Galois theory

In mathematics, **Galois theory** provides a connection between field theory and group theory. Using Galois theory, certain problems in field theory can be reduced to group theory, which is in some sense simpler and better understood.

The subject is named after Évariste Galois, who introduced it for studying the roots of a polynomial and characterizing the polynomial equations that are **solvable by radicals** in terms of properties of the permutation group of their roots—an equation is solvable by radicals if its roots may be expressed by a formula involving only integers, nth roots and the four basic arithmetic operations.

The theory has been popularized (among mathematicians) and developed by Richard Dedekind, Leopold Kronecker and Emil Artin, and others, who, in particular, interpreted the permutation group of the roots as the automorphism group of a field extension.

Galois theory has been generalised to Galois connections and Grothendieck's Galois theory.

Contents

Application to classical problems

The birth and development of Galois theory was caused by the following question, whose answer is known as the Abel–Ruffini theorem:

> Why is there no formula for the roots of a fifth (or higher) degree polynomial equation in terms of the coefficients of the polynomial, using only the usual algebraic operations (addition, subtraction, multiplication, division) and application of radicals (square roots, cube roots, etc)?

Galois' theory not only provides a beautiful answer to this question, but also explains in detail why it is possible to solve equations of degree four or lower in the above manner, and why their solutions take the form that they do. Further, it gives a conceptually clear, and often practical, means of telling when some particular equation of higher degree can be solved in that manner.

Galois' theory also gives a clear insight into questions concerning problems in compass and straightedge construction. It gives an elegant characterization of the ratios of lengths that can be constructed with this method. Using this, it becomes relatively easy to answer such classical problems of geometry as

1. Which regular polygons are constructible polygons?[1]
2. Why is it not possible to trisect every angle using a compass and straightedge?[2]

History

Pre-history

Galois' theory originated in the study of symmetric functions – the coefficients of a monic polynomial are (up to sign) the elementary symmetric polynomials in the roots. For instance, $(x-a)(x-b)=x^2-(a+b)x+ab$, where $x+b$ and ab are the elementary symmetric polynomials of degree 1, and 2 in two variables.

This was first formalized by the 16th-century French mathematician François Viète, in Viète's formulas, for the case of positive real roots. In the opinion of the 18th-century British mathematician Charles Hutton,[3] the expression of coefficients of a polynomial in terms of its roots (not only positive roots) was first understood by the 17th-century French mathematician Albert Girard; Hutton writes:

> ...[Girard was] the first person who understood the general doctrine of the formation of the coefficients of the powers from the sum of the roots and their products. He was the first who discovered the rules for summing the powers of the roots of any equation.

In this vein, the discriminant is a symmetric function in the roots that reflects properties of the roots – it is zero if and only if the polynomial has a multiple root, and for quadratic and cubic polynomials it is positive if and only if all roots are real and distinct, and negative if and only if there is a pair of distinct complex conjugate roots. See Discriminant Nature of the roots for details.

The cubic was first partly solved by the 15–16th-century Italian mathematician Scipione del Ferro, who did not however publish his results; this method, though, only solved one type of cubic equation. This solution was then rediscovered independently in 1535 by Niccolò Fontana Tartaglia, who shared it with Gerolamo Cardano, asking him to not publish it. Cardano then extended this to numerous other cases, using similar arguments; see more details at Cardano's method. After the discovery of Ferro's work, he felt that Tartaglia's method was no longer secret, and thus he published his solution in his 1545 *Ars Magna*.[4] His student Lodovico Ferrari solved the quartic polynomial; his solution was also included in *Ars Magna*. In this book, however, Cardano does not provide a "general formula" for the solution of a cubic equation, as he had neither complex numbers at his disposal, nor the algebraic notation to be able to describe a general cubic equation. With the benefit of modern notation and complex numbers, the formulae in this book do work in the general case, but Cardano did not know this. It was Rafael Bombelli who managed to understand how to work with complex numbers in order to solve all forms of cubic equation.

A further step was taken in the 1770 paper *Réflexions sur la résolution algébrique des équations* by the French-Italian mathematician Joseph Louis Lagrange, in his method of Lagrange resolvents, where he analyzed Cardano and Ferrari's solution of cubics and quartics by considering them in terms of *permutations* of the roots, which yielded an auxiliary polynomial of *lower* degree, providing a unified understanding of the solutions and laying the groundwork for group theory and Galois theory. Crucially, however, he did not consider composition of permutations. Lagrange's method did not extend to quintic equations or higher, because the resolvent had higher degree.

