Galois Theory and its Applications in Modern Algebra

Atharv Chagi

Introduction

Deducing the solvability of polynomial equations has led to major breakthroughs across history in physics, biology, engineering, economics, and other fields. A lot of real world phenomena is modeled by polynomials, and understanding information about solvability and a polynomial's roots yield crucial insight in specific domains. Up until the early 19th century, mathematicians were still puzzled about whether higher degree polynomials could be solved with radicals. Évariste Galois was a French mathematician whose contributions helped revolutionize algebra. Not only did Galois solve the mystery, but he also formalized what is known today as Galois Theory.

At its core, Galois Theory exploits symmetries. Galois created a path merging algebra and group theory, explaining the solvability of polynomial equations. The fundamental idea obtained from Galois theory states that the stucture of roots of a polynomial equation is directly related to a particular symmetric group.

This paper aims to give a high level overview of Galois Theory assuming basic group/field theory; starting with the life of Évariste Galois and transitioning to Galois Theory and applications.

The 20 years of Évariste Galois

Galois was born in Bourg-la-Reine, a small town near Paris, France on October 25, 1811. Galois demonstrated signs of intelligence at a young age, but was very rebellious. Galois would clash with his instructors and had a hard time with formal education. Despite his intelligence, his unconventional ways of solving problems hindered him multiple times from getting admission to Ecole Polytechnique, a prestigious school in Paris.

He was also engaged in activism later in his life. His father was a Republican mayor, which likely influenced his activism. In the early 1830's, Galois supported revolutionary causes and took part in political activism in France. He was imprisoned several times, but he was still able to make significant contributions to mathematics.

Most of Galois' work focused on polynomial equations. In particular, Galois was interested in whether a polynomial could be solved with radicals. In the modern day, his work is observed in Galois Theory when studying the symmetries of polynomial roots. Galois developed foundation for what we know today as modern algebra and solved the mystery of solvabilty of higher order polynomials.

Many sources suggest Galois died due to a love-affair. He fell in love with a physician's daughter when in jail, but she was in love with someone else. Shortly after he was released from prison, Galois

challenged him to a duel and died at 20 years old as a result of the wounds from the duel. The day before he died, Galois sent a letter to a friend detailing his insights and expressing frustration about his work not being recognized. Galois' work was not recognized until years after his death; Joseph Liouville, a prominent mathematician at the time saw promise in Galois' work and published his work in 1846. Although Galois didn't get recognition in his 20 years, he will be remembered as one of the greatest mathematical minds of all time and his ideas will remain as the foundations of modern algebra.

Galois Theory at a High Level

Galois' work addressed the solvability of a polynomial with radicals. We say a polynomial is solvable with radicals if every root can be written in terms of elementary operations and nth roots $(+, -, \times, \div, \sqrt[n]{})$. Other mathematicians like Lagrange and Abel showed that solving higher order polynomials with radicals was constrained. Galois was able to find utility in group theory to exploit symmtries of the roots of polynomials.

Field Extensions

The concept of field extensions was created by Galois to help understand solvability. A **field extension** K/F is a larger field K that contains a smaller field F, and allows the inclusion of additional elements, such as the roots of a polynomial.

$F(\alpha)$ is a larger field F that contains an element α not in the field. This can also be thought of as adding the root α of a polynomial to F. For example, if we have $\mathbb{Q}$, we can extend it to a larger field that includes $\sqrt{2}$ by writing $\mathbb{Q}(\sqrt{2})$. Now, elements such as $\frac{1}{2} + \frac{\sqrt{2}}{3}$ exist in $\mathbb{Q}(\sqrt{2})$.

Galois Groups

Galois also went on to use groups to describe symmetries of the roots of a polynomial. The **Galois group** of a polynomial is a group of automorphisms on the splitting field K of the polynomial, over the field F, denoted $Gal(K/F)$. As an example, lets take $p(x) = x^2 - 2$. We know the roots are $\alpha_{1,2} = \pm\sqrt{2}$. Here, the splitting field $K = \mathbb{Q}(\sqrt{2})$, and the base field is $F = \mathbb{Q}$. The Galois Group consists of all field automorphisms that fix $\mathbb{Q}$. In this case, there are two automorphisms: the identity σ_0 that sends every element to itself, and σ_1 the map that flips $\sqrt{2}$ and $-\sqrt{2}$. We see here that the Galois Group $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ is isomorphic to the symmetric group of order 2. This is the core of Galois Theory – leveraging the connection between group and field theory to discover insights.

