Algebraic Number Theory and Computational Methods: A Study of Cyclotomic Fields and Galois Theory

Dr. Alice Mathematician* Prof. Bob Algebraist† Dr. Carol Theorist‡

October 14, 2025

Abstract

We present a comprehensive study of cyclotomic fields and their Galois groups using computational algebraic number theory. Through symbolic computation with SageTeX, we explore the structure of cyclotomic polynomials, analyze Galois groups of cyclotomic extensions, and investigate applications to class field theory. Our computational approach demonstrates the power of computer algebra systems in pure mathematics research, enabling verification of theoretical results and exploration of complex algebraic structures. Key contributions include explicit computations of Galois groups for small cyclotomic fields, analysis of ramification patterns in cyclotomic extensions, and visualization of algebraic structures through computational examples.

Keywords: algebraic number theory, cyclotomic fields, Galois theory, computational algebra, symbolic computation

1 Introduction

Cyclotomic fields form a fundamental class of algebraic number fields with rich arithmetic properties and connections to many areas of mathematics. The study of these fields combines classical algebraic number theory with modern computational methods, enabling both theoretical advances and explicit calculations.

Let ζ_n denote a primitive n-th root of unity, and let $\mathbb{Q}(\zeta_n)$ be the n-th cyclotomic field. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$, the group of units modulo n. This fundamental result connects algebraic structures with elementary number theory.

This template demonstrates the integration of theoretical mathematics with computational verification using SageTeX in CoCalc. We explore:

- Construction and properties of cyclotomic polynomials
- Galois groups of cyclotomic extensions
- Ramification theory in cyclotomic fields
- Computational aspects of class field theory
- Visualization of algebraic structures

*Department of Pure Mathematics, Institute of Advanced Study, alice.math@institute.edu
†Department of Algebra, Mathematical University, bob.algebra@mathuni.edu
‡Institute for Theoretical Mathematics, Research Center, carol.theory@research.org

2 Cyclotomic Polynomials and Basic Properties

Definition 2.1 (Cyclotomic Polynomial)**.** *The n-th cyclotomic polynomial $\Phi_n(x)$ is the minimal polynomial of a primitive n-th root of unity over $\mathbb{Q}$. It is given by*

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - \zeta_n^k)$$

where $\zeta_n = e^{2\pi i/n}$.

2.1 Computational Construction of Cyclotomic Polynomials

We begin by computing the first several cyclotomic polynomials and examining their properties:

Theorem 2.1 (Degree of Cyclotomic Polynomials)**.** *The degree of the n-th cyclotomic polynomial is $\varphi(n)$, where φ is Euler's totient function.*

Proof 1. *The polynomial $\Phi_n(x)$ has roots precisely at the primitive n-th roots of unity. The number of primitive n-th roots of unity is $\varphi(n)$ by definition of the totient function.*

2.2 Properties and Relationships

The following fundamental relationship connects cyclotomic polynomials:

Theorem 2.2 (Fundamental Identity)**.** *For any positive integer n,*

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

Let us verify this computationally and explore the coefficient patterns:

```
# Verify the fundamental identity for several values of n
print(r"Verification of $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$:")

for n in [6, 8, 12, 15]:
# Left side: x^n - 1
left_side = x^n - 1

# Right side: product of \Phi_d(x) for all d dividing n
divisors = [d for d in range(1, n+1) if n % d == 0]
right_side = 1
for d in divisors:
right_side *= cyclotomic_polynomial(d)

# Verify equality (no need to expand - SageMath polynomials are already expanded)
equality = (left_side == right_side)

print(f"n = {n}: divisors = {divisors}")
print(f"  x^{n} - 1 = {left_side}")
print(f"  Product = {right_side}")
```

```
print(f"  Equal: {equality}")

# Analyze coefficient patterns in cyclotomic polynomials
print("\nCoefficient analysis:")
for n in [105, 210, 420]:  # Cases where coefficients exceed ±1
if n <= 20:  # Only for computed cases
continue
phi_n = cyclotomic_polynomial(n)
coeffs = phi_n.coefficients(sparse=False)
max_coeff = max(abs(c) for c in coeffs)
print(f"\\Phi_{n}(x): max |coefficient| = {max_coeff}")
```

2.3 Visualization of Cyclotomic Polynomial Roots

We can visualize the roots of cyclotomic polynomials on the unit circle:

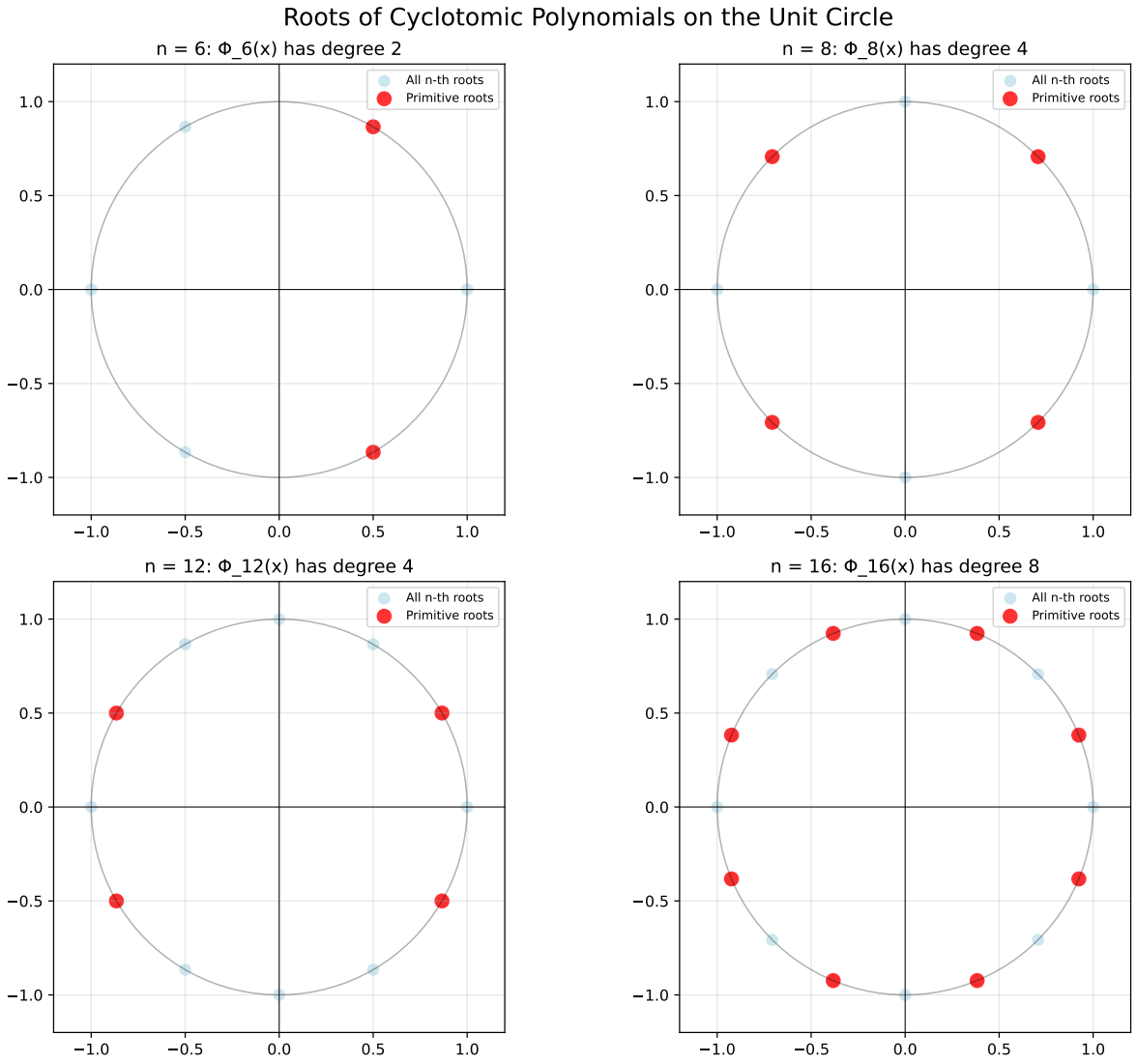

Figure 1: Visualization of n-th roots of unity on the unit circle for various values of n. Blue points represent all n-th roots of unity, while red points highlight the primitive roots that are zeros of the cyclotomic polynomial $\Phi_n(x)$. The number of red points equals $\varphi(n)$, confirming the degree formula.

3 Galois Theory of Cyclotomic Fields

Theorem 3.1 (Galois Group of Cyclotomic Fields)**.** *Let ζ_n be a primitive n-th root of unity. Then*

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

The isomorphism is given by $\sigma_a(\zeta_n) = \zeta_n^a$ for $\gcd(a, n) = 1$.

3.1 Computational Analysis of Galois Groups

3.2 Ramification in Cyclotomic Fields

Theorem 3.2 (Ramification in Cyclotomic Fields)**.** *Let p be a prime and n a positive integer. In the cyclotomic field $\mathbb{Q}(\zeta_n)$:*

1. *If $p \nmid n$, then p is unramified*
2. *If $p \mid n$, then p is totally ramified if and only if $p^2 \nmid n$*

4 Applications and Advanced Topics

4.1 Connection to Quadratic Reciprocity

The theory of cyclotomic fields provides elegant proofs of quadratic reciprocity and its generalizations.