The quintic was showed unsolvable in general using methods by Paolo Ruffini in 1799, whose key insight was to use *permutation groups*, not just a single permutation. His solution contained a gap, which Cauchy considered minor, though this was not patched until the work of Norwegian mathematician Niels Henrik Abel, who published a proof in 1824, thus establishing the Abel–Ruffini theorem.

While Ruffini and Abel established that the *general* quintic could not be solved, some *particular* quintics can be solved, such as $(x-1)^5=0$, and the precise criterion by which a given quintic or higher polynomial could be determined to be solvable or not was given by Évariste Galois, who showed that whether a polynomial was solvable or not was equivalent to whether or not the permutation group of its roots – its modern terms, its Galois group – had a certain property – in modern terms, whether or not it was a solvable group. This group was always solvable for polynomials of degree four or less, but not always so for polynomials of degree five and greater, which explains why there is no general solution in higher degree.

Galois' writings

In 1830 Galois (at the age of 18) submitted to the Paris Academy of Sciences a memoir on his theory of solvability by radicals; Galois' paper was ultimately rejected in 1831 as being too sketchy and for giving a condition in terms of the roots of the equation instead of its coefficients. Galois then published in a duel in 1832, and his paper, "*Mémoire sur les conditions de résolubilité des équations par radicaux*", remained unpublished until 1846 when it was published by Joseph Liouville accompanied by some of his own explanations.[4] Prior to this publication, Liouville announced Galois' result to the Academy in a speech he gave on 4 July 1843.[5] According to Allan Clark, Galois's characterization "dramatically supersedes the work of Abel and Ruffini."[6]

Aftermath

Galois' theory was notoriously difficult for his contemporaries to understand, especially to the level where they could expand on it. For example, in his 1846 commentary, Liouville completely missed the group-theoretic core of Galois' method.[7] Joseph Alfred Serret who attended some of Liouville's talks, included Galois' theory in his 1866 (third edition) of his textbook *Cours d'algebre supérieure*. Serret's pupil, Camille Jordan, had an even better understanding reflected in his 1870 book *Traité des substitutions et des équations algebriques*. Outside France, Galois' theory remained more obscure for a longer period. In Britain, Cayley failed to grasp its depth and popular British algebra textbooks did not even mention Galois' theory until after the turn of the century. In Germany, Kronecker's writings focused more on Abel's result. Dedekind wrote little about Galois' theory, but lectured on it at Göttingen in 1858, showing a very good understanding.[8] Eugen Netto's books of the 1880s, based on Jordan's *Traité*, made Galois theory accessible to a wider German and American audience as did Heinrich Martin Weber's 1895 algebra textbook.[9]

Permutation group approach to Galois theory

Given a polynomial, it may be that some of the roots are connected by various algebraic equations. For example, it may be that for two of the roots, say A and B, that $A^2+5B^3=7$. The central idea of Galois' theory is to consider permutations (or rearrangements) of the roots such that any algebraic equation satisfied by the roots is still satisfied after the roots have been permuted. Originally, the theory has been developed for algebraic equations whose coefficients are rational numbers. It extends naturally to equations with coefficients in any field, but this will not be considered in the simple examples below.

These permutations together form a permutation group, also called the Galois group of the polynomial, which is explicitly described in the following examples.

First example: a quadratic equation

Consider the quadratic equation

$$x^2-4x+1=0.$$

By using the quadratic formula, we find that the two roots are

$$\begin{aligned}A&=2+\sqrt{3},\\B&=2-\sqrt{3}.\end{aligned}$$

Examples of algebraic equations satisfied by A and B include

$$A+B=4,$$

and

$$AB=1.$$

Obviously, in either of these equations, if we exchange A and B, we obtain another true statement. For example, the equation $A+B=4$ becomes simply $B+A=4$. Furthermore, it is true, but less obvious, that this holds for *every* possible algebraic relation between A and B such that all coefficients are rational (in any such relation, swapping A and B yields another relation). This results from the theory of symmetric polynomials, which, in this simple case, may be replaced by formula manipulations involving binomial theorem. (One might object that A and B are related by the algebraic equation $A-B-2\sqrt{3}=0$, which does not remain true when A and B are exchanged. However, this relation is not considered here, because it has the coefficient $-2\sqrt{3}$ which is not rational.)

