

Galois Theory

Robert F. Coleman

Lecture 19

Roots of Unity

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

Theorem. *The Galois group over \mathbf{Q} of a splitting field K_n of $x^n - 1$ is naturally isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$. Explicitly, if $[a]_n \neq 0$ and σ_a is the corresponding elt. of $\text{Gal}(K_n/\mathbf{Q})$,*

$$\sigma_a \zeta = \zeta^a,$$

for any root ζ of $x^n - 1$ in K_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. $\text{Aut}(\mathbf{Z}/n\mathbf{Z}) = (\mathbf{Z}/n\mathbf{Z})^*$.

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 $\phi(n)$.

Examples. $(\mathbf{Z}/4\mathbf{Z})^*$

$(\mathbf{Z}/8\mathbf{Z})^*$

$(\mathbf{Z}/3\mathbf{Z})^*$

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

Lemma. *We have a homomorphism $h: G \rightarrow (\mathbf{Z}/n\mathbf{Z})^*$ 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 is a splitting field of $\Phi_n(T)$.

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

Read 9.4.

Homework for Monday

Do exers. 9.4 and 9.8.