0.1 Cyclotomic Extensions

F field, assume $x^n - 1$ is sep.

$F(\zeta_n)/F$, ζ_n is a primitive n^{th} root of unity.

$\{1, \zeta_n, ..., \zeta_n - 1\}$

Roots of $x^n - 1$ and C_n, $x^n = 1$.

These extensions come up $f(x) = x^n - a, a \in F$.

$\sqrt[n]{a}, \zeta_n \sqrt[n]{a}, \ldots$

Q: Number of generators of C_n?

$C_n =< b >$.

$|b|= n$

$|b^j|= \frac{n}{(j,n)}$

Number of generators of $|(\mathbb{Z}/n\mathbb{Z})^\times|= \phi(n)$.

$\phi(p) = p - 1$

$\phi(p^r) = p^r - p^{r-1}(p - 1)$

$\{1, 2, \ldots, p^r\}$

Theorem 0.1 *$a.b \in \mathbb{Z}$ are coprime, $\mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.*

Ex: $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

$a + 6z \to \alpha + 2\mathbb{Z}, \alpha + 3\mathbb{Z}$.

Ex: $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$a + 4z \to \alpha + 2\mathbb{Z}, \alpha + 2\mathbb{Z}$.

By induction, suppose that $n = p_1^{r_1} \ldots p_k^{r_k}$.

$p_1^{r_1} \ldots$ distinct primes.

$\mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}/p^{r_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p^{r_k}\mathbb{Z})^\times$

$\phi(n) = \phi(p_1^{r_1}) \ldots \phi(p_k^{r_k}) = n \prod_{p|n} (1 - \frac{1}{p})$

0.2 Study $Gal(F(\zeta_n)/F)$

Lemma $\sigma \in Gal(F(\zeta_n)/F)$

and let $\zeta \in \mu_n(F(\zeta_n)) = \{\zeta_n^k | 1 \le k \le n\}$ then $\exists a = a_\sigma, (a, n) = 1$ s.t. $\sigma(\zeta) = \zeta^a$

Rem:

$Gal(F(\zeta_n)/F) \to Perm(\{1, \zeta_n, ..., \zeta_n - 1\})$

Pf: ζ_n is primitive, $\zeta_n = 1$, $\zeta_n^j \neq 1$, $1 \leq j \leq n$.

$\sigma(\zeta_n)$ must be a generator.

$\implies \sigma(\zeta_n) = \zeta_n^a$, $(a, n) = 1$ for some a.

$\sigma(\zeta) = \sigma(\zeta_n^k) = \sigma(\zeta_m)^k = (\zeta_n^a)^k = (\zeta_n^k)^a$

Thm: $Gal(F(\zeta_n)/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$

$\sigma \to a_\sigma$ an injective homo.

$\sigma\tau = a_\sigma a_\tau$

$\zeta^{a_{\tau\sigma}} = (\tau\sigma)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{a\tau}) = (\sigma(\zeta))^{a\tau} = (\zeta^{a\sigma})^{a\tau} = \zeta^{a_\sigma, a_\tau}$

$\sigma \in \text{kernel} : \sigma(\zeta_n) = \zeta_n^1$

$F(\zeta_n) \qquad \sigma_{|F} = id$

generated by $F, \zeta_n \implies \sigma = id$.

Cor: $Gal(F(\zeta_n)/F)$ abelian.

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

0.3 Cyclotomic Polynomials

$\mathbb{Q}, x^n - 1$, $\zeta = \zeta_n$ primitive.

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

$\Phi_2(x) = x - (-1) = x + 1$

$\Phi(x) = (x - \zeta)(x - \zeta^2), \zeta^3 = 1 = x^2 - (\zeta + \zeta^2)x + 1$

$= x^2 + x + 1$

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