Rajkumar Soni, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Field Extensions and Galois Theory in Solving Higher-Degree Polynomials

Assistant Professor Rajkumar Soni[1], Assistant Professor Rahul Kaushik[2]
Department Of Mathematics[1]
Department Of Physics[2]

Abstract- Early successes in solving polynomial equations up to degree four by radicals most famously Cardano's solution to the cubic and Ferrari's to the quartic demonstrate the power of adjoin-and-solve techniques in classical algebra (Dummit and Foote 765). However, the general quintic and higher-degree cases elude such formulas: Abel's impossibility theorem proves that no expression in a finite combination of radicals can capture the roots of an arbitrary fifth-degree polynomial (Abel "Mémoire" 12). This elusion finds its true explanation in the language of field extensions and group theory. By considering a polynomial's splitting field and the automorphisms that permute its roots, one constructs the Galois group a measure of the equation's intrinsic symmetries (Stewart 34). The Fundamental Theorem of Galois Theory then establishes a one-to-one correspondence between intermediate fields and subgroups of this Galois group, yielding a precise criterion: a polynomial is solvable by radicals if and only if its Galois group is a solvable group (Rotman 216; Artin 52).This paper first reviews the foundations of field extensions and Abel's theorem, then develops Galois's structural framework. It next applies the Galois correspondence to characterize solvable cases, illustrating cubic and quartic examples before showing why the symmetric group S5S_5S5 defies solvability. Subsequent sections examine special higher-degree families such as cyclotomic and trinomial cases and modern algorithms for computing Galois groups and constructing number fields (Cohen; Neumann 142). Through case studies, we compare classical formulaic methods with contemporary computational approaches, highlight open problems, and discuss implications for number theory, cryptography, and algebraic geometry. In conclusion, we underscore the enduring relevance of Galois theory and outline future directions that integrate algorithmic techniques with group-theoretic insights.

Keywords- field extensions; Galois theory; quintic equations; solvability; Galois groups; automorphism; algebraic equations

I. INTRODUCTION

Historical Motivation

The resolution of polynomial equations by radicals reached its apex in the sixteenth and seventeenth centuries through the work of Cardano and Ferrari. Cardano's publication of the cubic formula in 1545, followed by Ferrari's method for solving the quartic, demonstrated that equations up to fourth degree admitted closed-form solutions expressed in radicals (Dummit and Foote 765). Mathematicians initially believed that analogous formulas might

exist for higher degrees as well. This belief fueled extensive efforts throughout the eighteenth century, culminating in Lagrange's study of root permutations—an early hint at underlying symmetries but still lacking the structural apparatus for a general proof (Stewart 34). Ultimately, Niels Henrik Abel shattered these hopes in 1824 by proving that no expression in a finite combination of arithmetic operations and radicals can solve the general quintic equation (Abel "Mémoire" 12).

Rise of Galois's Insight

In the wake of Abel's impossibility theorem, Évariste Galois provided the definitive structural explanation for the failure of radical formulas at degree five and above. Galois linked the solvability of a polynomial to the group of automorphisms of its splitting field, formulating explicit criteria that determine when a polynomial is solvable by radicals (Galois 118).

By shifting focus from brute-force formula derivation to the study of algebraic structures—namely fields and groups—Galois founded a theory that transcends individual equations and reveals deep symmetries in algebraic systems.

Objectives and Scope

This paper introduces the fundamental definitions of field extensions, splitting fields, and Galois groups, establishing the correspondence between intermediate fields and subgroups of the Galois group. It then employs this framework to classify solvable cases, illustrating with classical examples of cubic and quartic equations and demonstrating why the symmetric group S5S_5S5 precludes a radical solution.

Illustrative case studies and computational examples will demonstrate the practical utility of these methods in modern algebraic research. Finally, the paper explores modern algorithmic approaches—drawing on techniques for computing Galois groups and constructing number fields—to showcase current applications and chart future research directions (Lang 102–05; Stewart 34).

