

International Journal of Statistics and Applied Mathematics

ISSN: 2456-1452
NAAS Rating (2026): 4.49
Maths 2026; 11(7): 112-116
© 2026 Stats & Maths
<https://www.mathsjournal.com>
Received: 06-04-2026
Accepted: 10-05-2026

Anchal Vasuniya
Department of Allied Science
(Mathematics), Mandsaur
University, Mandsaur, Madhya
Pradesh, India

Md Afzal
Department of Allied Science
(Mathematics), Mandsaur
University, Mandsaur, Madhya
Pradesh, India

Kapil Kumar
Department of Engineering
(Civil Engineering), Jharkhand
University of Technology,
Ranchi, Jharkhand, India

Corresponding Author:
Anchal Vasuniya
Department of Allied Science
(Mathematics), Mandsaur
University, Mandsaur, Madhya
Pradesh, India

Modern horizons of Galois theory: Computational complexity, post-quantum cryptography, and equivariant AI

Anchal Vasuniya, Md Afzal and Kapil Kumar

DOI: <https://www.doi.org/10.22271/math.2026.v11.i7b.2627>

Abstract

Galois Theory represents one of the most elegant and unifying frameworks in mathematics, bridging abstract algebra, geometry, and number theory. While historically conceived to resolve the solvability of polynomial equations by radicals, its modern extensions permeate computational complexity, cryptography, and artificial intelligence. This paper presents a comprehensive study of classical Galois Theory, its computational paradigms, and its engineering applications. To establish significant novelty over the existing literature, we introduce three new mathematical developments: (1) the formal integration of cyclotomic Galois groups within Ring Learning With Errors (Ring-LWE) for lattice-based post-quantum cryptography, (2) the conceptual and mathematical formulation of Galois-Equivariant Neural Networks (GENNs) that exploit automorphism actions to enforce symmetry invariants over algebraic number fields, and (3) a Galois solvability analysis of high-degree algebraic systems arising from the discretization of magnetohydrodynamic (MHD) boundary-layer flow equations. Additionally, we analyze the implementation of Stauduhar's method and resolvent computations within software suites like MAGMA, GAP, and SageMath. Our synthesis demonstrates that the structural symmetries identified by Galois remain critical to the design of next-generation secure and intelligent systems.

Keywords: Galois theory, computational algebra, post-quantum cryptography, Ring-LWE, equivariant neural networks, magnetohydrodynamics, algebraic solvability

Introduction

The inception of Galois Theory in the early 19th century by Evariste Galois marked a paradigm shift in algebra. Instead of searching for ad-hoc formulas to solve algebraic equations, Galois investigated the underlying symmetries of the roots of polynomials. By associating a group of permutations with each polynomial, now known as the Galois Group, he established the definitive criterion for whether a polynomial equation can be solved using basic arithmetic operations and radicals.

In the nearly two centuries since its formulation, Galois Theory has evolved far beyond its classical roots. Today, it serves as a cornerstone of algebraic number theory, algebraic geometry, and arithmetic geometry. Moreover, with the advent of digital computers, the theoretical constructs of Galois Theory have been translated into concrete algorithmic procedures. Modern computer algebra systems (CAS) such as MAGMA [4], GAP [5], and SageMath [6] routinely compute Galois groups of high-degree polynomials, providing researchers with tools to verify conjectures and explore complex algebraic structures.

Crucially, the utility of Galois Theory is no longer confined to pure mathematics. Its structural concepts have found fertile ground in several applied domains:

- 1. Cryptography and Coding Theory:** Finite fields (Galois fields) are the bedrock of symmetric cryptography (e.g., the Advanced Encryption Standard, AES) and error-correcting codes (e.g., Reed-Solomon codes) [8].
- 2. Post-Quantum Cryptography (PQC):** Lattice-based cryptosystems, particularly those utilizing Ring-Learning with Errors (Ring-LWE) [9], rely on the arithmetic of cyclotomic fields and their Galois groups to secure data against quantum attacks.

3. **Artificial Intelligence (AI):** Group-equivariant neural networks exploit mathematical symmetries to achieve sample efficiency and robustness^[11, 12]. Galois groups provide a natural mechanism to define equivariance over algebraic structures.
4. **Physical and Engineering Systems:** Discretized boundary-layer equations in fluid mechanics and magnetohydrodynamics (MHD) yield complex systems of algebraic equations^[13, 14]. Galois Theory provides analytical limits on the solvability of these discretized systems.

This paper explores these modern horizons. In addition to reviewing the classical foundations and computational algorithms, we introduce novel integrations of Galois Theory in Ring-LWE, Equivariant AI, and MHD modeling, providing a unified perspective on the algebraic structure of secure and physical systems.

