Lecture 17 : Cyclotomic Extensions I

Objectives

(1) Roots of unity in a field.
(2) Galois group of $x^n - a$ over a field having n^{th} roots of unity.
(3) Irreduciblilty of the cyclotomic polynomial $\Phi_n(x)$ over $\mathbb{Q}$.
(4) A recursive formula for $\Phi_n(x)$.

Keywords and phrases : Roots of unity, Galois group of $x^n - a$, cyclotomic polynomials.

---

18. Cyclotomic Extensions

Roots of unity in any field

Let F be a field. A root $z \in F$ of $x^n - 1$ is called an n^{th} root of unity in F. Roots of unity play important role in algebra and number theory. Their analysis led Gauss to his first mathematical discovery: construction of a regular polygon of 17 sides.

Suppose that char $F = p$ and $n = p^e m$ where $(m, p) = 1$. Then $x^n - 1 = (x^m - 1)^{p^e}$. By the derivative criterion, $x^m - 1$ is separable. Hence the splitting field of $x^n - 1$ is equal to that of $x^m - 1$. Therefore we consider fields of chararacteristic zero or of characteristic p where $(p, n) = 1$.

Let k be a field and $(n, \text{char } k) = 1$. Then $x^n - 1$ is separable by the derivative criterion. Let $Z = \{z_1, z_2, \ldots, z_n\}$ be the set of its roots of in k^a. Then Z is a multiplicative subgroup of $(k^a)^\times$. Hence it is cyclic. Any of the $\varphi(n)$ generators of Z is called a **primitive n^{th} root of unity.** Let z be any such generator. Then $k(z)$ is a splitting field of $x^n - 1$ over k. Let $\Phi_n(x) = \text{ irr } (z, \mathbb{Q})$. A primitive n^{th} root of unity over $\mathbb{Q}$ is denoted by ζ_n.

Definition 18.1. *A splitting field of $x^n - 1$ over F is called a* **cyclotomic field of order n over F.**

Proposition 18.2. *Let $(\text{char } F, n) = 1$ and $f(x) = x^n - 1 \in F[x]$. Then G_f is isomorphic to a subgroup of $U(n)$. In particular G_f is an abelian group and $o(G_f) \mid \varphi(n)$.*

Proof. As $f(x)$ is separable, it has n distinct roots. Let $\{z_1, z_2, \ldots, z_n\} = Z$ be the set of roots of $f(x)$ in F^a and $E = F(z_1, z_2, \ldots, z_n)$. Since $Z \subseteq E^\times$ is a subgroup, it is cyclic. The map $\psi : G(E/F) \to Aut(Z)$ such that $\sigma \mapsto \sigma|_Z$ is an injective group homomorphism. Since $Aut(Z) \simeq \{\bar{m} \mid (m, n) = 1\} := U(n)$ is an abelian group, $G(E/F)$ is also an abelian group whose order divides $\varphi(n)$. □

Example 18.3. Let $F = \mathbb{F}_2$. Then $x^3 - 1 = (x-1)(x^2 + x + 1)$. Any root z of $x^2 + x + 1$ is a primitive cube root of unity over F. Hence $[F(z) : F] = 2$. To find the degree of a primitive seventh root of unity over F, consider the factorization of $x^7 - 1$ into irreducible polynomials over F :

$$x^7 - 1 = (x-1)(x^3 + x^2 + 1)(x^3 + x + 1).$$

Therefore there are 6 primitive $7th$ roots of unity over F with two minimal polynomials. In contrast to this, we shall see that all the primitive n^{th} roots of unity over $\mathbb{Q}$ have the same irreducible polynomial called the n^{th} cyclotomic polynomial $\Phi_n(x)$.