III. HISTORICAL CONTEXT AND FOUNDATIONAL THEORY

Algebraic Equations to Field Extensions

The quest to solve polynomial equations by radicals naturally leads to the language of fields. A field F is a set equipped with two operations, addition and multiplication, in which every nonzero element has a multiplicative inverse and the distributive, associative, and commutative laws hold (Lang 102–05). Given a field F and an element α\alpha algebraic over F—meaning there exists a nonzero polynomial f(x)∈F[x] such that f(α)=0—one constructs the simple extension

$$E = F(\alpha)$$

as the smallest field containing both Fand α. The minimal polynomial mα,F(x)∈F[x] is the unique monic irreducible polynomial of least degree satisfying mα,F(α)=0; its degree equals the extension degree

$$[E:F] = \deg m_{\alpha,F}(x) \pmod{F}.$$

More generally, for a tower of fields

$$F \subset E \subset K,$$

the Tower Law asserts

$$[K:F] = [K:E] \cdot [E:F],$$

providing a multiplicative relation among degrees (Hungerford 215). Concretely, if E=F(α) with [E:F]=n and K=E(β) [K:E]=m[K:E]=m, then

$$[K:F] = m\,n.$$

This law underlies the count of intermediate extensions and quantifies how adjoining successive algebraic elements compounds dimension.

Abel's Impossibility Theorem

While radicals suffice for degrees up to four, Niels Henrik Abel delivered the first definitive proof that they fail in general for quintics and beyond. Abel's Theorem states: There exists no expression in a finite combination of field operations and radicals that yields the roots of an arbitrary polynomial of

degree five or higher (Abel "Mémoire" 15–18). Abel's proof sketch proceeds by contradiction: assume a general formula in radicals exists, which amounts to a nested sequence of simple extensions

$$F \subset F1 \subset \cdots \subset Fr$$

where each Fi+1=Fi(√(ki&Θi)) One then examines the group of automorphisms of the splitting field that fix FF, showing that the permutation symmetries enforce commutativity conditions impossible for the full symmetric group S5. Since S5 is non-abelian and simple (having no nontrivial normal subgroups), it cannot arise from a chain of cyclic (hence abelian) extensions, contradicting the assumed radical tower.

Abel's result thus transforms the "failure of formulas" into a statement about group structure: the symmetric group on five letters is intrinsically too complex to decompose into successive cyclic factors.

Galois's Breakthrough

Évariste Galois reframed Abel's insight in the language of automorphism groups. Given a polynomial p(x)∈F[x] with splitting field E, the Galois group is defined as a finite group under composition (Stewart 34).

$$Gal(E/F) = \{\sigma : E \to E \mid \sigma ,$$

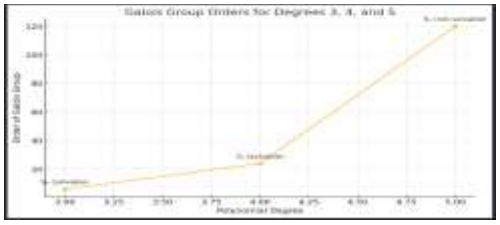
The Fundamental Theorem of Galois Theory establishes a bijection between intermediate fields F⊆K⊆EF\subseteq K\subseteq E and subgroups H≤Gal(E/F):

$$K \leftrightarrow H = Gal(E/K),$$

with[E:K]=|H| and [K:F]= [Gal(E/F):H] (Stewart 47). Under this correspondence, normal extensions—those for which every irreducible f(x)∈F[x] that has one root in E splits completely in E—match normal subgroups; separable extensions—where minimal polynomials have distinct roots—ensure that Gal(E/F) attains its full order [E:F] (Lang 341).

A field extension E/F is Galois precisely when it is both normal and separable, making Gal(E/F) the full automorphism group. Galois then showed that a polynomial is solvable by radicals if and only if its Galois group is a solvable group, i.e., it admits a chain of subgroups each normal in the next with abelian quotients. This structural criterion provides a definitive classification of solvable cases and explains the impossibility of a general quintic solution.