Fundamental Theorem of Galois Theory

Arguably the most major result from Galois Theory is the criteria of a polynomial being solvable with radicals. We say a polynomial is solvable with radicals if and only if its associated Galois Group is a solvable group. To know what it means for a group to be solvable, we need to understand what the derived series is. The **derived series** is a series of groups $\{G_i\}_{i\in\mathbb{N}}$ where G_j is smaller than G_{j-1}. The derived series is constructed by taking successive commutator subgroups of the original group. We say a Galois Group is **solvable** if its derived series terminates in the trivial subgroup. For example:

$$G \geq G_1 \geq G_2 \geq ... \geq \{e\}$$

In this case, G is the original group and G_i are successive subgroups. It is like peeling an onion's layers; if we reach the proper center of the onion (trivial subgroup), then the group is solvable. Using this idea of reaching the trivial subgroup at the end of a derived series, Galois was able to show that the quadratic, cubic, and quartic equations were solvable and the quintic equation was not.

The previous idea is the **Fundamental Theorem of Galois Theory**: there is an isomorphism between the intermediate fields of an extension K/F and the subgroups of its Galois Group $Gal(K/F)$. If the Galois group is solvable, then the polynomial can be solved by radicals. This is especially meaningful, as it connects the symmetries of polynomial roots and utility of the Galois group to determining the solvability of the polynomial.

$$\text{Gal}(K/F) \leftrightarrow \{\text{subgroups of Gal}(K/F)\}$$

Applications of Galois Theory

In the previous section, it was stated one of the main utilities for Galois Theory at the time of it's discoveries was deducing solvability of higher order polynomials. Not only did Galois help answer a centuries old question, he connected algebra to group theory and formed the foundations of modern algebra. Outside of determining whether an arbitrary polynomial is solvable or not, there are many real-world applications of Galois Theory.

Cryptography

A lot of cryptographic systems rely on the structure of finite fields. In the Advanced Encryption Standard, they use the Rijndael algorithm operating over a finite field $\mathbb{F}_{2^8}$ which leverages properties of field extensions from Galois Theory. It helps keep data secure and creates an encryption such that third parties cannot decrypt information without a key.

Error Correcting Codes

In data storage and communication systems, error correcting codes are a method used to detect and correct errors in data transmission or storage. Galois theory is used once more in the form of field extensions to ensure data integrity. Using field extensions, codes can encode and decode information quickly, making communication more robust despite noise.

Quantum Mechanics

In quantum mechanics, states of subatomic particles are often defined by wavefunctions. In these quantum systems, quantities such as angular momentum and spin exhibit really nice symmetries. Galois theory can be used to pry information from these symmetries; physicists can understand how symmetries transform between energy states and describe the behavior of operators under these transformations. The group of all unitary operators on an inifinte dimenstional Hilbert space can be used to describe symmetries that can be linked to structures in algebra analagous to those highlighted by Galois Theory.

Conclusion

Galois' work has had a profound impact on modern mathematics, changing the way we understand polynomials. Galois Theory gives a framework for connecting symmetries between group theory and algebra. Although he lived a short life, Evariste Galois' impact on mathematics can still be seen in many applications today. The legacy of Galois will not be forgotten, as one of the greatest mathematicians in history, Galois' ideas are a reminder of the interconnectedness and beauty of mathematics.

References

- Choe, X., & Rastogi, G. (n.d.). Number Fields and Galois Theory. Retrieved from MIT PRIMES Circle.
- MacTutor History of Mathematics Archive. (n.d.). Évariste Galois. University of St Andrews. https://mathshistory.st-andrews.ac.uk/Biographies/Galois/
- Mathemaniac. (2022, July 3). Why you can't solve quintic equations (Galois theory approach) #SoME2 [Video]. YouTube. https://www.youtube.com/watch?v=zCU9tZ2VkWc
- Math Visualized. (2020, November 9). Galois Theory Explained Simply [Video]. YouTube. https://www.youtube.com/watch?v=Ct2fyigNgPY
- Milne, J. S. (2022). Fields and Galois Theory (v5.10). Retrieved from https://www.jmilne.org/math/.
- Nasseef, M. T. (2017). Field Extension by Galois Theory. General Letters in Mathematics, 3(3), 132-153. http://www.refaad.com