Proposition 18.4. *Let $x^n - a = f(x) \in F[x]$ and suppose F has n distinct roots of $x^n - 1$. Then G_f is a cyclic group and $o(G_f)$ divides n.*

Proof. Let $Z = \{z_1, z_2, \ldots, z_n\} \subset F$ be the set of roots of $x^n - 1$. Let r be a root of $f(x)$ in a splitting field E of $f(x)$. Then $rz_1, rz_2, \ldots, rz_n$ are roots of $f(x)$. Thus $E = F(r)$. Let $\sigma, \tau \in G(E/F)$. Then $\sigma(r) = z_\sigma r$ and $\tau(r) = z_\tau r$ for some $z_\sigma, z_\tau \in Z$. Hence $\sigma\tau(r) = \sigma(z_\tau r) = z_\tau z_\sigma r$. Define

$$\psi : G(E/F) \to \mathbb{Z} \text{ such that } \psi(\sigma) = z_\sigma.$$

Then ψ is a group homomorphism. The map ϕ is clearly injective. Since Z is a subgroup of $F^\times$, it is a cyclic group of order n. Hence $|G_f|$ divides n and G_f is cyclic.

□

Theorem 18.5. (1) $\Phi_n(x) \in \mathbb{Z}[x]$, (2) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \deg \Phi_n(x)$ *and* (3) $G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq U_n$.

Proof. Let $\Phi_n(x) = \text{ irr } (\zeta_n, \mathbb{Q})$. Then $x^n - 1 = \Phi_n(x)h(x)$, where $h(x)$ is monic in $\mathbb{Q}[x]$. By Gauss' Lemma $\Phi_n(x), h(x) \in \mathbb{Z}[x]$. We show that each

primitive n^{th} root of unity is a root of $\Phi_n(x)$. Let p be a prime number and $(p,n)=1$. Suppose $\Phi_n(\zeta_n^p) \neq 0$. Hence $h(\zeta_n^p)=0$. Hence ζ_n is a root of $h(x^p)$. Thus

$$h(x^p) = \Phi_n(x)g(x) \text{ for some monic } g(x) \in \mathbb{Z}[x].$$

Reduce mod p to get

$$(\bar{h}(x))^p = \bar{\Phi}_n(x)\bar{g}(x) \quad ,$$

where "–" denotes reduction of coefficients mod p. Hence $\bar{\Phi}_n(x)$ and $\bar{h}(x)$ have a common root mod p. But x^n-1 has distinct roots over $\mathbb{F}_p$. Hence ζ_n^p is a root of $\Phi_n(x)$. Hence all primitive n^{th} roots of unity are roots of $\Phi_n(x)$. Since $G = G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to a subgroup of $U(n)$, $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = |G| \leq \varphi(n)$. But $\deg \Phi_n(x) \geq \varphi(n)$. Hence $|G| = \varphi(n)$. Hence $G \simeq U(n)$. □

Computation of Cyclotomic Polynomials

Let ζ_n be a primitive n^{th} root of unity. Then the other roots of $\Phi_n(x)$ are ζ_n^i such that $(i,n)=1$. Thus

$$\Phi_n(x) = \prod_{(i,n)=1} (x-\zeta_n^i).$$

Since the roots of x^n-1 form a cyclic group of order n, the order of any root divides n. Since $\Phi_d(x) = \prod_{o(z)=d}(x-z)$, it follows that

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Therefore

$$\Phi_n(x) = \frac{x^n-1}{\prod_{d|n,d<n} \Phi_d(x)}.$$

This is a recursive formula for computation of $\Phi_n(x)$. First few cyclotomic polynomials are:

$$\begin{aligned}
\Phi_1(x) &= x-1 \\
\Phi_2(x) &= \frac{x^2-1}{\Phi_1(x)} = x+1 \\
\Phi_3(x) &= \frac{x^3-1}{\Phi_1(x)} = x^2+x+1 \\
\Phi_4(x) &= \frac{x^4-1}{\Phi_1(x)\Phi_2(x)} = x^2+1 \\
\Phi_5(x) &= x^4+x^3+x^2+x+1 \\
\Phi_6(x) &= \frac{x^6-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = x^2-x+1
\end{aligned}$$