INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT

eISSN 2394-6334 Impact factor: 8.854 Volume 13, issue 02 (2026)

GALOIS THEORY AND ITS APPLICATIONS IN MODERN MATHEMATICS

Jo'rayeva Sitora

ABSTRACT

This article examines Galois theory as one of the fundamental frameworks of modern algebra and analyzes its main theoretical principles and applications. The study focuses on the relationship between field extensions and group theory, emphasizing the role of Galois groups in determining the solvability of polynomial equations by radicals. Using a theoretical and analytical approach, the article demonstrates how Galois theory provides a structural explanation for classical algebraic problems and establishes deep connections between algebra, number theory, and geometry. Particular attention is given to the applications of Galois theory in finite field theory, which forms the mathematical foundation of coding theory and cryptography. The results of the study confirm that Galois theory is not only a cornerstone of pure mathematics but also a powerful tool with significant relevance in applied mathematics and modern technological systems.

Keywords:

Galois theory, field extensions, Galois groups, solvability by radicals, abstract algebra, finite fields, cryptography.

INTRODUCTION

Galois theory occupies a central position in modern abstract algebra, providing a deep and unifying connection between field theory and group theory. Originally developed in the early nineteenth century by Évariste Galois, the theory was introduced to address a classical problem in mathematics: determining when polynomial equations can be solved by radicals. Although Galois's life was short, his ideas laid the foundation for a profound theoretical framework that continues to influence many areas of mathematics and its applications [1].

At its core, Galois theory establishes a correspondence between algebraic field extensions and groups of automorphisms, known as Galois groups. This correspondence allows algebraic problems to be translated into group-theoretic ones, making it possible to analyze the structural properties of polynomial equations through symmetry considerations [2]. As a result, questions about solvability, factorization, and algebraic dependence can be addressed using the language and methods of group theory.

One of the most significant achievements of Galois theory is the characterization of solvable polynomial equations. The theory provides a precise criterion for determining whether a given polynomial equation can be solved using a finite sequence of algebraic operations and radical extractions. This result not only resolved a centuries-old mathematical problem but also marked a turning point in the development of modern algebra by shifting the focus from explicit computations to structural analysis [3].

Beyond its theoretical importance, Galois theory has found numerous applications in various branches of mathematics. In number theory, it plays a crucial role in the study of algebraic number fields, class field theory, and arithmetic geometry [4]. In algebraic geometry, Galois groups are used to analyze coverings of algebraic varieties and the symmetries of geometric objects. Furthermore, the theory provides essential tools for understanding finite fields, which are fundamental in coding theory and cryptography [5].

In applied mathematics and computer science, Galois theory contributes indirectly through its influence on finite field theory. Finite fields, whose structure is best understood using Galois theory, are widely applied in error-correcting codes, cryptographic algorithms, and digital communication systems [6]. Thus, a theory originally developed for abstract algebraic purposes has become an indispensable component of modern technological applications.

The continued relevance of Galois theory lies in its ability to connect abstract mathematical concepts with practical problems. Its applications demonstrate how deep theoretical ideas can lead to powerful tools across diverse scientific domains. Therefore, studying Galois theory and its applications remains an important task in both pure and applied mathematics.

The aim of this article is to analyze the fundamental principles of Galois theory and to examine its main applications in modern mathematics and related fields. The study seeks to highlight the theoretical significance of the theory as well as its practical relevance in contemporary scientific research.

MATERIALS AND METHODS

This study is based on a theoretical and analytical approach aimed at examining the fundamental principles of Galois theory and its applications in modern mathematics. The research materials consist of classical and contemporary mathematical literature on field theory, group theory, and algebraic equations, including textbooks, monographs, and peer-reviewed journal articles devoted to Galois theory and related algebraic structures [1–3]. These sources provide the theoretical foundation necessary for understanding the core concepts, definitions, and theorems of the theory.

The methodological framework of the study relies primarily on deductive and logical analysis. Key definitions and results of Galois theory, such as field extensions, automorphism groups, Galois groups, and solvability by radicals, are examined through formal mathematical reasoning. The study employs an axiomatic approach, starting from basic algebraic structures and progressively developing more complex theoretical constructs. This method allows for a systematic presentation of the theory and ensures conceptual coherence.

In addition, comparative analysis is used to highlight the role of Galois theory in relation to other areas of mathematics, including number theory, algebraic geometry, and finite field theory. By comparing different applications, the study identifies common structural principles that underline the wide applicability of Galois theory. Abstract examples and illustrative cases are analyzed to demonstrate how theoretical results are applied to concrete algebraic problems, such as determining the solvability of polynomial equations.

The research also applies a structural approach, focusing on the correspondence between algebraic field extensions and group-theoretic properties. This approach emphasizes the role of symmetry and automorphisms in understanding algebraic phenomena. Furthermore, methods of mathematical generalization and abstraction are used to synthesize results and to draw broader conclusions regarding the significance of Galois theory in both pure and applied mathematics.

Overall, the combination of analytical, deductive, and comparative methods provides a comprehensive framework for investigating Galois theory and its applications. This methodological approach ensures that the study not only presents theoretical results but also clarifies their relevance and impact across various mathematical domains.

RESULTS

The results of the study demonstrate that Galois theory provides a powerful and systematic framework for understanding the structural properties of polynomial equations and field extensions. The analysis confirms that the central contribution of Galois theory lies in establishing a precise correspondence between algebraic field extensions and groups of automorphisms, known as Galois groups. This correspondence allows algebraic problems to be reformulated in group-theoretic terms, significantly simplifying the analysis of polynomial solvability.