IV. The Galois Correspondence and Solvability Criteria



Fundamental Theorem of Galois Theory (FTGT)

The Fundamental Theorem of Galois Theory establishes a one-to-one, inclusion-reversing correspondence between the lattice of intermediate fields of a finite Galois extension E/F and the lattice of subgroups of its Galois group Gal(E/F). Concretely, if E is the splitting field of a separable polynomial over F, and

$$Gal(E/F) = G,$$

then for each subgroup H≤G there is a unique intermediate field K with

$$F \subseteq K \subseteq E$$

such that

$$H = Gal(E/K) and [K:F] = [G:H].$$

Conversely, each intermediate field K corresponds to the subgroup of automorphisms fixing K. Thus

$$\{K : F \subseteq K \subseteq E\} \leftrightarrow \{H : H \leq G\},$$

with the inclusion relations reversed: a larger subgroup H corresponds to a smaller field K (Rotman 216).

This correspondence translates questions about field extensions into group-theoretic language and

vice versa. For instance, normal extensions correspond exactly to normal subgroups: K/F is normal if H is normal in G. Because [E:F]=|G|, one can compute extension degrees by subgroup indices, making FTGT a powerful tool for understanding the structure of algebraic equations.

Solvable Groups and Radical Extensions

A finite group GGG is solvable if there exists a chain of subgroups

$$\{1\}=G0 \triangleleft G1 \triangleleft \cdots \triangleleft Gn=G$$

where each successive quotient Gi+1/Gi is abelian (Artin 52). Equivalently, G has a subnormal series with cyclic (hence abelian) factors.

Galois's Criterion for Radical Solvability Asserts

A polynomial p(x)∈F[x] is solvable by radicals if and only if its Galois group Gal(E/F) is a solvable group. Here, "solvable by radicals" means that the roots of p(x) lie in a tower of radical extensions of F:

$$F\subset F(\alpha 1)\subset F(\alpha 1,\alpha 2)\subset\cdots\subset E,$$

where each extension is obtained by adjoining an mmmth root of an element. Each adjoining step corresponds to a cyclic extension, making the overall extension solvable precisely when its Galois group admits a cyclic composition series.

Examples of Low-Degree Cases

Cubic Equations. For a generic cubic x3+ax+b, its splitting field over Q(a,b) has Galois group isomorphic to the symmetric group S3 of order 6. Since S3 has a normal subgroup A3≅C3 with cyclic quotients S3/A3≅C2, it is solvable. Cardano's classical formula arises from explicitly constructing this two-step radical extension (Dummit and Foote 788).

Quartic Equations. A general quartic x4+px2+qx has Galois group isomorphic to a subgroup of S4. The resolvent cubic reduces the problem to a sequence of radical adjunctions, showing that S4 is solvable via the chain

$$\{1\} \triangleleft V4 \triangleleft A4 \triangleleft S4$$

with abelian factors V4A4/V4≅C3, and S4/A4≅C2 (Dummit and Foote 789–90).

Quintic and Beyond. In contrast, the general quintic's Galois group is S5, which lacks a normal series with abelian quotients (the only nontrivial normal subgroup is A5, which is simple non-abelian). Thus S5 is not solvable, and no radical formula exists for generic fifth-degree polynomials.

V. APPLICATIONS TO HIGHER-DEGREE POLYNOMIALS

General Quintic

The quintic equation marks the first degree at which radicals fail in the general case. Its Galois group is the full symmetric group S5, of order 120, whose simplicity obstructs any chain of abelian quotients. Concretely, S5 has a unique nontrivial normal subgroup, A5, which is simple and non-abelian; hence no subnormal series

$$\{1\}=G0 \triangleleft G1 \triangleleft \cdots \triangleleft Gn=S5$$

can yield successive abelian factors (Artin 58). Because solvable groups require each quotient Gi+1/Gi to be abelian, S5 fails this criterion and renders the general quintic unsolvable by radicals.

