Notes on Cyclotomic Fields and Galois Theory

Blackboard Transcription

1 Introduction to Cyclotomic Fields

We begin by considering cyclotomic fields, which are extensions of the rational numbers obtained by adjoining roots of unity. These fields play a fundamental role in algebraic number theory and have deep connections to Galois theory.

2 Galois Group of Cyclotomic Extensions

Definition 1 *Let ζ_n denote a primitive nth root of unity. The nth cyclotomic field is $\mathbb{Q}(\zeta_n)$.*

Theorem 1 *The Galois group of the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of units modulo n.*

Let us examine this isomorphism more carefully. For any integer a coprime to n, there is an automorphism σ_a of $\mathbb{Q}(\zeta_n)$ defined by:

$$\sigma_a(\zeta_n) = \zeta_n^a.$$

This assignment gives the isomorphism:

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

3 Subfields and Fixed Fields

An important aspect of Galois theory is the correspondence between subgroups of the Galois group and intermediate fields. For cyclotomic fields, this correspondence is particularly explicit.

Consider the subgroup $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$. The fixed field of the corresponding subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is:

$$\mathbb{Q}(\zeta_n)^H = \{x \in \mathbb{Q}(\zeta_n) : \sigma(x) = x \text{ for all } \sigma \in H\}.$$

3.1 Example: Quadratic Subfields

When n is an odd prime p, the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$. If $p-1$ is even, then there is a unique subgroup of index 2. The corresponding fixed field is a quadratic extension of $\mathbb{Q}$.

In fact, one can show that:

$$\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p),$$

where $p^* = (-1)^{\frac{p-1}{2}}p$. This quadratic field is fixed by the unique subgroup of index 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$.

4 Ramification in Cyclotomic Fields

The study of how primes factor in cyclotomic extensions is central to algebraic number theory. The following result is fundamental:

Theorem 2 *Let p be a prime number and n a positive integer. The prime p is ramified in $\mathbb{Q}(\zeta_n)$ if and only if p divides n.*

More precisely, if $n = p^e m$ with $p \nmid m$, then the ramification index of p in $\mathbb{Q}(\zeta_n)$ is $\varphi(p^e) = p^{e-1}(p-1)$.

5 Discriminant Calculations

The discriminant of a number field provides important information about its arithmetic properties. For cyclotomic fields, we have:

Theorem 3 *The discriminant of $\mathbb{Q}(\zeta_n)$ is given by:*

$$\Delta_{\mathbb{Q}(\zeta_n)} = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

This formula reveals that the primes dividing the discriminant are exactly those dividing n, consistent with the ramification theorem above.

6 Units and the Cyclotomic Unit Group

The unit group of cyclotomic fields has a rich structure. Of particular interest are the *cyclotomic units*, which generate a subgroup of finite index in the full unit group.

For $\mathbb{Q}(\zeta_p)$ with p an odd prime, the cyclotomic units are defined as:

$$\eta_a = \frac{\zeta_p^a - 1}{\zeta_p - 1}, \quad \text{for } a = 2, 3, \ldots, \frac{p-1}{2}.$$

These units satisfy various norm relations and play a crucial role in the proof of the Kronecker-Weber theorem and in Iwasawa theory.

7 Class Number Formulas

The class number of cyclotomic fields, which measures the failure of unique factorization, can be related to special values of L-functions. For $\mathbb{Q}(\zeta_p)$, we have:

$$h_p = \frac{\prod_{\chi \text{ odd}} (-\frac{1}{2} B_{1,\chi})}{2^{\frac{p-3}{2}} R_p},$$

where $B_{1,\chi}$ are generalized Bernoulli numbers and R_p is the regulator.

This formula connects the arithmetic of cyclotomic fields to analytic objects, illustrating the deep unity between number theory and analysis.

8 Conclusion

Cyclotomic fields provide a beautiful testing ground for many concepts in algebraic number theory. Their explicit Galois groups, well-understood ramification behavior, and connections to special values of L-functions make them indispensable in modern number theory.

Further study leads to class field theory, Iwasawa theory, and the theory of p-adic L-functions, where cyclotomic fields continue to play a central role.