Cyclotomic Extensions and Their Galois Groups

Mathematics Lecture Notes

1 Introduction to Cyclotomic Fields

In algebraic number theory, cyclotomic fields play a fundamental role. These are field extensions obtained by adjoining roots of unity to the rational numbers. In these notes, we explore the structure of cyclotomic extensions and compute their Galois groups.

2 The n-th Cyclotomic Field

Definition 1 *Let n be a positive integer. The **n-th cyclotomic field** is the field extension $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity.*

A primitive n-th root of unity satisfies $\zeta_n^n = 1$ and $\zeta_n^k \neq 1$ for any $1 \leq k < n$. The minimal polynomial of ζ_n over $\mathbb{Q}$ is the **n-th cyclotomic polynomial**:

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \zeta_n^k).$$

This polynomial has degree $\varphi(n)$, where φ is Euler's totient function.

3 Galois Group of Cyclotomic Extensions

Theorem 1 *The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, and its Galois group is isomorphic to the multiplicative group of units modulo n:*

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

To understand this isomorphism, we describe the action of the Galois group on the primitive roots. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, we have:

$$\sigma(\zeta_n) = \zeta_n^a$$

for some integer a with $\gcd(a, n) = 1$. This gives a well-defined map:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto a \mod n.$$

One can verify that this map is a group isomorphism.

3.1 Example: The Case $n = p$ is Prime

When $n = p$ is an odd prime, the cyclotomic field $\mathbb{Q}(\zeta_p)$ has degree $\varphi(p) = p - 1$. The Galois group is cyclic of order $p - 1$:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$

This cyclic structure has important consequences for the arithmetic of these fields.

4 Subfields and Their Galois Groups

A fundamental problem is to classify the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_n)$. By the Galois correspondence, these subfields correspond to subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$.

4.1 Quadratic Subfields

An important class of subfields are the quadratic extensions of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_n)$. These correspond to subgroups of index 2 in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 2 *Let $n > 2$. Then $\mathbb{Q}(\zeta_n)$ contains a unique quadratic subfield:*

$$\mathbb{Q}(\sqrt{d}), \quad \textit{where } d = \begin{cases} (-1)^{\frac{p-1}{2}} p & \textit{if } n = p \textit{ is an odd prime}, \\ (-1)^{\frac{n}{2}} n & \textit{if } n \equiv 0 \pmod 4, \\ (-1)^{\frac{n-1}{2}} n & \textit{if } n \equiv 1, 2 \pmod 4. \end{cases}$$

The discriminant d can be computed using properties of Gauss sums. For example, when $n = p$ is an odd prime, we have:

$$\mathbb{Q}(\zeta_p) \supset \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p}).$$

5 Decomposition of Primes in Cyclotomic Fields

The behavior of prime numbers in cyclotomic extensions is described by classical results in algebraic number theory.

Theorem 3 *Let p be a prime number not dividing n. Then p is unramified in $\mathbb{Q}(\zeta_n)$, and its decomposition is determined by the order of p modulo n. Specifically, the inertial degree f equals the multiplicative order of p modulo n.*

This theorem illustrates the deep connection between arithmetic properties of primes and the structure of cyclotomic fields.

6 Applications and Further Directions

Cyclotomic fields have numerous applications in number theory, including:

- Proofs of quadratic reciprocity
- Construction of abelian extensions (Kronecker-Weber theorem)
- Studies of class numbers and Iwasawa theory

The rich structure of these fields continues to be an active area of research in modern number theory.