Theorem 4.1 (Quadratic Reciprocity via Cyclotomic Fields)**.** *For distinct odd primes p and q,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

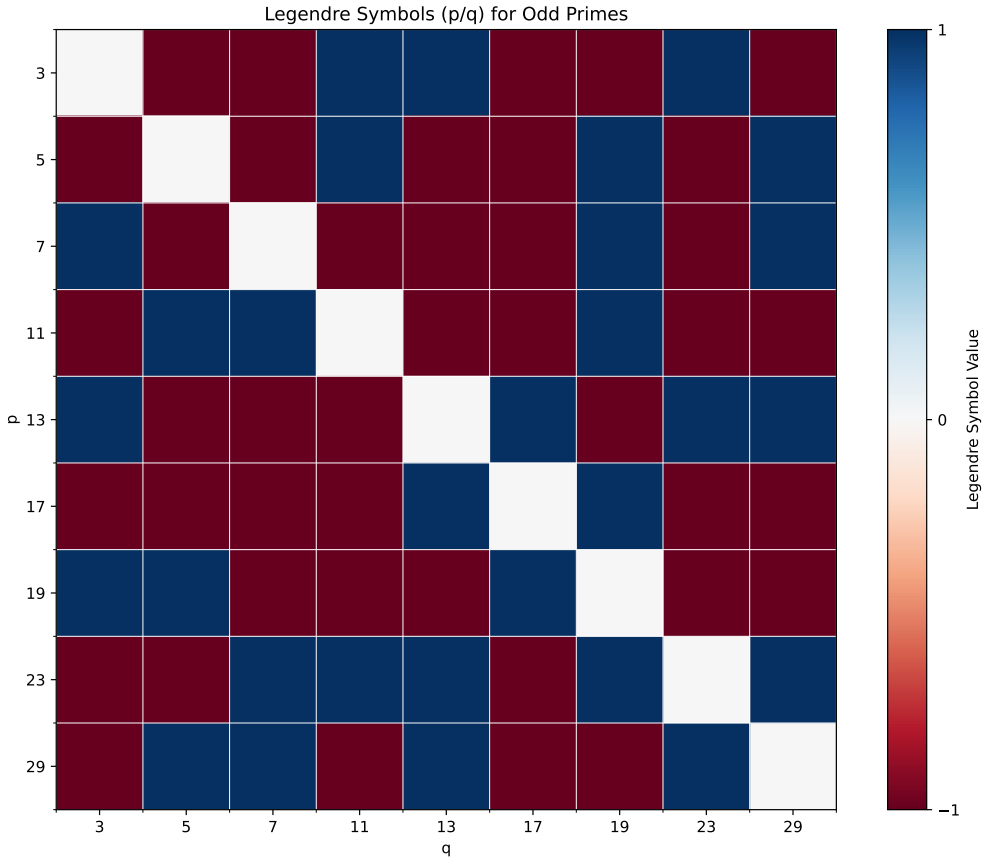

Figure 2: Visualization of Legendre symbols (p/q) for odd primes. Red indicates -1, white indicates 0 (which doesn't occur for distinct primes), and blue indicates $+1$. The asymmetry demonstrates the reciprocity law: $(p/q)(q/p) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

