

Galois Theory

Robert F. Coleman

Lecture 20

Roots of Unity

Notation: Suppose $n \in \mathbf{Z}$. If $a \in \mathbf{Z}$, $[a]_n$ will denote its congruence class mod n .

The group $\mu_m(K)$ of roots of $x^m - 1$ in K is cyclic for any field K . If K contains a splitting field of $x^m - 1$ and the characteristic of K doesn't divide m , a generator is called a primitive m -th root of unity.

Lemma. *if C is a cyclic group of order n , $\text{Aut}(C) = (\mathbf{Z}/n\mathbf{Z})^*$.*

Proof.

In particular, if ζ is primitive n -th root of unity, ζ^a is primitive if and only if $[a]_n \in (\mathbf{Z}/n\mathbf{Z})^*$. One denotes $|(\mathbf{Z}/n\mathbf{Z})^*|$ by $\phi(n)$.

Let $G_n = \text{Gal}(K_n/\mathbf{Q})$.

Lemma. *We have an injective homomorphism $h: G_n \rightarrow (\mathbf{Z}/n\mathbf{Z})^*$ such that*

$$\sigma\zeta = \zeta^{h(\sigma)} \text{ for } \zeta \in \mu_n.$$

Proof.

Let

$$\Phi_n(T) = \prod_{\substack{\zeta \in \mu_n(K_n) \\ \zeta \text{ is primitive}}} (T - \zeta).$$

Proposition. $\Phi_n(T) \in \mathbf{Z}[T]$.

Proof. First, $\Phi_n(T) \in \mathbf{Q}[T]$ and

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

Lemma. If $f(T), g(T) \in \mathbf{Z}[T]$ are monic and $f(T)/g(T) \in \mathbf{Q}[T]$ then $f(T)/g(T) \in \mathbf{Z}[T]$. ■

Proof of proposition.

Example. $\Phi_{12}(T) = (T^{12} - 1)/$

This is called the n -th **cyclotomic polynomial**.

Lemma. $K_n = \mathbf{Q}(\zeta)$ for any primitive n -root of unity ζ .

Proof.

Proposition. $\Phi_n(T)$ is irreducible.

Proof.

Corollary. $G_n \cong (\mathbf{Z}/n\mathbf{Z})^*$.

Proof.

Read 9.5.

Homework for Monday

Show every finite Abelian group is the Galois group of some finite extension of \mathbf{Q} .

You will need,

Dirichlet's theorem, states that for any two positive coprime integers a and d , there are infinitely many primes of the form $a + nd$, where $n \geq 0$, or in other words: there are infinitely many primes which are congruent to a modulo d .