

THE GALOIS GROUP OF $x^n - 1$ OVER \mathbb{Q}

Theorem 1. *The Galois group of $x^n - 1$ over \mathbb{Q} is isomorphic to \mathbb{Z}_n^* , the group of units in \mathbb{Z}_n .*

Proof. Let $f(x) = x^n - 1$. Let $\omega \in \mathbb{C}$ be a primitive n^{th} root of unity. Then the roots of f are the powers of ω , and in particular form a cyclic group of order n . Every element $\tau \in \text{Gal}(f)$ is determined by $\tau(\omega)$. Furthermore, we must have

$$\tau(\omega) = \omega^r$$

for a unique r between 1 and n , relatively prime to n . This follows since τ is a group isomorphism on the set of roots and therefore takes ω to a generator. The assignment

$$\tau \mapsto r$$

is a group homomorphism, and imbeds $\text{Gal}(f)$ as a subgroup of \mathbb{Z}_n^* . It remains to show that every element $r \in \mathbb{Z}_n^*$ arises in this way. Let \mathcal{O} denote the orbit of ω under the action of the Galois group. Let $g(x)$ denote the minimal polynomial of ω over \mathbb{Q} . Then

$$g(x) = \prod_{\eta \in \mathcal{O}} (x - \eta) .$$

What we must show therefore is the following claim: For every primitive root of unity ω and every $r \in \mathbb{Z}_n^*$, ω and ω^r have the same minimal polynomial. By induction on the number of primes appearing in a factorization of r , the claim reduces to the following claim: For every prime p not dividing n ,

$$g(\omega^p) = 0 .$$

We prove this by contradiction. Let $h(x)$ be the minimal polynomial of ω^p , and assume that $h \neq g$. Then h and g are distinct irreducible factors of f . Since $h(\omega^p) = 0$, the polynomial $g(x)$ divides $h(x^p)$. A key point here is that, since g and h are monic factors of f , they are polynomials over \mathbb{Z} . Hence it makes sense to consider their reductions mod p . Denoting this reduction by $(\bar{\cdot})$, we have

$$\bar{g}(x) | \bar{h}(x^p) = \bar{h}(x)^p$$

This implies that \bar{g} and \bar{h} have a nontrivial common factor in $\mathbb{F}_p(x)$. But \bar{g} and \bar{h} are distinct factors of \bar{f} , which implies that \bar{f} has a repeated factor. This happens if and only if \bar{f} and \bar{f}' have a common

factor. But $\bar{f}' = \bar{n}x^{n-1}$, and $\bar{n} \neq 0$. We have reached a contradiction. \square

Definition 2. *The n^{th} cyclotomic polynomial over is the polynomial*

$$\Psi_n(x) = \prod_{\omega} (x - \omega)$$

as ω runs over the primitive n^{th} roots of unity in \mathbb{C} .

Corollary 3. *The cyclotomic polynomials have coefficients in \mathbb{Z} . They are irreducible over \mathbb{Z} and therefore over \mathbb{Q} . Furthermore, one has the following factorization of $x^n - 1$:*

$$x^n - 1 = \prod_{d|n} \Psi_d(x) .$$