Roots of Unity & Field Theory

Skyler Hu

October 29, 2025

Contents

1 Introduction

In this handout we will explore the significance of roots of unity in Galois theory, and in abstract algebra in general. Roots of unity have always been an intriguing object of study over the evolution of mathematics: not only are they the solution to the simple and beautiful polynomials $x^n - 1 = 0$, they also have interesting algebraic structures with various applications. In addition, they can be considered to pave the way for the discovery of complex numbers, since they are the simplest complex numbers to attain in an algebraic sense.

We will briefly cover properties of the roots of unity as a group, then move on to roots of unity and field theory with cyclotomic extensions (field extensions obtained by adjoining certain roots of unity), Galois groups and the ultimate question of solvability by radicals. We will see the crucial structure the roots of unity brings to a field and the implications they have on solving a polynomial.

2 Roots of Unity: Overview

Definition 2.1. (Roots of Unity.) The nth roots of unity are the n solutions to the polynomial $x^n - 1$ over $\mathbb{C}$.

Corollary 2.1. (nth roots of unity form a group.) The nth roots of unity form a cyclic group of order n under multiplication.

Proof. We only need to verify the group axioms for roots of unity:

1. **Closure.** Let ζ_1, ζ_2 be two nth roots of unity. Then $(\zeta_1\zeta_2)^n = (\zeta_1)^n(\zeta_2)^n = 1$, so the nth roots of unity is closed under multiplication.

2. **Associativity.** Follows from the associativity of multiplication.

3. **Identity.** The identity is 1, which is an nth root of unity for any n.

4. **Inverse.** For nth root of unity ζ, $\frac{1}{\zeta}^n = \frac{1}{\zeta^n} = 1$, so the nth roots of unity are closed under inverses. Therefore the nth roots of unity form a group. Furthermore, this group is cyclic because we know that the nth roots of unity are precisely

   $$e^{\frac{2\pi ik}{n}} \text{ for integer } k < n,$$

   and $e^{\frac{2\pi i}{n}}$ is a generator. Similarly, for all $\gcd(k, n) = 1$, $e^{\frac{2\pi ik}{n}}$ is a generator for the group of the nth roots of unity.
   The group of nth roots of unity is denoted μ_n.

□

Since we have shown that the roots of unity form a cyclic group, we can define the *primitive roots of unity* as the set of its generators:

Definition 2.2. (Primitive Roots of Unity.) The nth primitive roots of unity are the generators of μ_n.

Some important results concerning μ_n:

Corollary 2.2. (Properties.)

1. If ζ is a dth root of unity and $d \mid n$, ζ is also an nth root of unity. Hence $\mu_d \leq \mu_n$ for all $d \mid n$.

2. Conversely, if ζ is an nth root of unity which is also a dth root of unity ($d \leq n$), then $d \mid n$. The order of ζ in μ_n is d.

3 Cyclotomic Polynomials

Definition 3.1. (Cyclotomic Polynomials.) The nth cyclotomic polynomial $\phi_n(x)$ is the polynomial whose roots are the primitive nth roots of unity:

$$\phi_n(x) = \prod_{\zeta \text{ is a primitive nth root of unity}} (x - \zeta).$$

Some properties of the cyclotomic polynomial:

Theorem 3.1. The nth cyclotomic polynomial $\phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$, where φ denotes Euler's Totient Function, the number of naturals less than or equal to n that are coprime with n.

Proof. It is clear that $\phi_n(x)$ is a monic polynomial. Since there are $\varphi(n)$ primitive nth roots of unity, the degree of $\phi_n(x)$ is $\varphi(n)$. We only need to prove that the coefficients of $\phi_n(x)$ lie in $\mathbb{Z}$.
Proof by Induction.
Base Case. The 1st cyclotomic polynomial is $x - 1$, which clearly has all coefficients in $\mathbb{Z}$.
Inductive Hypothesis. Suppose that the statement is true for $1 \leq d \leq n$. We have

$$x^n - 1 = \phi_n(x)(\prod_{d|n, d<n} \phi_d(x)).$$

Now we know that $x^n - 1$ and $f(x) = \prod_{d|n,d<n} \phi_d(x)$ all have integer coefficients, and $f(x)$ divides $x^n - 1$ in $\mathbb{Q}(\zeta)$, the field extension of the nth roots of unity over the rationals, so $f(x)$ divides $x^n - 1$ in $\mathbb{Q}$ and therefore in $\mathbb{Z}$ by Gauss's Lemma. □

Theorem 3.2. (Cyclotomic Polynomial is irreducible) The nth cyclotomic polynomial $\phi_n(x)$ is a monic *irreducible* polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$.

Proof. We only need to show that $\phi_n(x)$ is irreducible over $\mathbb{Z}$.
Suppose, for a contradiction, that $\phi_n(x) = f(x)g(x)$ for monic $f(x), g(x) \in \mathbb{Z}[x]$. Let ζ be a root of $\phi_n(x)$ and $f(x)$ be the minimal polynomial of ζ over $\mathbb{Z}$. Let p be a prime not dividing n. Then ζ^p is a primitive nth root of unity, and is therefore a root of either $f(x)$ or $g(x)$.
Case 1. ζ^p is a root of $g(x)$.
Then ζ is a root of $g(x^p)$. Since $f(x)$ is the minimal polynomial of ζ, $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$:

$$g(x^p) = f(x)h(x)textforsomeh(x) \in \mathbb{Z}[x].$$

Reducing mod p gives us $g(\bar{x^p}) = f(x)\bar{h}(\bar{x})$ in F_p. Using the fact that $g(\bar{x^p}) = (g(x))^p$:

$$(g(x))^p = f(\bar{x})h(\bar{x}) \text{ in } F_p.$$

Therefore $g(x)$ and $f(x)$ have a factor in common in $F_p[x]$.
Similarly, we can reduce the cyclotomic polynomial mod p:

$$\phi_n\bar{(x)} = f(\bar{x})\bar{(}g(x)) \text{ in } F_p[x].$$

Since $f(x)$ and $g(x)$ share a root in $F_p[x]$, $\phi_n(x)$ has a multiple root, contradicting the separability of $x^n - 1$. This case gives a contradiction and is therefore invalid.

Case 2. ζ^p is a root of $f(x)$.
This applies to every ζ a root of $\phi_n(x)$, so $\phi_n(x) = f(x)$, and $\phi_n(x)$ is irreducible. □

We can conclude from the above theorem:

Corollary 3.1. The degree over $\mathbb{Q}$ of the cyclotomic field (field containing all the nth roots of unity) $\mathbb{Q}(\zeta_n)$ is $\varphi(n)$:

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$$

.

Proof. The minimal polynomial of any primitive nth root of unity is $\phi_n(x)$ with degree $\varphi(n)$. Note that the primitive nth roots of unity generate the nth roots of unity, so $\mathbb{Q}$ adjoined the primitive nth roots of unity is exactly $\mathbb{Q}$ adjoined the nth roots of unity. Since $phi_n(x)$ is separable, the degree of $\mathbb{Q}(\zeta_n)$ is exactly the number of primitive nth roots of unity, which is $\varphi(n)$. □