Galois theory

Samuel Henshaw

December 1, 2020

1 Introduction

Galois theory, roughly speaking, is the study of polynomials. A bit more specifically, it is the study of automorphism groups of fields and polynonomial rings over fields. It is a fruitful theory, having provided proofs of the impossibility of trisecting the angle and the unsolvability of the general quintic equation. It also introduced many important ideas and techniques later used in serious mathematics. This paper will provide a brief summary of its history and a heuristic introduction to its methods and fundamental ideas.

2 History

It begins, of course, with Evariste Galois. Born in France in 1811, he took an interest in mathematics as a teenager. He started to read the cutting-edge works of Legendre and Lagrange while still in school. He was, however, denied admission to the most advanced mathematical universities of his day, so in obscurity he began to work on polynomial equations. The chief problem of his day was to discover a solution for the general quintic polynomial. He applied himself to this and to the development of the theory of fields. His work laid the foundations of permutation-based group theory and field theory, and he proved the Fundamental Theorem of Galois Theory, an important connection between groups and fields. He made significant progress on the quintic problem. Despite all of this, he was disliked by his peers, who considered him obnoxious and arrogant or disregarded him altogether. He never achieved worldly success as a mathematician. His life of failure culminated in expulsion from college and imprisonment. Upon his release from jail, he participated in a duel. The reason for this is debated; some say he was involved in a love affair with a prostitute while others say that he was to be made a political martyr. What is not debated is the fact that he lost the duel and died. He was not even twenty two years of age at his death. He was buried in a common grave, and his work was ignored for a while after his death. It was rediscovered by Joseph Liouville, who published it to great acclaim.

3 Polynomial rings, field extensions, and automorphism groups

Let R be a commutative unital ring. $R[x]$ is taken to be the ring of polynomials in the variable x with coefficients in R. Addition is vector addition and multiplication is polynomial multiplication. In Galois theory, one is only concerned with polynomial rings over fields.

F will denote a field. Polynomials over $F[x]$ can be reducible or irreducible. Predictable, reducible polynomials may be factored into at least two non-invertible (i. e. nonconstant) components while irreducible ones may not. An example of reducibility is $x^2 - 4x + 3 = (x - 1)(x - 3)$ over $R[x]$. Over the same field, the polynomial $x^2 + 1$ is irreducible, for a real facorization of it implies a real root of it. The only roots are purely imaginary, so the polynomial is irreducible.

Irreducible polynomials are the generating set of the polynomial ring, but the are useful beyond that. We can use them to make the underlying fields bigger. If $p(x)$ is irreducible over $F[x]$, we may define α as a root of $p(x)$ and adjoin it to F to create $F(\alpha)$. This is a vector space over F of dimension equal to the degree of $p(x)$; its basis elements are 1, α, α^2... α^n where $n = \dim F - 1$. Once α is taken to the $n + 1^{th}$ power, we use $p(x)$ to remove it, for it is a root of the polynomial $p(x)$ of degree $n+1$. We define addition on $F(\alpha)$ as vector addition and multiplication as distributive polynomial multiplication; these operations make it into a field. Here are some examples. The polynomial $x^2 - 2$ is irreducible over $\mathbb{Q}[x]$. $\sqrt{2}$ is defined as one of its roots, and affixing it to $\mathbb{Q}$ begets $\mathbb{Q}(\sqrt{2})$: the set of elements of the form $a + b\sqrt{2}$. Similarly, since $x^2 + 1$ is irreducible over $\mathbb{R}[x]$, we define i as one of its roots and adjoin it to $\mathbb{R}$ to create $\mathbb{R}(i) = \mathbb{C}$: the set of elements of the form $a + bi$. For any field extension done in such a manner, it does not matter which root of the polynomial is taken; the resulting fields are isomorphic. We arbitrarily impose the order on i and $\sqrt{2}$ to make them the positive roots; their negative counterparts would suffice as well.

A field automorphism is a nontrivial map $\phi : F \longrightarrow F$ commuting with addition and multiplication. Since all nontrivial field homomorphisms are injective, any such ϕ is an isomorphism. Since automorphisms are invertible and they have the same domain and codomain, they can be composed to form a group called $\mathrm{Aut}(F)$.