Mathematical Foundations of Galois Theory

To set the stage, we recall the fundamental definitions and theorems of Galois Theory. Let F be a field, and let K be an extension field of F , denoted by K/F . The degree of the extension, $[K:F]$, is the dimension of K as a vector space over F .

Definition 2.1 (Galois Group). The Galois group of a field extension K/F , denoted by $\text{Gal}(K/F)$, is the group of all automorphisms of K that fix F pointwise:

$$\text{Gal}(K/F) = \{\sigma \in \text{Aut}(K) \mid \sigma(\alpha) = \alpha \forall \alpha \in F\}. \quad (2.1)$$

An extension K/F is called Galois if it is both normal (it is the splitting field of a family of polynomials in $F[x]$) and separable (the minimal polynomial of every element in K has distinct roots)^[1, 2].

Theorem 2.2 (Fundamental Theorem of Galois Theory). *Let K/F be a finite Galois extension with Galois group $G = \text{Gal}(K/F)$. There is a bijection between the set of intermediate fields M ($F \subseteq M \subseteq K$) and the set of subgroups H of G , given by:*

$$M' \rightarrow \text{Gal}(K/M), H' \rightarrow KH, \quad (2.2)$$

Where $K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \forall \sigma \in H\}$ is the fixed field of H . Moreover, the extension M/F is normal if and only if $H = \text{Gal}(K/M)$ is a normal subgroup of G , in which case $\text{Gal}(M/F) \cong G/H$ ^[1, 2, 3].

Solvability by Radicals

The historical culmination of Galois Theory is the resolution of solvability by radicals. A polynomial $f(x) \in F[x]$ is solvable by radicals if its splitting field K can be embedded in a radical extension of F (an extension obtained by sequentially adjoining roots of elements).

Definition 2.3 (Solvable Group). *A group G is solvable if it has a subnormal series:*

$$\{1\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G, \quad (2.3)$$

Such that each factor group H_{i+1}/H_i is abelian.

Theorem 2.4 (Galois' Theorem on Solvability). A polynomial equation $f(x) = 0$ is solvable by radicals if and only if its Galois group $\text{Gal}(K/F)$ is a solvable group, where K is the splitting field of $f(x)$ over F ^[2].

Since the symmetric group S_n is not solvable for $n \geq 5$ (its alternating subgroup A_n is simple and non-abelian for $n \geq 5$), the general polynomial equation of degree 5 or higher cannot be solved by radicals, which is the famous Abel-Ruffini theorem.

Resolvent Polynomials and Discriminants

In practice, determining the Galois group of a polynomial $f(x)$ of degree n involves identifying it as a subgroup of the symmetric group S_n . The primary algebraic tools for this task are discriminants and resolvent polynomials.

The discriminant of a monic polynomial $F(X) = \prod_{i=1}^n (x_i - \alpha_i)$ with roots $\alpha_1, \dots, \alpha_n$ is defined by.

$$D(F) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \quad (3.1)$$

The discriminant is a symmetric function of the roots, and thus $D(f) \in F$. It is closely related to the Galois group:

Proposition 3.1. Let $f(x) \in F[x]$ be a separable polynomial with Galois group $G \subseteq S_n$. Then G is contained in the alternating group A_n if and only if the discriminant $D(f)$ is a square in F ^[2].

To distinguish between subgroups of S_n that are both contained in (or contain) A_n , one utilizes Galois resolvents. Let $P(X_1, \dots, X_n)$ be a polynomial in $F[X_1, \dots, X_n]$, and let H be the stabilizer of P under the natural action of S_n . The resolvent polynomial is defined as:

$$R(y) = \prod_{\sigma \in S_n/H} (y - p(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})) \quad (3.2)$$

The coefficients of $R(y)$ are symmetric under S_n and thus lie in F . The distribution of the roots of $R(y)$ in F provides information about the Galois group of $f(x)$. For example, if $R(y)$ has a root in F , then the Galois group is conjugate to a subgroup of H .

Computational Galois Theory and Modern Software

The algebraic formulations of Galois Theory have been implemented in computer algebra systems, transforming abstract proofs into computational procedures.

Software Platforms: MAGMA, GAP, and SageMath

MAGMA: Highly optimized for group theory, algebraic geometry, and number theory. It implements advanced algorithms for computing Galois groups over the rational field $\mathbb{Q}$, function fields, and local fields.

GAP (Groups, Algorithms, and Programming): Designed specifically for computational group theory. It excels in analyzing the structure of Galois groups once they are represented permutationally.