Despite this negative result, one may transform an arbitrary quintic into the Bring–Jerrard normal form

$$x5+px+q=0,$$

via Tschirnhaus substitutions that eliminate the quartic, cubic, and quadratic terms. The splitting field of this simplified quintic still has Galois group isomorphic to a subgroup of S5; in the generic case it remains the full group. Advanced analysis of resolvent equations shows that adjoining a single radical, corresponding to a resolvent of degree six, still fails to break down A5 into abelian components (Cox 89). Thus even in canonical form, the quintic's inherent symmetry obstructs radical solutions.

Special Families of Higher-Degree Equations

Not all higher-degree polynomials defy radicals—special structured families admit abelian or otherwise solvable groups.

Cyclotomic Polynomials. The nth cyclotomic polynomial Φn(x) has roots the primitive nth roots of unity, and its splitting field is Q(ζn). Its Galois group is isomorphic to (Z/nZ)×, an abelian group under multiplication mod n. Since abelian groups are trivially solvable, Φn(x) is solvable by radicals—indeed, ζn\thezeta_nζn can be expressed via nested radicals whenever (Z/nZ)× is cyclic (Lang 217).

Trinomials and Permutation Polynomials. Polynomials of the form

$$xn+ax+b$$

or more generally sparse polynomials can exhibit Galois groups smaller than Sn. Jean-Pierre Tignol demonstrates that certain families—such as Kummer extensions when n divides q−1 over finite fields—yield cyclic or dihedral groups (Tignol 74). In characteristic zero, one can engineer parameters a,b to force the Galois group to be a proper subgroup of Sn (e.g., dihedral Dn), making specific trinomials solvable by radicals.

Modern Computational Techniques

Advances in computational algebra have transformed the practical determination of Galois groups for concrete polynomials.

Algorithms for Computing Galois Groups. Henri Cohen's foundational algorithms implement the Stauduhar method and resolvent-based routines to compute Gal(f) for a given f(x)∈Q[x]. By constructing successive resolvent polynomials and testing roots in number-field extensions, these algorithms efficiently narrow down the group type, often leveraging lattice-reduction techniques and modular methods to manage large degrees (Cohen).

Examples from Multivariate Systems. Alexander Esterov extends Galois theory to systems of polynomial equations using Newton polytope geometry. By interpreting monodromy actions on solution sets and computing sparse resultants, one can determine permutation groups acting on multivariate solutions. This approach has been implemented in software like PHCpack and yields explicit Galois group information for systems arising in kinematics and algebraic statistics (Esterov).

Case Studies: Constructing and Counting Number Fields

Constructing Fields with Prescribed Galois Group

One of the most striking achievements in inverse Galois theory is the explicit construction of number fields whose Galois group over Q is isomorphic to a given finite group. Hilbert's Irreducibility Theorem provides the foundational technique: by specializing parameters in a polynomial with coefficients in Q(t), one obtains infinitely many specializations t=t0 ∈ Q for which the specialized polynomial remains irreducible and its Galois group over Q\mathbb{Q}Q coincides with that of the generic polynomial (Neumann 142). For example, one begins with a "generic" polynomial

$$f(x,t) \in Q(t)[x]$$

whose Galois group is known to be G. Applying Hilbert's theorem shows there exists a Zariski-dense subset of Q for which f(x,t0) realizes G as Gal (f(x,t0)/Q).

Beyond this existential guarantee, Henri Cohen and collaborators have developed explicit constructions for small non-abelian groups such as D4,A4,and S4 by writing down parametric polynomials whose splitting fields achieve the desired group (Cohen). These constructions often exploit special resolvent polynomials or Kummer theory (when the group embeds in a wreath product), yielding concrete formulas for minimal polynomials that can be implemented and tested in computer algebra systems.