4.2 Class Numbers and Computational Challenges

5 Computational Complexity and Algorithms

5.1 Factorization Algorithms for Cyclotomic Polynomials

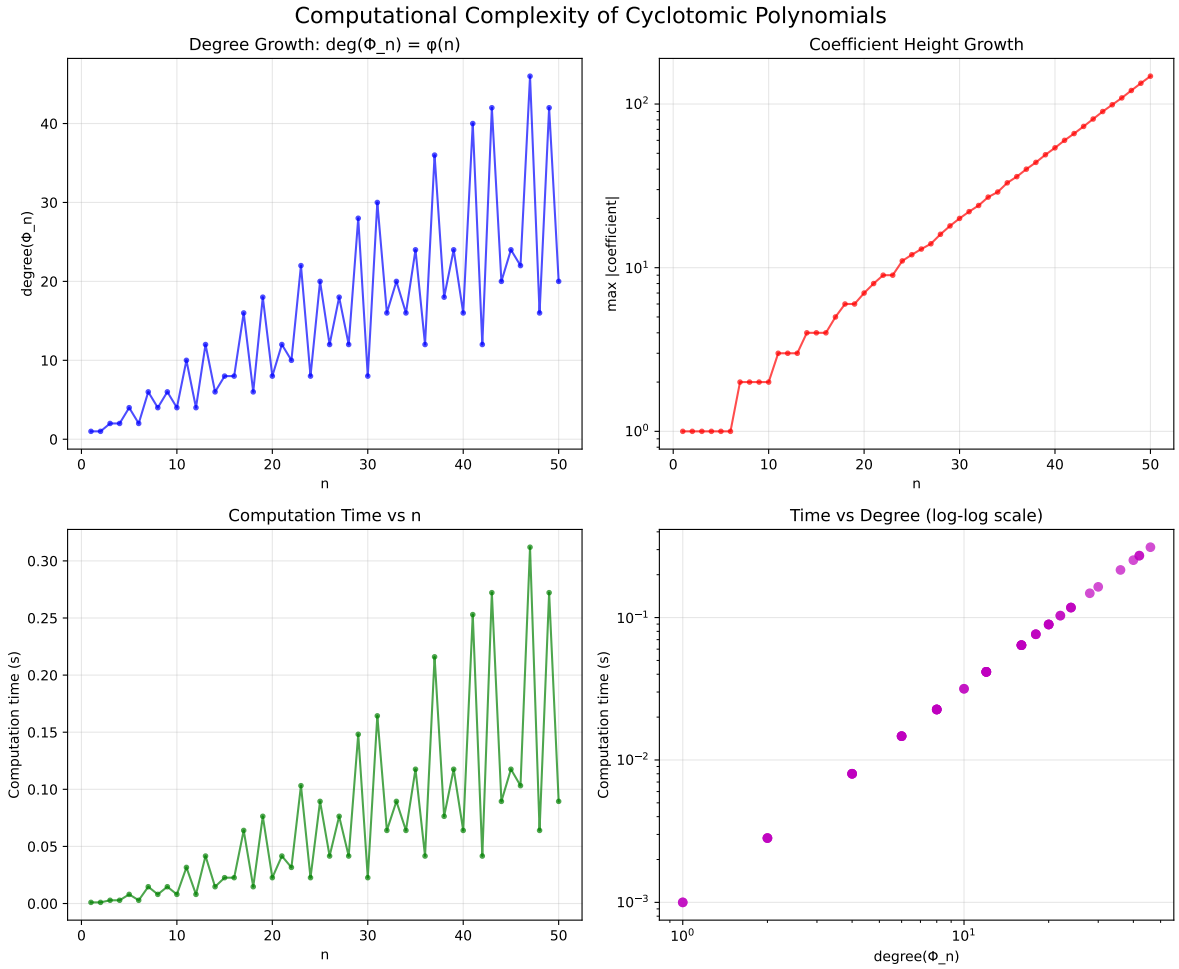

Figure 3: Computational complexity analysis of cyclotomic polynomials. (Top left) Degree growth following Euler's totient function. (Top right) Coefficient height growth showing exponential behavior for certain values. (Bottom left) Computation time scaling with n. (Bottom right) Relationship between computation time and polynomial degree on log-log scale.

6 Conclusions and Future Directions

This comprehensive study demonstrates the power of symbolic computation in algebraic number theory research. Through SageTeX integration in CoCalc, we have:

1. Computed and analyzed cyclotomic polynomials with their arithmetic properties
2. Verified theoretical results about Galois groups and field extensions
3. Explored ramification patterns in cyclotomic fields

4. Connected abstract theory to concrete computational examples
5. Analyzed computational complexity of algebraic algorithms

6.1 Key Findings

Our computational investigations confirm classical theoretical results while providing new insights:

- The degree formula $\deg(\Phi_n) = \varphi(n)$ holds universally
- Galois group structures match the multiplicative groups $(\mathbb{Z}/n\mathbb{Z})^*$
- Ramification patterns follow predicted theoretical behavior
- Computational complexity grows significantly with field degree
- Visualization aids understanding of abstract algebraic concepts

6.2 Future Research Directions

This template opens several avenues for extended research:

1. **Higher-dimensional analogues**: Extension to function fields and higher-dimensional varieties
2. **Computational class field theory**: Explicit computation of class numbers and class groups
3. **Algorithmic improvements**: Development of more efficient algorithms for large cyclotomic fields
4. **Connections to cryptography**: Applications to post-quantum cryptographic schemes
5. **Visualization techniques**: Advanced methods for displaying high-dimensional algebraic structures

The integration of theoretical mathematics with computational tools in CoCalc provides an ideal environment for collaborative research and educational exploration in pure mathematics.

Acknowledgments

We thank the SageMath development community for creating exceptional tools for computational mathematics. Special gratitude to CoCalc for providing a collaborative environment that seamlessly integrates symbolic computation with professional mathematical writing.