SageMath: An open-source Python-based system that integrates GAP, Maxima, and Singular, providing a unified interface for algebraic computations.

Stauduhar's Algorithm

For polynomials over $\mathbb{Q}$, the standard method for computing the Galois group is Stauduhar's algorithm^[7]. It operates in a top-down fashion:

1. Initialize the candidate group as the symmetric group S_n (or A_n if the discriminant is a square).
2. Find a maximal subgroup U of the current candidate group G .
3. Construct a G -relative U -invariant polynomial $P(X_1, \dots, X_n)$.
4. Evaluate the corresponding resolvent polynomial at the roots of $f(x)$ computed to high numerical precision.
5. If the resolvent has an integer root (verified using rigorous bounds), the Galois group is conjugate to a subgroup of U . The candidate group is updated to U , and the process repeats.
6. If no maximal subgroup contains the Galois group, the candidate group is the Galois group.

Galois Applications in Cryptography (With PQC Novelty) Classical Symmetric Cryptography

In symmetric cryptography, Galois fields (finite fields) of the form $GF(2^k)$ are widely used. The Advanced Encryption Standard (AES) operates on bytes, which are treated as elements of the field $GF(2^8) \cong F_2[x]/(x^8 + x^4 + x^3 + x + 1)$ [8]. The S-box operation,

Which provides the non-linear confusion step in AES, is defined by the multiplicative Inverse map:

$$f: GF(2^8) \rightarrow GF(2^8) \alpha \rightarrow \begin{cases} \alpha^{-1}, & \alpha \neq 0 \\ 0, & \alpha = 0 \end{cases} \quad (5.1)$$

Followed by an affine transformation over F_2 . The algebraic structure of $GF(2^8)$ ensures optimal resistance to linear and differential cryptanalysis [8].

Novel Addition: Cyclotomic Galois Groups in Ring-LWE Post-Quantum Cryptography

With the advent of quantum computing, classical public-key cryptosystems (RSA, ECC) are vulnerable to Shor's algorithm. Lattice-based cryptography, specifically the Ring-Learning with Errors (Ring-LWE) problem, has emerged as a leading alternative, forming the basis of standards like CRYSTALS-Kyber [10, 9].

Let $\Phi_m(x)$ be the m -th cyclotomic polynomial of degree $n = \phi(m)$. The quotient ring:

$$R = Z[x]/(\Phi_m(x)) \quad (5.2)$$

Is the ring of integers of the cyclotomic field $K = Q(\zeta_m)$, where $\zeta_m = e^{2\pi i/m}$. The Galois extension K/Q is abelian, with Galois group:

$$G = \text{Gal}(K/Q) \cong (Z/mZ)^*. \quad (5.3)$$

Each element $g \in (Z/mZ)^*$ corresponds to an automorphism $\sigma_g \in G$ defined by its action on the primitive root:

$$\sigma_g(\zeta_m) = \zeta_m^g. \quad (5.4)$$

In Ring-LWE, we sample a secret $s \in R_q = R/qR$ and an error $e \in R_q$ according to a discrete Gaussian distribution. The adversary observes pairs $(a, b) \in R_q \times R_q$ where:

$$b = a \cdot s + e \pmod{q}. \quad (5.5)$$

The security of Ring-LWE is tied to the hardness of finding s . We propose a novel integration where the Galois automorphisms σ_g are utilized to define a homomorphic key-

switching mechanism. Since σ_g is a ring automorphism, we can apply it to the Ring-LWE sample:

$$\sigma_g(b) = \sigma_g(a) \cdot \sigma_g(s) + \sigma_g(e) \pmod{q}. \quad (5.6)$$

Let $a' = \sigma_g(a)$, $b' = \sigma_g(b)$, $s' = \sigma_g(s)$, and $e' = \sigma_g(e)$. Then (a', b') is a valid Ring-LWE sample under the permuted secret s' .

Because the Galois action preserves the algebraic norms, it also preserves the noise distribution:

$$\|\sigma_g(e)\| = \|e\|, \quad (5.7)$$

Where $\|\cdot\|$ denotes the canonical embedding norm [9]. Equation (5.7) guarantees that applying Galois automorphisms does not increase the noise of the ciphertexts, which is a critical constraint in homomorphic encryption schemes (such as BGV and BFV). This property allows for efficient rotation of ciphertexts in multi-party homomorphic computations.

Galois Theory in Machine Learning (With GENN Novelty)

Group-equivariant neural networks (G-CNNs) enforce symmetry constraints on deep learning architectures, guaranteeing that if an input is transformed by a group element, the output is transformed accordingly [11, 12].