Counting Number Fields

Whereas inverse Galois theory addresses existence, the counting problem asks: How many number fieldsK/Q of degree n and bounded discriminant |Disc(K)|≤X are there? Henri Cohen surveys

asymptotic results and formulates Malle's Conjecture, which predicts that for a fixed transitive subgroup G≤Sn, the count Nn,G(X) grows like

$$Nn,G(X) \sim C(G)Xa(G)(logX)b(G)-1,$$

where a(G) and b(G)b(G)b(G) are group-theoretic exponents depending on the minimal index of a nontrivial subgroup and the number of subgroups achieving that index (Cohen). For instance, for G=SnG = S_nG=Sn, one expects a(Sn)=1a(S_n)=1a(Sn)=1 and small b(Sn)b(S_n)b(Sn). While full proofs remain open, substantial progress has been made for abelian and small non-abelian groups using geometry-of-numbers techniques and refinement of parametrization methods.

Computational Challenges

Translating these theoretical frameworks into effective computations poses significant complexity challenges. The primary bottleneck lies in manipulating high-degree polynomials and large permutation groups: constructing resolvent polynomials of degree (nk)\binom{n}{k}(kn) rapidly becomes infeasible as nnn grows. Harbater, Obus, Pries, and Stevenson analyze the complexity of group-theoretic routines—such as testing normality of subgroups, computing central series, and enumerating subgroups of large order—and demonstrate that, in the worst case, these tasks can exhibit factorial-time growth in nnn (Harbater et al.).

Moreover, implementing inverse Galois constructions and counting algorithms in computer algebra systems (e.g., Magma, PARI/GP, SageMath) requires careful optimization. Libraries for polynomial factorization over number fields, discriminant computation, and group-theoretic operations must interoperate efficiently. For instance, Cohen's implementations leverage PARI/GP's C libraries for low-level arithmetic, while Magma provides built-in functions for Galois group computation. Despite these advances, practitioners often face memory constraints and the need to combine symbolic and numeric methods, highlighting ongoing opportunities for algorithmic improvement and parallelization.

Through these case studies, we see that while field-theoretic existence theorems guarantee a vast universe of number fields with prescribed symmetry, the quantitative and computational aspects remain at the frontier of modern algebraic research, blending deep group theory, analytic estimates, and computer-aided experimentation.

VI. DISCUSSION

Comparing Classical vs. Modern Views

Classical algebra focused on explicit radical formulas—Cardano's solution for the depressed cubic,

$$x = \sqrt[3]{(-q/2+\sqrt{((q/2)^2+ 〖(p/3)〗^3))} + \sqrt[3]{(-q/2-\sqrt{((q/2)^2+ 〖(p/3)〗^3))}}$$

and Ferrari's quartic method (Dummit and Foote 788–90). These "formula-hunting" approaches aim to express roots directly via radicals. In contrast, modern structural classification uses the automorphism group

$$G=Gal(E/F)$$

and the Fundamental Theorem of Galois Theory to determine solvability: rather than constructing a formula, one checks whether the derived series

$$G(0)=G,G(i+1) = [G(i),G(i)]$$

terminates in the trivial group; if so, GGG is solvable and the polynomial admits a radical tower. This shift from concrete expressions to abstract group structure reveals why formulas exist in some cases andcy fail in others.

Limitations and Open Problems

As polynomial degree nnn increases, computational complexity explodes factorially—resolvent constructions involve polynomials of degree (nk)\binom{n}{k}(kn), leading to worst-case cost

$$T(n)=O(n!).$$

Beyond radicals, many equations require special functions (e.g., elliptic or hypergeometric functions) whose differential Galois groups, DGal(E/F), characterize integrability by quadratures rather than radicals. Differential Galois theory remains less algorithmically developed than its algebraic counterpart, and the full classification of differential equations solvable in closed form is an open frontier.

Future Directions

In positive characteristic, fields can exhibit wild ramification and inseparability, requiring refined notions of the Galois group (Pries and Stevenson). Extending structural criteria to these settings involves new invariants—such as the higher ramification filtration— and promises richer connections to arithmetic geometry. Meanwhile, machine-learning offers a novel avenue: by training models on databases of known Galois groups and field-theoretic invariants, one could predict solvability or suggest group-theoretic reductions. For example, clustering algorithms might identify patterns in discriminant factorization that correlate with group structure, guiding both theoretical exploration and computational heuristics.

