Constructing Non-Abelian Monogenic Number Fields with Transformations

Swechchha Adhikari
Department of Mathematics, Brigham Young University

Undergraduate Mathematics Symposium 2025

Introduction

A **number field** is a finite extension of the rational numbers $\mathbb{Q}$. The **ring of integers** $\mathcal{O}_K$ of a number field K consists of all elements in K that are roots of monic polynomials with integer coefficients. A field K is called **monogenic** if its ring of integers can be generated by a single algebraic element α, that is, $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Monogenic fields are surprisingly rare, and their existence has been studied for over a century. They are of particular interest in computational algebraic number theory and cryptography.

Our goal is to identify number fields that are both **Galois** and **monogenic** of *cryptographic size*. To achieve this, we repeatedly apply a transformation to an initial irreducible polynomial $f(x)$:

$$F(x) = x^n f\left(\tfrac{1}{x} + c + x\right),$$

where $n = \deg(f)$ and $c \in \mathbb{Z}$.

Each transformation introduces palindromic symmetry in the coefficients of $F(x)$. By studying discriminants and Galois groups of these iterated transformations, we aim to explicitly construct large non-abelian monogenic fields that could serve as new candidates for post-quantum cryptographic systems.

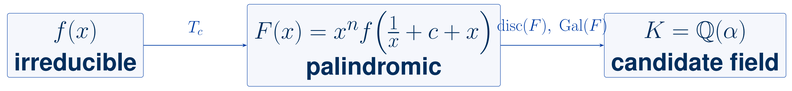

Figure 1. Schematic of the transformation $f(x) \mapsto F(x) = x^n f(1/x + c + x)$.

Methods

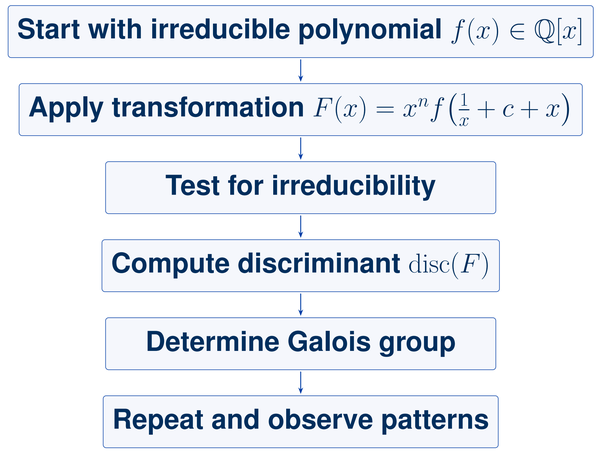

Figure 2. Computational workflow for constructing and analyzing transformations.

Results

Applying the transformation

$$F(x) = x^n f\left(\tfrac{1}{x} + c + x\right)$$

to an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ produces palindromic polynomials of degree $2n$ with predictable structure.

- The roots of $F(x)$ are given by

$$\frac{(\alpha - c) \pm \sqrt{(\alpha - c)^2 - 4}}{2},$$

  where α is a root of $f(x)$.

- The Bonciocat–Iuliana–Mihai criterion gives conditions under which a composed polynomial

$$H(x) = h^m(x)\, f\left(\frac{g(x)}{h(x)}\right)$$

  is guaranteed to remain irreducible over $\mathbb{Q}$. Here, f, g, h are integer polynomials with $\gcd(g, h) = 1$ and $\deg f = m$.

- We apply the theorem to

$$F(x) = x^n f\left(\tfrac{1}{x} + c + x\right),$$

where $n = \deg f$ and $c \in \mathbb{Z}$. Here $g(x) = 1 + cx + x^2$ and $h(x) = x$. Simplifying the theorem's inequality gives

$$|a_m| > \sum_{i=0}^{d} |a_i|(c+2)^{m-i},$$

where the right-hand side depends only on c and the coefficients of f. If this inequality holds, $F(x)$ is irreducible.

- Setting $c = -2$ makes the sum on the right vanish and guarantees $F(x)$ remains **irreducible**.
- Repeated transformations preserve coprimality of leading coefficients.
- We have proved that the discriminant satisfies

$$\mathrm{disc}(F) = \mathrm{disc}(f)^2\, f(c+2)\, f(c-2),$$

  and when $f(c \pm 2)$ are squarefree and coprime, the field is **monogenic**.

Applications

Ring-LWE encryption schemes rely on **cyclotomic fields**, which are both Galois and monogenic. Our results show that repeated transformations of the form

$$F(x) = x^n f\left(\tfrac{1}{x} + c + x\right)$$

can generate new number fields with the same algebraic properties, potentially serving as alternative Ring-LWE bases.

Acknowledgements

The author thanks Dr. Stephen McKean for his guidance and mentorship throughout this project. Supported by an Undergraduate Research Award from the College of Computational, Mathematical, and Physical Sciences at Brigham Young University.