Lecture 19 : Abelian and Cyclic Extensions

Objectives

(1) Infinitude of primes $p \equiv 1$ (mod n).
(2) Inverse Galois problem for finite abelian groups.
(3) Structure of some cyclic extensions.

Keywords and phrases : Primes of the form $p \equiv 1$ (mod n), abelian extension, cyclic extension, inverse Galois problem.

The Inverse Galois Problem for Finite Abelian Groups

A Galois extension E/F is called **abelian (resp. cyclic)** if $G(E/F)$ is abelian (resp. cyclic). In this section we will show that any finite abelian group is the Galois group of a Galois extension of $\mathbb{Q}$. In other words, any finite abelian group is the Galois group of a polynomial with rational coefficients. A proof of this theorem requires the theorem from number theory that there are infinitely many primes $p \equiv 1(\text{ mod } n)$. We shall prove this using cyclotomic polynomials. This is a special case of Dirichlet's theorem about infinitude of primes in the arithmetic progression $a+nb$ where a, b are coprime natural numbers and $n = 1, 2, 3, \ldots$. We will also construct cyclic extensions of fields having enough roots of unity.

Lemma 19.1. *Let p be a prime number and n be relatively prime to p. Let $\bar{\Phi}_n(x)$ have a root in $\mathbb{F}_p$. Then $p \equiv 1$ (mod n).*

Proof. Let $k \in \mathbb{Z}$, $\bar{k} \in \mathbb{F}_p$ and $\bar{\Phi}_n(\bar{k}) = 0$. Then $p \mid \Phi_n(k)$. Hence $p \mid k^n - 1$. Thus $k^n \equiv 1(\text{mod } p)$. We claim that $o(\bar{k}) = n$ in the group $(\mathbb{F}_p)^\times$. Suppose $o(\bar{k}) = m < n$. Then $\bar{k^m} = 1$. Hence

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \Phi_d(x) = \Phi_n(x) \prod_{d<n} \Phi_d(x) \\ &= \Phi_n(x) \prod_{d|m} \Phi_d(x) h(x) \\ &= \Phi_n(x)(x^m - 1)h(x) \end{aligned}$$

Hence $\bar{k}^n - 1 = \Phi_n(\bar{k})(\bar{k}^m - 1)h(\bar{k})$. This means $x^n - 1$ has a multiple root in $\mathbb{F}_p$. This is a contradiction. Hence $o(\bar{k}) = n$. Hence $n \mid p - 1$. Thus $p \equiv 1 \bmod n$. □

Theorem 19.2. *There are infinitely many primes* $p \equiv 1$ (mod n).

Proof. Suppose to the contrary, $p_1, p_2, \ldots, p_g$ are all such primes. Let $m = np_1p_2 \ldots p_g$. Since $\Phi_m(x) \in \mathbb{Z}[x]$, is monic, $\lim_{x\to\infty} \Phi_m(mx) = \infty$. Hence there exists k such that $\Phi_m(mk) \geq 2$. Let p be a prime factor of $\Phi_m(mk)$. Then $p \mid (mk)^m - 1$. Hence p does not divide mk. Hence $(p, n) = 1$ and $p \neq p_1, \ldots, p_n$. Moreover $\bar{\Phi}_m(\overline{mk}) = 0$. Hence $p \equiv 1$(mod n). This is a contradiction. □

Theorem 19.3. *Let G be a finite abelian group. Then there is a Galois extension $K/\mathbb{Q}$ such that $G(K/\mathbb{Q}) = G$.*

Proof. We may assume that $|G| \geq 2$. Then $G \simeq C_{n_1} \times \cdots \times C_{n_k}$. where $|G| = n = n_1n_2 \ldots n_k$ and $n_1|n_2| \cdots |n_k$. There exist infinitely many primes $p_i \equiv 1 \pmod{n_i}$ for $i = 1, 2, \ldots, k$. We can find subgroups $H_1 < U(p_1), H_2 < U(p_2), \ldots, H_k < U(p_k)$ such that

$$\frac{U(p_1)}{H_1} \simeq C_{n_1},\ \frac{U(p_2)}{H_2} \simeq C_{n_2},\ \ldots, \frac{U(p_k)}{H_k} \simeq C_{n_k}.$$

$$\frac{U(p_1) \times U(p_2) \times \cdots \times U(p_k)}{H_1 \times H_2 \times \cdots \times H_k} \simeq C_{n_1} \times \cdots \times C_{n_k}.$$

Let $H < U(n)$ and $H \simeq H_1 \times H_2 \times \cdots \times H_k$. Then $\frac{U(n)}{H} \simeq G$. By the FTGT

$$G(\mathbb{Q}(\zeta_n)^H/\mathbb{Q}) = \frac{U(n)}{H} \simeq G.$$

□

Cyclic Galois Extensions

In this section we discuss cyclic extensions of degree n if F has a primitive n^{th} root of unity or when F has characteristic $p > 0$ and E/F has degree p. There is no simple description of cyclic extensions of $\mathbb{Q}$ or fields devoid of roots of unity. We need a theorem of Dedekind about linear independence over K of automorphims of a field K.

