International Journal of Advanced Research in Engineering and Applied Sciences
ISSN: 2278-6252
Impact Factor:8.055

GALOIS THEORY : A STUDY

Dr. Santosh Kumar Singh Bhadauria
Associate Professor
Department of Mathematics
Pt. J.L.N. College Banda

ABSTRACT

Galois Theory, named after the French mathematician Évariste Galois, represents one of the most profound achievements in 19th-century mathematics. It establishes a deep connection between field theory and group theory, providing a framework for understanding the solvability of polynomial equations. This paper explores the historical development of Galois Theory, introduces fundamental algebraic structures such as fields and groups, elucidates the concepts of field extensions and Galois groups, and examines the theory's principal theorems. Additionally, it demonstrates the applications of Galois Theory in solving polynomial equations, addressing classical geometric problems, advancing number theory, and influencing cryptography. By combining historical narrative, theoretical exposition, and practical examples, this paper emphasizes the lasting significance of Galois Theory in modern mathematics.

Keywords: Galois Theory, modern mathematics, polynomial equations.

INTRODUCTION

The study of polynomial equations has a long and illustrious history, beginning in ancient civilizations where mathematicians sought methods to solve quadratic and higher-degree equations.

While the solutions to quadratic, cubic, and quartic equations were discovered and generalized over centuries, the general quintic equation—polynomials of degree five—posed a major unsolved problem. Mathematicians initially attempted to find solutions in terms of radicals, but repeated failures suggested inherent limitations.

The breakthrough came with the work of Évariste Galois (1811–1832), who introduced a novel approach: analyzing the symmetries among the roots of a polynomial using group theory.

By linking algebraic structures with group-theoretic concepts, Galois provided a criterion to determine whether a polynomial is solvable by radicals. This theory not only answered longstanding questions about polynomial equations but also laid the foundations of modern abstract algebra. Galois Theory has since become a central area in algebra, influencing diverse mathematical fields, including number theory, geometry, and cryptography. Its importance lies in providing a unified language for discussing field extensions, polynomial solvability, and group symmetries.

Historical Background

Early Developments in Algebra: The roots of algebra trace back to Babylonian mathematics, where quadratic equations were solved geometrically. Over time, algebraic techniques evolved in medieval Islamic mathematics and European Renaissance, leading to systematic methods for solving cubic and quartic equations. Mathematicians like Scipione del Ferro, Niccolò Tartaglia, and Gerolamo Cardano contributed significantly to the development of these formulas.

Niels Henrik Abel and the Quintic Equation: Despite successes with lower-degree polynomials, the quintic equation remained elusive. In the early 19th century, Niels Henrik Abel rigorously proved that there is no general solution in radicals for polynomial equations of degree five or higher. Abel's result highlighted a fundamental limit in classical algebraic methods, motivating a deeper investigation into the structure of polynomials.

Évariste Galois: Évariste Galois introduced a revolutionary approach: instead of attempting to solve equations directly, he studied the symmetries of their roots. He associated each polynomial with a group of automorphisms, now known as the Galois group, and demonstrated that the structure of this group determines the solvability of the polynomial by radicals. Tragically, Galois died at the age of 20 in a duel, but his manuscripts laid the foundation for modern algebra.
Later Developments: The publication of Galois' work in the mid-19th century transformed algebra. Mathematicians such as Camille Jordan and Leopold Kronecker expanded Galois' ideas, formalizing the correspondence between fields and groups. Today, Galois Theory underpins modern algebraic structures and provides insights into number theory, geometry, and cryptography.

Preliminaries

Fields: A field F is a set equipped with two operations: addition (+) and multiplication (×), satisfying closure, associativity, commutativity, distributivity, identity elements, and inverses. Examples include rational numbers Q, real numbers R, complex numbers C, and finite fields F_p with prime p.
Field Extensions: A field extension E/F occurs when E is a field containing F as a subfield. The degree of the extension, denoted [E : F], is the dimension of E as a vector space over F. Field extensions allow the study of algebraic elements (roots of polynomials) over a given base field.
Polynomials and Splitting Fields: A polynomial f(x) ∈ F[x] is an expression of the form a_nx^n + ... + a_0. A polynomial is irreducible over F if it cannot be factored into polynomials of lower degree with coefficients in F. The splitting field of f(x) over F is the smallest field containing all roots of f(x).
Groups: A group G is a set with a binary operation satisfying closure, associativity, identity, and inverses. Groups capture symmetry, a concept central to Galois Theory.

Fundamental Concepts of Galois Theory

Galois Groups: The Galois group of a field extension E/F, denoted Gal(E/F), is the set of all automorphisms of E that fix F. These automorphisms represent symmetries of the roots of polynomials.

Normal and Separable Extensions: A normal extension is one where every irreducible polynomial over F with a root in E splits completely in E. A separable extension is one where the minimal polynomial of every element of E over F has distinct roots. A Galois extension is both normal and separable.
Fundamental Theorem of Galois Theory: There is a bijective correspondence between subgroups of Gal(E/F) and intermediate fields F ⊆ K ⊆ E. Larger subgroups correspond to

smaller intermediate fields, and normal subgroups correspond to normal extensions. This correspondence allows algebraic problems to be studied using group theory.

Key Theorems

Abel-Ruffini Theorem: The general quintic equation cannot be solved by radicals.
Solvability by Radicals: A polynomial is solvable by radicals if and only if its Galois group is a solvable group.
Galois Correspondence: The correspondence between subfields and subgroups of the Galois group provides a framework to classify field extensions and understand their structure.

Applications of Galois Theory

Solvability of Polynomials: Determines which polynomials can be solved using radicals.

Classical Geometric Problems: Ancient problems such as trisecting an angle or doubling the cube are impossible using only compass and straightedge. Galois Theory explains these impossibilities via field extensions.
Number Theory: Helps study algebraic numbers, cyclotomic fields, and Diophantine equations. Instrumental in advanced results like Fermat's Last Theorem and class field theory.

Cryptography: Finite fields and Galois extensions underpin modern cryptography, including public-key algorithms and error-correcting codes.

Examples

Quadratic Polynomial: f(x) = x^2 - 2 over Q. Splitting field: Q(√2). Galois group: Z/2Z.

Cubic Polynomial: f(x) = x^3 - 2 over Q. Splitting field: $Q(\sqrt[3]{2}, \omega)$, ω a primitive cube root of unity. Galois group: S_3.
Cyclotomic Polynomials: The n-th cyclotomic polynomial Φ_n(x) has roots that are primitive n-th roots of unity. Its Galois group is isomorphic to (Z/nZ)*.

CONCLUSION

Galois Theory is a cornerstone of modern algebra, linking fields, groups, and polynomial equations. Its historical development demonstrates the evolution of mathematical thought from solving equations to understanding symmetry and structure. The theory's applications—from polynomial solvability to cryptography—highlight its enduring significance. By studying Galois Theory, mathematicians gain a powerful framework for understanding the fundamental properties of algebraic structures, solving classical problems, and advancing modern mathematical research.

REFERENCES

1. Dummit, D. S., & Foote, R. M. (2004). Abstract Algebra (3rd ed.). Wiley.
2. Artin, M. (2011). Algebra. Pearson.
3. Stewart, I. (2004). Galois Theory. Chapman & Hall/CRC.
4. Jacobson, N. (2009). Basic Algebra I. Dover Publications.
5. Galois, É. (1832). Mémoire sur les conditions de résolubilité des équations par radicaux.