Notes on Cyclotomic Extensions and Galois Theory

Mathematical Blackboard Transcription

1 Introduction to Cyclotomic Extensions

These notes explore the structure of cyclotomic extensions and their Galois groups. We begin by recalling the definition of a cyclotomic extension and then proceed to analyze its Galois group structure in detail.

2 The n-th Cyclotomic Extension

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

The minimal polynomial of ζ_n over $\mathbb{Q}$ is the n-th cyclotomic polynomial $\Phi_n(x)$, which 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 $(\mathbb{Z}/n\mathbb{Z})^\times$, the multiplicative group of units modulo n.*

Every automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is determined by its action on ζ_n, and we must have $\sigma(\zeta_n) = \zeta_n^a$ for some integer a coprime to n. This gives the isomorphism:

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

The isomorphism sends σ to the residue class of a modulo n.

4 Subfields and Fixed Fields

Let H be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Then the fixed field $\mathbb{Q}(\zeta_n)^H$ is a subfield of $\mathbb{Q}(\zeta_n)$.

Remark 1 *By the Fundamental Theorem of Galois Theory, there is a one-to-one correspondence between subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$ and subfields of $\mathbb{Q}(\zeta_n)$ containing $\mathbb{Q}$.*

5 Example: The Case $n = 8$

Let us consider the specific case where $n = 8$. The primitive 8th roots of unity are $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7$, where $\zeta_8 = e^{2\pi i/8}$.

The Galois group is:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$$

This group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Let us compute the fixed field corresponding to the subgroup $H = \{1, 5\}$. The automorphisms are:

$$\sigma_1 : \zeta_8 \mapsto \zeta_8, \quad \sigma_5 : \zeta_8 \mapsto \zeta_8^5$$

We look for elements fixed by both σ_1 and σ_5. Consider:

$$\alpha = \zeta_8 + \zeta_8^5$$

Since $\zeta_8^5 = -\zeta_8$, we have:

$$\alpha = \zeta_8 - \zeta_8 = 0$$

This is not useful. Instead, consider:

$$\beta = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \zeta_8^7$$

Note that $\zeta_8^7 = \zeta_8^{-1}$. Under σ_5:

$$\sigma_5(\beta) = \zeta_8^5 + \zeta_8^{35} = \zeta_8^5 + \zeta_8^3$$

This is not equal to β.

Let's try a different approach. Consider:

$$\gamma = \zeta_8 + \zeta_8^3$$

Under σ_5:

$$\sigma_5(\gamma) = \zeta_8^5 + \zeta_8^{15} = \zeta_8^5 + \zeta_8^7$$

This is different from γ.

Actually, let's compute the fixed field systematically. The subgroup $H = \{1, 5\}$ has order 2, so the fixed field should have degree $[\mathbb{Q}(\zeta_8) : \mathbb{Q}]/|H| = 4/2 = 2$ over $\mathbb{Q}$.

Consider the element:

$$\theta = \zeta_8 + \zeta_8^5$$

We already computed that $\zeta_8^5 = -\zeta_8$, so:

$$\theta = \zeta_8 - \zeta_8 = 0$$

This is trivial.

Let's try:

$$\eta = \zeta_8^2$$

Then $\eta^2 = \zeta_8^4 = -1$, so $\eta = i$ (a primitive 4th root of unity). Under σ_5:

$$\sigma_5(\eta) = \sigma_5(\zeta_8^2) = (\zeta_8^5)^2 = \zeta_8^{10} = \zeta_8^2 = \eta$$

So η is fixed by H. Therefore, the fixed field is $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$.

6 General Structure

In general, for a subgroup H of $(\mathbb{Z}/n\mathbb{Z})^\times$, the fixed field $\mathbb{Q}(\zeta_n)^H$ consists of all rational linear combinations of ζ_n^a that are invariant under all automorphisms in H.

If H is the subgroup corresponding to $a \equiv 1 \pmod{m}$ for some $m \mid n$, then the fixed field is $\mathbb{Q}(\zeta_m)$.

7 Conclusion

Cyclotomic extensions provide rich examples of abelian Galois extensions over $\mathbb{Q}$. Their Galois groups are well-understood, and the correspondence between subgroups and subfields can be explicitly computed in many cases. The case $n = 8$ illustrates how even simple examples can reveal interesting structure.