Novel Addition: Galois-Equivariant Neural Networks (GENNs)

We introduce the concept of Galois-Equivariant Neural Networks (GENNs). Consider a neural network designed to process features defined over algebraic number fields. Let K/F be a Galois extension of degree n , and let $G = \text{Gal}(K/F)$ be the Galois group.

Let the input space V be a vector space over K , representing algebraic features. The Galois group G acts on V by applying the automorphism component-wise:

$$\sigma \cdot v = (\sigma(v_1), \dots, \sigma(v_d))^T, v \in K^d, \sigma \in G. \quad (6.1)$$

A neural network layer $L: K^d \rightarrow K^m$ is defined to be Galois-equivariant if:

$$L(\sigma \cdot v) = \sigma \cdot L(v) \forall \sigma \in G, v \in K^d. \quad (6.2)$$

Consider a linear layer defined by a weight matrix $W \in K^{m \times d}$ and a bias vector $b \in K^m$:

$$L(v) = Wv + b. \quad (6.3)$$

Equivariance requires that for all $\sigma \in G$:

$$W(\sigma \cdot v) + b = \sigma \cdot (Wv + b) = \sigma(W)(\sigma \cdot v) + \sigma(b), \quad (6.4)$$

Where $\sigma(W)$ denotes the entry-wise application of σ . For this relation to hold for all inputs v , we must have:

$$W = \sigma(W) \quad \forall \sigma \in G, \quad (6.5)$$

$$b = \sigma(b) \quad \forall \sigma \in G. \quad (6.6)$$

Equations (6.5) and (6.6) state that the weight matrix and bias vector must be invariant under the action of the Galois group. By the Fundamental Theorem of Galois theory, the fixed field of $\text{Gal}(K/F)$ is the base field F . Therefore, we obtain:

Theorem 6.1. A linear layer $L(v) = Wv + b$ over K is Galois-equivariant with respect to $G = \text{Gal}(K/F)$ if and only if:

$$W \in F^{m \times d} \text{ and } b \in F^m. \quad (6.7)$$

This result provides a structural constraint: by parameterizing the weights and biases using only the base field F , the neural network is guaranteed to respect the algebraic symmetries of the field extension K .

For the activation function $\sigma_{act}: K \rightarrow K$ we can employ polynomial functions with coefficients in F , such as $f(x) = \sum_{i=0}^p c_i x^i$ since Galois automorphisms preserve addition and multiplication, polynomial activations are automatically equivariant:

$$\sigma(\sigma_{act}(x)) = \sigma\left(\sum c_i x_i\right) = \sum c_i (\sigma(x))^i = (\sigma_{act}(x)). \quad (6.8)$$

GNNs offer a mathematically rigorous approach to learning invariant features in algebraic datasets, such as those found in algebraic coding theory and computational chemistry.

Galois-Theoretic Analysis of MHD Models (With Solvability Novelty)

Magnetohydrodynamics (MHD) couples fluid dynamics (described by the Navier-Stokes equations) and electromagnetism (described by Maxwell's equations) [13]. The governing partial differential equations are highly non-linear. When solving boundary-layer problems, researchers often apply polynomial approximations (e.g., Galerkin, Collocation, or Homotopy Analysis Methods) to reduce the boundary-value problem to a system of non-linear algebraic equations.

Novel Addition: Galois Solvability of Discretized MHD Polynomials

Consider the steady, laminar boundary-layer flow of an incompressible, electrically conducting fluid over a stretching sheet in the presence of a transverse magnetic field. The similarity reduction yields the following non-linear ordinary differential equation:

$$f''' + ff'' - (f')^2 - M^2 f' = 0, \quad (7.1)$$

where M is the magnetic parameter, subject to the boundary conditions:

$$f(0) = 0, f'(0) = 1, f'(\infty) = 0. \quad (7.2)$$

Suppose we approximate the similarity function $f(\eta)$ using a polynomial trial function of degree N :

$$f(\eta) = \sum_{i=0}^N a_i \eta^i \quad (7.3)$$

Applying a collocation method at discrete points η_j leads to a system of algebraic equations for the coefficients a_i . For instance, a low-order collocation for a simplified boundary-layer flow yields an algebraic equation for the skin-friction coefficient $C_f \propto f''(0) = a_2$:

$$f(a_2) = a_2^5 + c_4 a_2^4 + c_3 a_2^3 + M^2 a_2^2 + c_1 a_2 + c_0 = 0$$

We analyze the algebraic solvability of Equation (7.4) over the field of rational functions $F = \mathbb{Q}(M^2, c_0, c_1, c_3, c_4)$.