One of the key results concerns the criterion for solvability of polynomial equations by radicals. The study shows that a polynomial equation is solvable by radicals if and only if its associated Galois group is a solvable group. This result highlights the fundamental role of group structure in determining algebraic solvability and explains why general polynomial equations of degree five or higher cannot, in general, be solved by radicals. This finding represents a major shift from computational approaches to structural reasoning in algebra.

The analysis further demonstrates that Galois theory is not limited to theoretical considerations but has wide-ranging applications in modern mathematics. In number theory, the results confirm that Galois groups play a central role in describing the symmetries of algebraic number fields and in understanding field extensions generated by algebraic numbers. In algebraic geometry, Galois-theoretic methods are shown to be essential for studying coverings of algebraic varieties and morphisms between fields of functions.

In addition, the study reveals the importance of Galois theory in finite field theory. Finite fields are characterized as Galois extensions of prime fields, and their structure can be fully described using Galois groups. This result explains why finite fields are uniquely determined by their order and why they are particularly suitable for applications in coding theory and cryptography.

The main theoretical results and applications of Galois theory identified in this study are summarized in Table 1.

Table 1

Key Results and Applications of Galois Theory

Aspect of Galois theory	Main result	Mathematical or practical significance

Aspect of Galois theory	**Main result**	**Mathematical or practical significance**
Polynomial equations	Solvability depends on the solvability of the Galois group	Explains limits of solving equations by radicals
Field extensions	One-to-one correspondence with automorphism groups	Connects field theory and group theory
Number theory	Galois groups describe symmetries of number fields	Foundation of class field theory
Algebraic geometry	Use of Galois groups in field coverings	Analysis of geometric symmetries
Finite fields	Finite fields as Galois extensions of prime fields	Basis for coding theory and cryptography

The data presented in Table 1 indicate that Galois theory serves as a unifying theory across multiple areas of mathematics. The results confirm that its strength lies in revealing hidden symmetries and structural relationships rather than providing explicit computational formulas. This structural perspective not only deepens theoretical understanding but also enables practical applications in areas that rely on finite field arithmetic.

Overall, the results validate the significance of Galois theory as a cornerstone of modern algebra and demonstrate its enduring impact on both pure mathematical theory and applied disciplines.

DISCUSSION

The results of this study highlight the central role of Galois theory as a unifying framework in modern algebra and its significant influence on both theoretical and applied mathematics. The discussion confirms that the fundamental strength of Galois theory lies in its ability to translate algebraic problems into group-theoretic terms, thereby revealing the underlying symmetries of polynomial equations and field extensions. This structural perspective distinguishes Galois theory from earlier algebraic approaches that relied primarily on explicit calculations.

One of the most important implications of the findings is the criterion for solvability of polynomial equations by radicals. The identification of solvable Galois groups as the determining factor provides a clear explanation for the historical problem of solving higher-degree polynomial equations. This result demonstrates how abstract group properties directly govern algebraic behavior, reinforcing the idea that structural analysis is essential for understanding fundamental mathematical limitations.

The discussion also emphasizes the broad applicability of Galois theory across different mathematical domains. In number theory, the interpretation of field extensions through Galois groups offers deep insight into the arithmetic structure of algebraic numbers. This approach forms the theoretical basis of class field theory and has contributed to significant developments in modern arithmetic geometry. The results discussed in this study are consistent with existing literature that identifies Galois theory as a cornerstone of number-theoretic research.

Furthermore, the study highlights the relevance of Galois theory in algebraic geometry, where it is used to analyze morphisms between algebraic varieties and the symmetries of function fields. The application of Galois groups to geometric problems demonstrates the flexibility of the theory and its capacity to connect algebraic and geometric viewpoints. This interdisciplinary role strengthens the position of Galois theory as a central mathematical framework.

In the context of applied mathematics, the discussion confirms that the practical importance of Galois theory is most evident in finite field theory. Finite fields, understood as Galois extensions, are essential in coding theory, cryptography, and digital communication systems. The theoretical results discussed in this study explain why finite fields have a rigid and well-defined structure, which makes them particularly suitable for reliable and secure information processing.

Despite its abstract nature, Galois theory thus proves to be highly relevant to real-world applications. The discussion suggests that the continued study of Galois theory is crucial not only for advancing pure mathematics but also for supporting technological innovation. The ability of the theory to provide a conceptual foundation for practical tools highlights the enduring value of abstract mathematical research.

Overall, the discussion reinforces the view that Galois theory represents a paradigm shift in mathematical thinking. By focusing on symmetry and structure rather than explicit solutions, the theory has reshaped the development of algebra and influenced a wide range of mathematical disciplines. These findings underscore the importance of Galois theory as both a theoretical achievement and a practical resource in contemporary science.

REFERENCES

1. Évariste Galois. *Mémoire sur les conditions de résolubilité des équations par radicaux.* Paris, 1832.
2. Abstract Algebra. Dummit D.S., Foote R.M. *Abstract Algebra.* 3rd ed. Hoboken: John Wiley & Sons; 2004.
3. A First Course in Galois Theory.Rotman J.J. *A First Course in Galois Theory.* 2nd ed. New York: Springer; 2010.
4. Galois Theory. Stewart I. *Galois Theory.* 4th ed. Boca Raton: CRC Press; 2015.
5. Algebra. Lang S. *Algebra.* Revised 3rd ed. New York: Springer; 2002.
6. Field and Galois Theory. Morandi P.J. *Field and Galois Theory.* New York: Springer; 1996.
7. Number Fields. Marcus D.A. *Number Fields.* New York: Springer; 1977.
8. Introduction to Finite Fields and Their Applications. Lidl R., Niederreiter H. *Introduction to Finite Fields and Their Applications.* Cambridge: Cambridge University Press; 1994.