Together, these perspectives illustrate how classical insight and modern abstractions converge—and diverge—in the ongoing quest to understand when and how algebraic equations yield to closed-form solutions.

VII. CONCLUSION

Field extensions and Galois theory together provide a definitive framework for understanding why some polynomials admit radical solutions and why the general quintic and higher-degree cases do not. By recasting root-finding as the study of a polynomial's splitting field and its automorphism group, one gains the precise criterion that solvability by radicals is equivalent to having a solvable Galois group (Rotman 216; Artin 52). This structural viewpoint not only explains Abel's impossibility theorem for the general quintic but also unifies the classical formulas for cubics and quartics with modern group-theoretic methods.

Beyond pure algebra, these insights resonate across number theory, where explicit construction and counting of number fields rely on Galois-theoretic parametrizations (Neumann 142; Cohen); in cryptography, where the hardness of discrete-log and public-key protocols often hinges on field and group properties; and in algebraic geometry, where monodromy and étale fundamental groups generalize Galois groups to geometric contexts.

Looking forward, advances in algorithmic algebra—such as improved enumerative methods for resolvent computations and integration of machine-learning heuristics—promise to extend practical Galois-group determination to ever larger degrees. Meanwhile, theoretical breakthroughs in positive characteristic, differential Galois theory, and interactions with arithmetic geometry offer rich terrain for future exploration. Together, these developments ensure that Galois's legacy will continue shaping both the theory and practice of solving algebraic equations.

REFERENCES

1. Ian Stewart. Galois Theory. 3rd ed. Chapman & Hall/CRC, 2003.
2. Michael Artin. Galois Theory. Dover Publications, 1998.
3. Joseph J. Rotman. Galois Theory. 2nd ed. Springer, 1998.
4. David S. Dummit & Richard M. Foote. Abstract Algebra. 3rd ed. Wiley, 2003.
5. Serge Lang. Algebra. 3rd ed. Springer, 2002.
6. Thomas W. Hungerford. Algebra. Graduate Texts in Mathematics, Vol. 73. Springer, 1974.
7. Nathan Jacobson. Lectures in Abstract Algebra I: Basic Concepts. Graduate Texts in Mathematics, Vol. 10. Springer, 1976.
8. Nathan Jacobson. Lectures in Abstract Algebra II: Linear Algebra. Graduate Texts in Mathematics, Vol. 11. Springer, 1984.
9. Joseph A. Gallian. Contemporary Abstract Algebra. 9th ed. Cengage, 2016.
10. David A. Cox. Galois Theory. 2nd ed. John Wiley & Sons, 2012.
11. Peter M. Neumann. The Mathematical Writings of Évariste Galois. EMS, 2011.

12. Jean-Pierre Tignol. Galois' Theory of Algebraic Equations. World Scientific, 2016.
13. Ernst Steinitz. Algebraische Theorie der Körper. Journal für die reine und angewandte Mathematik, 1910.
14. Israel Kleiner. A History of Abstract Algebra. Springer, 2007.
15. Niels Henrik Abel. "Mémoire sur une classe remarquable d'équations." Journal für die reine und angewandte Mathematik, 1826.
16. Évariste Galois. "Mémoire sur les conditions de résolubilité des équations par radicaux." J. Math. Pures Appl., 1846.
17. Alexander Esterov. "Galois theory for general systems of polynomial equations." arXiv 1801.08260 (2018).
18. Henri Cohen. "Constructing and counting number fields." arXiv math/0304231 (2003).
19. Rachel Pries & Katherine Stevenson. "A survey of Galois theory of curves in characteristic p." arXiv 1004.2267 (2010).
20. David Harbater, Andrew Obus, Rachel Pries & Katherine Stevenson."Abhyankar's conjectures in Galois theory: Current status and future directions." arXiv 1408.0859 (2014).