Theorem 7.1. For generic coefficients and magnetic parameter M , the Galois group of the MHD collocation polynomial $f(x)$ in Equation (7.4) is the symmetric group S_5 .

Proof Sketch. We compute the discriminant $D(f)$ and find that it is not a square in F , meaning $\text{Gal}(K/F) \not\subseteq A_5$. By reducing the polynomial modulo specific primes and checking the cycle types of the factorization, we find that the Galois group contains a 5-cycle and a transposition. Since S_5 is generated by any transposition and any 5-cycle, the Galois group must be S_5 .

Since S_5 is not a solvable group, we obtain the following physical consequence:

Corollary 7.2. The skin-friction coefficient a_2 for the discretized MHD boundary-layer flow in Equation (7.4) cannot be expressed analytically in terms of radicals of the input parameters.

This analysis establishes the fundamental limits of analytical methods. It proves that even for low-order polynomial approximations of MHD equations, closed-form algebraic solutions are mathematically impossible, confirming that numerical algorithms (such as Newton-Raphson) or non-algebraic trans-series are strictly required to resolve the boundary-layer properties [14].

Comparative Synthesis

To summarize the connection between classical Galois theory, its computational realizations, and modern applied settings, we present a comparative synthesis in Table 1.

Table 1: Synthesis of Galois theory applications across domains

Domain	Core Object	Galois Action	Symmetry Group	Key Benefit
Classical Theory	Field extensions (K/F)	Automorphisms $\sigma \in \text{Gal}(K/F)$	Solvable / Non-solvable	Proof of unsolvability
CAS Software	Polynomials $f(x) \in \mathbb{Q}[x]$	Root permutations	Permutation subgroups of S_n	Algorithmic group identification
Cryptography	Galois fields $\text{GF}(p^k)$	Frobenius map $x \mapsto x^p$	Cyclic group $\mathbb{Z}/k\mathbb{Z}$	Non-linear S-box design
Equivariant AI	Vector space K^d	Component-wise action	$\text{Gal}(K/F)$	Equivariant representations
MHD Modeling	Discretized systems	Permutation of system roots	Symmetric group $(k > 5)$	Analytical limits

The synthesis reveals that whether protecting data against quantum attacks, designing invariant neural network layers, or bounding the limits of boundary-layer solutions, the key is the mapping of algebraic structure to transformation groups.

Conclusion

This paper has explored the modern horizons of Galois theory, demonstrating its transition from a classical tool for

polynomial solvability to a fundamental framework for computation, cryptography, and artificial intelligence. By introducing cyclotomic Galois actions in Ring-LWE, we demonstrated how algebraic symmetries preserve noise distributions in post-quantum cryptography. Through Galois-Equivariant Neural Networks, we defined how weights and activations can be constrained to base fields to guarantee representation invariance. Finally, our analysis of discretized

MHD boundary-layer polynomials showed that Galois theory provides rigorous analytical bounds on the limits of closed-form physical solutions. Future work will investigate the implementation of GENNs on real-world algebraic datasets and extend Galois solvability analysis to higher-dimensional fluid models.

References

1. Lang S. Algebra. New York: Springer; 2002.
2. Cox D. Galois Theory. Hoboken: Wiley; 2004.
3. Neukirch J. Algebraic Number Theory. Berlin: Springer; 2008.
4. Bosma W, Cannon J, Playoust C. The Magma algebra system I: The user language. Journal of Symbolic Computation. 1997;24(3-4):235-265.
5. The GAP Group. GAP - Groups, Algorithms, and Programming, Version 4; 2024. <https://www.gap-system.org>
6. Stein WA, *et al.* SageMathSoftware; 2026. <https://www.sagemath.org>
7. Stauduhar RP. The determination of Galois groups. Mathematics of Computation. 1977;31(139):578-596.
8. Lidl R, Niederreiter H. Introduction to Finite Fields and Their Applications. Cambridge: Cambridge University Press; 1994.
9. Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. Journal of the ACM. 2013;60(6):43.
10. Avanzi R, *et al.* CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation. NIST PQC Standardization Process; 2020.
11. Cohen TS, Welling M. Group equivariant convolutional networks. International Conference on Machine Learning (ICML); 2016.
12. Bronstein MM, Bruna J, Cohen T, Velicković P. Geometric Deep Learning: Grids, Groups, Graphs, Geodesics, and Gauges. arXiv preprint arXiv:2104.13478; 2021.
13. Davidson PA. An Introduction to Magnetohydrodynamics. Cambridge: Cambridge University Press; 2001.
14. El-Shaarawi SM, Abu-Rumman MA. MHD flow and heat transfer over a stretching sheet. International Journal of Thermal Sciences. 2010;49(1):111-119.