1.

Def $\Phi(x) = \prod_{1 \leq i \leq n} (x - \zeta^i)$ n-th cyclotomic polynomial.

Examples: $\Phi_1(x) = x - 1$

Examples: $\Phi_2(x) = x + 1$

Examples: $\Phi_3(x) = x^2 + x + 11$

Examples: $\Phi_4(x) = x^2 + 1$

Examples: $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$

Observe $x^n - 1 = \prod_{d|n} \Phi_d(x) = \prod_{1 \leq i \leq n} (x - \zeta^i)$

In $C_n =< \zeta >$, we have elements of order $d|n$

$C_n \ C_{d_1} \ C_{d_2} \ C_{d_4} \ C_{d_3}$

Claim: $\Phi_n(x) \in \mathbb{Z}[x] \forall n \in \mathbb{N}$

Proof: Induction on n.

$n = 1 = x - 1 \in \mathbb{Z}[x]$

Assume $\Phi_m(x) \in \mathbb{Z}[x] \ \forall m < n$

$x^n - 1 = \Phi_n(x) = \prod_{d|n \quad d \neq n} \Phi_d(x) \in \mathbb{Z}[x]$.

By Gauss' Lemma $\Phi_n(x) \in \mathbb{Z}[x]$. ■

Theorem 0.1 *$\Phi_n(x)$ is irreducible over $\mathbb{Q}$ for $\forall n \in \mathbb{N}$.*

Proof: Let $f(x)$ be the minimal polynomial of $\zeta = \zeta_n$.

$\phi_n(x) = \prod_{1 \leq i \leq n \ (i,n)=1} (x - \zeta^i)$

$\implies f(x)|\Phi_n(x)$.

To show that $f(x) = \Phi_n(x)$, we show that ζ^i is a root of f, $\forall i, \ (i, n) = 1$.

Enough to show that ζ^p is a root of f for all primes p, $(p, n) = 1$.

Enoguh to show that $f(\eta) = 0$ then $f(\eta^p) = 0$ for $(p, n) = 1$.

$i = p_1 p_2 \ldots p_r$. $(p_j, n) = 1$

$\zeta, \zeta^{p_1}, \zeta^{p_1 p_2}, \zeta^{\overset{=i}{p_1 \cdots p_r}} = \zeta^i$

Claim: If $f(\eta) = 0, (p, n) = 1$ then $f(\eta^p) = 0$

Proof: Suppose for a contradiction, $f(\eta) = 0$, $f(\eta^p) = 0$.

Write $\Phi_n(x) = f(x)g(x)$.

So $g(\eta^p) = 0$

$\implies \eta$ is a root of $g(x^p)$

By Gauss' Lemma, $f(x), g(x) \in \mathbb{Z}[x]$

$f(x)|g(x^p)$

Reduce modulo p. $\overline{f}(x)$, $\overline{g}(x^p) \in \mathbb{F}_p$

$\overline{f(x)}|\overline{g(x^p)} = \overline{g(x)^p}$

$\implies \overline{f(x)}, \overline{g(x)}$ have common roots.

$f(x)g(x) = \Phi_n(x)|x^n - 1$

$\overline{f(x)g(x)} = \overline{\Phi_n(x)}|\overline{x^n - 1}$

$\overline{f(x)g(x)}$ has multiple roots.

But $\overline{x^n - 1}$ cannot have multiple roots.

Recall: $h(x) \in \mathbb{F}_p[x]$ has multiple roots iff $gcd(h, h') \neq 1$.

But $(\overline{x^n - 1})' = \overline{nx^{n-1}}$, only $\overline{0}$ is a root.

$\implies$ claim holds.

$\blacksquare$ $\blacksquare$

Cor: $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Proof: $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = deg\Phi_n(x) = \phi(n)$

$|(\mathbb{Z}/n\mathbb{Z})| = \phi(n)$

Gal$(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \hookrightarrow \mathbb{Z}/n\mathbb{Z}^x$.

$\blacksquare$

Theorem 0.2 *Any finite Galois extension $E/\mathbb{Q}$ with abelian Galois gp is ismorphic to a subfield of $\mathbb{Q}(\zeta_n)$ for some n.*

$E \hookrightarrow \mathbb{Q}(\zeta_n)$ *(ableian)* $\mathbb{Q}$ $\mathbb{Q}$