Definition 19.4. *Let G be a group and K a field. By a* **character of G in K** *we mean a homomorphism $\chi : G \to K^\times$. We say that characters $\chi_1, \chi_2, \ldots, \chi_n : G \to K^\times$ are* **linearly independent** *if for $a_1, \ldots, a_n \in K$ $a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$ if and only if $a_i = 0$ for $i = 1, 2, \ldots, n$.*

Theorem 19.5 (Dedekind). *Let $\chi_1, \chi_2, \ldots, \chi_n$ be distinct characters of a group G in a field K. Then $\chi_1, \chi_2, \ldots, \chi_n$ are linearly independent.*

Proof. Apply induction on n. If $n = 1$, then $\chi_1 : G \to K^\times$ is clearly linearly independent. Let $n \geq 2$. Let n be the smallest positive integer such that there exist $a_1, \ldots, a_n \in K$, not all zero with

$$a_1\chi_1 + \cdots + a_n\chi_n = 0. \tag{1}$$

Then $a_i \neq 0$, for all i. Since $\chi_1 \neq \chi_2$, there exists $z \in G$ such that $\chi_1(z) \neq \chi_2(z)$. Hence for all $x \in G$,

$$a_1\chi_1(xz) + a_2\chi_2(xz) + \cdots + a_n\chi_n(xz) = 0 \tag{2}$$

$$a_1\chi_1(z)\chi_1 + a_2\chi_2(z)\chi_2 + \cdots + a_n\chi_n(z)\chi_n = 0. \tag{3}$$

Multiply (1) by $\chi_1(z)$ and subtract (3) to get the relation :

$$(\chi_1(z) - \chi_2(z))a_2\chi_2 + (\chi_1(z) - \chi_3(z))a_3\chi_3 + \cdots + (\chi_1(z) - \chi_n(z))a_n\chi_n = 0.$$

The above relation has smaller length, which is a contradiction.

□

Lemma 19.6. *Let F be a field containing a primitive n^{th} root of unity ζ. Suppose that E/F is a Galois extension of degree n and $G = G(E/F) = (\sigma)$. Then ζ is an eigenvalue of σ.*

Proof. The field E is an n-dimensional F-vector space. Since σ has order n, σ satisfies $x^n - 1 = 0$. If σ is a root of a polynomial $f(x) \in F[x]$ of degree $m < n$ then $\sigma, \sigma^2, \ldots, \sigma^m$ are linearly dependent over F. This contradicts Dedekind's Theorem. Hence the minimal and the characteristic polynomials of σ are equal to $x^n - 1$. Hence ζ is an eigenvalue of σ.

□

We now describe the structure of cyclic extensions of degree n over a field having a primitive n^{th} root of unity.

Theorem 19.7. *Let E/F be a cyclic extension of degree n with $G = G(E/F) = (\sigma)$ and let $\zeta \in F$ be a primitive n^{th} root of unity. Then there exists a $b \in F$ so that $E = F(a)$ where $a^n = b$.*

Proof. Since ζ is an eigenvalue of σ, there exists an eigenvector $a \in E^\times$ so that $\sigma(a) = \zeta a$. Hence $\sigma^i(a) = \zeta^i a$ for all $i = 1, 2, \ldots, n$. Hence a has at least n conjugates in E. As E/F is a Galois extension of degree n, and E contains a splitting field of $f(x) = \text{ irr } (a, F)$, it follows that $E = F(a)$ and $a^n \in F$ since $\sigma(a^n) = \zeta^n a^n = a^n$. □

Intermediate subfields of a cyclic Galois extension

Let E/F be a cyclic Galois extension of degree n where F has a primitive n^{th} root of unity. We have proved that $E = F(a)$ where $a^n \in F$. The number of subgroups of the Galois group $G = G(E/F)$ is $d(n)$, the number of divisors of n. Each of these subgroups is cyclic. Hence there are $d(n)$ intermediate subfields of E/F. We show that they are $F(a^d)$ where d is a divisor of n.

Proposition 19.8. *Let E/F be a cyclic Galois extension of degree n where F has a primitive n^{th} root of unity. Let $E = F(a)$ where $a^n \in F$. Then The intermediate subfields of E/F are $F(a^d)$ where d is a divisor of n.*

Proof. The Galois group G has unique subgroup of order d for every divisor d of n. Hence E/F has a unique subfield of degree d for each divisor d of n. Consider the subfield $K = F(a^d)$. Then a is a root of $x^d - a^d \in K[x]$. Thus $[E : F(a^d)] \leq d$. Since $a^n \in F$, we have $(a^d)^{n/d} \in F$. Hence $[F(a^d) : F] \leq n/d$. It follows that $[E : F(a^d)] = d$. Hence the intermediate subfields of E/F are $F(a^d)$ where d varies over the divisors of n.

□