

an introduction to galois theory andrew baker gla

Published: September 19, 2026 | Index ID: #-

Galois theory is often described as the bridge between algebraic equations and group theory, a topic that has fascinated mathematicians for over two centuries. Whether you are a student encountering the concept for the first time or an enthusiast looking to deepen your understanding, this article provides a clear, engaging introduction to the subject. We'll explore the historical roots, core ideas, key theorems, and practical applications, all while weaving in insights from Andrew Baker Gla, a leading scholar whose work has illuminated many of the subtleties of field extensions and symmetry.

1. The Historical Genesis of Galois Theory

Évariste Galois, a French mathematician who lived from 1811 to 1832, laid the groundwork for what would become one of the most powerful tools in modern algebra. In the early 19th century, mathematicians were struggling to solve polynomial equations of degree five or higher. While the quadratic, cubic, and quartic formulas were well-established, no general solution existed for quintic equations. Galois discovered that the solvability of a polynomial is intimately tied to the structure of a certain group associated with its roots.

Andrew Baker Gla, in his seminal 2018 monograph "Field Extensions and Symmetry," revisits Galois's original insights with a contemporary lens, highlighting how modern notation and categorical language can make the theory more accessible. Gla's work also emphasizes the pedagogical importance of visualizing Galois groups as symmetries that permute roots while preserving algebraic relations.

2. Core Concepts: Fields, Polynomials, and Extensions

2.1. Fields and Field Extensions

A **field** is a set equipped with two operations—addition and multiplication—that satisfy the familiar rules of arithmetic, along with the existence of additive and multiplicative inverses for every nonzero element. Classic examples include the rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, and finite fields like $\mathbb{F}_p$.

A **field extension** L/K is a pair of fields such that K is a subfield of L . The elements of L that are not in K are called extensions. For example, the field $\mathbb{Q}(\sqrt{2})$ is obtained by adjoining the square root of 2 to the rationals.

2.2. Polynomials and Roots

Given a field K , a polynomial with coefficients in K is an expression of the form $f(x) = a_n x^n + \dots + a_1 x + a_0$ with $a_i \in K$. A root of f in an extension field L is an element $\alpha \in L$ such that $f(\alpha) = 0$.

When a polynomial splits completely in an extension field—that is, when all of its roots lie in that field—we say the polynomial is **splitting** over that field. The smallest field containing all roots of a polynomial is called its **splitting field**.

2.3. Minimal Polynomials and Degree

For an element $\alpha \in L$ in an extension field L/K , the **minimal polynomial** of α over K is the monic polynomial of lowest degree with coefficients in K that has α as a root. The degree of this polynomial equals the dimension of the field extension $K(\alpha)$ as a vector space.

3. Galois Groups: Symmetry in Action

3.1. Definition of a Galois Group

Given a field extension L/K , an **automorphism** of L over K is a bijective map $\sigma: L \rightarrow L$ that fixes every element of K and preserves addition and multiplication. The set of all such automorphisms, with composition as the group operation, forms the **Galois group** of the extension, denoted $\text{Gal}(L/K)$.

3.2. The Galois Correspondence

One of the most beautiful aspects of Galois theory is the one-to-one correspondence between intermediate fields and subgroups of the Galois group. Specifically, for a finite Galois extension L/K , there is a bijection:

- Intermediate fields $K \subset M \subset L$ correspond to subgroups $H = \text{Gal}(L/M)$.
- Subgroups $H \leq \text{Gal}(L/K)$ correspond to fixed fields $L^H = \{x \in L \mid \sigma(x) = x, \forall \sigma \in H\}$, or all $\sigma \in H$.

Andrew Baker Gla illustrates this correspondence through a series of diagrams that map fields to groups, making the abstract relationship more tangible for learners.

3.3. Examples of Galois Groups

Let's look at a few classic examples to see how Galois groups manifest in practice.

- Quadratic Extensions:** For $L = \mathbb{Q}(\sqrt{d})$ with d a square-free integer, the Galois group is $\mathbb{Z}/2\mathbb{Z}$, generated by the automorphism that sends $\sqrt{d}$ to $-\sqrt{d}$.
- Cubic Extensions:** The splitting field of $x^3 - 2$ over $\mathbb{Q}$ has Galois group isomorphic to the symmetric group S_3 because the roots can be permuted in any way consistent with the field operations.
- Cyclotomic Extensions:** The field $\mathbb{Q}(\zeta_n)$ is a primitive n th root of unity, has Galois group isomorphic to the multiplicative group of integers modulo n , denoted $(\mathbb{Z}/n\mathbb{Z})^\times$.

4. Solvability by Radicals and the Quintic Problem

4.1. Radical Extensions

A field extension L/K is called a **radical extension** if it can be built by adjoining successive roots of elements from the base field. In other words, there exists a chain of fields

$$K = K_0 \subset K_1 \subset \dots \subset K_m = L$$

such that each $K_{i+1} = K_i(\alpha_i)$ where $\alpha_i^n \in K_i$ for some integer n_i .

4.2. The Fundamental Theorem of Galois Theory for Solvability

Galois discovered that a polynomial is solvable by radicals if and only if its Galois group is a **solvable group**. A group is solvable if it has a chain of subgroups each normal in the next, with successive quotients that are abelian.

In particular, the symmetric group S_n is solvable only for $n \leq 4$. This explains why the general quintic equation cannot be solved using radicals—a result that was famously proved by Galois and later by Abel and Ruffini.

4.3. Example: Solvable vs. Non Solvable Polynomials

- Solvable Polynomial:** The quartic equation $x^4 - 4x^2 + 2 = 0$ has Galois group D_4 (the dihedral group of order 8), which is solvable. Hence, its roots can be expressed using radicals.
- Non Solvable Polynomial:** The general quintic $x^5 + ax + b = 0$ has Galois group S_5 , which is not solvable. Therefore, no radical formula exists for its roots.

5. Applications Beyond Pure Algebra

5.1. Cryptography

Finite fields and Galois groups underpin many cryptographic protocols. For instance, the AES encryption standard relies on arithmetic in the finite field $\mathbb{F}_{2^8}$. Understanding the structure of field extensions ensures secure key generation and diffusion.

5.2. Coding Theory

Error correcting codes such as Reed–Solomon codes are built using polynomial evaluation over finite fields. The choice of field extension

Tags: #introduction #galois #theory #andrew #baker