When one field E contains another F, we call E an extension of F and write it as E/F. This is most often used when adjoining elements to fields, like $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. When we write $\mathrm{Aut}(E/F)$, we are referring to the subgroup of $\mathrm{Aut}(E)$ acting as the identity on F. One can consider the smallest subfield of any field: the set of positive and negative finite sums of 1 and quotients by those sums. Since automorphisms distribute over sums and quotients, this field is fixed by all automorphisms (they act as the identity on it.) This is called the prime subfield. For finite fields, the prime subfield is isomorphic to $\mathbb{F}_p$ for some prime p. For infinite fields, the prime subfield is isomorphic either to $\mathbb{F}_p$ or to $\mathbb{Q}$. Since it is always fixed, we have that $\mathrm{Aut}(E)$=$\mathrm{Aut}(E/F)$ when F is the prime subfield of E.

4 Good extensions

Like many other objects, there are "good" field extensions, just as normal subgroups are the "good" subgroups and ideals are the "good" subrings. They are called Galois extensions, and there are many equivalent definitions of them. The most useful definition is as follows: E/F is a Galois extension if and only if E is the splitting field of an irreducible polynomial over F.

The splitting field of $p(x)$ over F is the smallest extension over which $p(x)$ factors into linear components, or, equivalently, is F with all of the roots of $p(x)$ adjoined. The automorphism group of a splitting field (a Galois extension) is called its Galois group. Here is a non-example. Let ζ be the unique real cube root of 2. Then $\mathbb{Q}(\zeta)$ is a subfield of $\mathbb{R}$, so it cannot contain the complex cube roots of 2. Thus the irreducible polynomial $x^3 - 2$ over $\mathbb{Q}$ cannot factor all the way into linear components over $\mathbb{Q}(\zeta)$. $\mathbb{Q}(\zeta)$ is not the splitting field for $x^3 - 2$. $\mathbb{Q}(\sqrt{2})$, however, is the splitting field for $x^2 - 2$. Since it contains the positive root of 2 and all rational multiples of it, it contains the negative root as well. Since it contains all the roots of that polynomial, it contains its splitting field. In the other direction, the splitting field of that polynomial contains $\sqrt{2}$ and $\mathbb{Q}$, so it contains $\mathbb{Q}(\sqrt{2})$. Thus it is the splitting field for $x^2 - 2$.

The algebraic closure of a field F is the smallest field over which all polynomials factor into linear components and is written as $\overline{F}$. F is algebraically closed if $F = \overline{F}$. The complex numbers, for example, are algebraically closed by the Fundamental Theorem of Algebra, while the reals are not.

5 The Fundamental Theorem

Let K/F be a Galois extension with Galois group $G = \mathrm{Aut}(K/F)$. There is a bijection between the set of subfields between K and F and the subgroups of G. It maps the subfield E to $\mathrm{Aut}(K/E)$ and the subgroup H to the fixed field of H. This bijection reverses inclusion. Further, we have that K/E is always Galois and E/F is Galois if and only if its corresponding subgroup H is normal. We also have that $[K : E] = |H|$ and $[E : F] = [G : H]$. Lastly, the intersection of two subfields corresponds to the subgroup generated by their respective groups and the compositum of two fields corresponds to the intersection of the groups.

6 Results of Galois theory

The most famous result of Galois theory is the Abel-Ruffini Theorem: the quintic polynomial has no general solution. Galois proved it independently using his work on permutation groups; he showed that a polynomial has a solution in radicals if and only if its Galois group is solvable. Quintic polynomials correspond to A_5, which is not solvable. Since the quintic is not solvable, higher order polynomials are not solvable either. Another neat result is the development of the domain of differential Galois theory. There, one deals with fields of functions that have a derivative operation, like the rational function fields. Extensions are made by taking exponentials and logarithms of functions. The jewel of this theory is the proof of the lack of a conventional form of the antiderivative of e^{-x^2}. Using the elementary tools of Galois theory, one can prove the impossibility of trisecting the angle, doubling the cube, and squaring the circle with the standard Euclidean operations. Also, Gauss famously proved the constructability of the regular 17-gon with the techniques of Galois theory and field extensions.

7 Other topics

Transcendental numbers like π and e can be treated by Galois theory. They are transcendental extensions of the rational numbers: field elements not defined algebraically, elements that are not a zero of any polynomial in any algebraic extension of the rationals. This is the basis of the theory of transcendental numbers. A current hot problem is to determine whether they are algebraically independent. Elements are algebraically independent when there no a polynomial of which they are both roots. The polynomial in this case would have to be over an algebraic extension of the rationals. Galois theory also has many advanced applications in cryptography and category theory. Its applications are more often not direct results of its theorems, but spiritual imitators of its various attitudes. There is another fruitful object of study in the Galois connection, which is a generalization of the type of bijection seen in the Fundamental Theorem of Galois theory.

8 Sources

https://mathshistory.st-andrews.ac.uk/Biographies/Galois

Professor Vinroot's Galois theory course and its textbook Abstract Algebra by Dummit and Foote