We conclude that the Galois group of the polynomial x^2-4x+1 consists of two permutations: the identity permutation which leaves A and B untouched, and the transposition permutation which exchanges A and B. It is a cyclic group of order two, and therefore isomorphic to $\mathbf{Z}/2\mathbf{Z}$.

A similar discussion applies to any quadratic polynomial ax^2+bx+c, where a, b and c are rational numbers.

- If the polynomial has rational roots, for example $x^2-4x+4=(x-2)^2$, or $x^2-3x+2=(x-2)(x-1)$, then the Galois group is trivial; that is, it contains only the identity permutation.
- If it has two irrational roots, for example x^2-2, then the Galois group contains two permutations, just as in the above example.

Second example

Consider the polynomial

$$x^4-10x^2+1,$$

which can also be written as

$$\left(x^2-5\right)^2-24.$$

We wish to describe the Galois group of this polynomial, again over the field of rational numbers. The polynomial has four roots:

$$\begin{aligned}A&=\sqrt{2}+\sqrt{3},\\B&=\sqrt{2}-\sqrt{3},\\C&=-\sqrt{2}+\sqrt{3},\\D&=-\sqrt{2}-\sqrt{3}.\end{aligned}$$

There are 24 possible ways to permute these four roots, but not all of these permutations are members of the Galois group. The members of the Galois group must preserve any algebraic equation with rational coefficients involving A, B, C and D.

Among these equations, we have:

$$\begin{aligned}AB&=-1\\AC&=1\\A+D&=0\end{aligned}$$

It follows that, if φ is a permutation that belongs to the Galois group, we must have:

$$\begin{aligned}\varphi(B)&=\frac{-1}{\varphi(A)},\\\varphi(C)&=\frac{1}{\varphi(A)},\\\varphi(D)&=-\varphi(A).\end{aligned}$$

This implies that the permutation is well defined by the image of A, and that the Galois group has 4 elements, which are:

$$\begin{aligned}&(A,B,C,D)\to(A,B,C,D)\\&(A,B,C,D)\to(B,A,D,C)\\&(A,B,C,D)\to(C,D,A,B)\\&(A,B,C,D)\to(D,C,B,A)\end{aligned}$$

This implies that the Galois group is isomorphic to the Klein four-group.

Modern approach by field theory

In the modern approach, one starts with a field extension L/K (read "L over K"), and examines the group of field automorphisms of L/K (these are bijective ring homomorphisms $\alpha:L\to L$ such that $\alpha(x)=x$ for all $x\in K$). See the article on Galois groups for further explanation and examples.

The connection between the two approaches is as follows. The coefficients of the polynomial in question should be chosen from the base field K. The top field L should be the field obtained by adjoining the roots of the polynomial in question to the base field. Any permutation of the roots which respects algebraic equations as described above gives rise to an automorphism of L/K, and vice versa.

In the first example above, we were studying the extension $\mathbf{Q}(\sqrt{3})/\mathbf{Q}$, where $\mathbf{Q}$ is the field of rational numbers, and $\mathbf{Q}(\sqrt{3})$ is the field obtained from $\mathbf{Q}$ by adjoining $\sqrt{3}$. In the second example, we were studying the extension $\mathbf{Q}(A,B,C,D)/\mathbf{Q}$.

There are several advantages to the modern approach over the permutation group approach.

- It permits a far simpler statement of the fundamental theorem of Galois theory.
- The use of base fields other than $\mathbf{Q}$ is crucial in many of mathematics. For example, in algebraic number theory, one often does Galois theory using number fields, finite fields or local fields as the base field.
- It allows one to more easily study infinite extensions. Again this is important in algebraic number theory, where for example one often discusses the absolute Galois group of $\mathbf{Q}$, defined to be the Galois group of $A/\mathbf{Q}$ where A is an algebraic closure of $\mathbf{Q}$.
- It allows for consideration of inseparable extensions. This issue does not arise in the classical framework, since it was always implicitly assumed that arithmetic took place in characteristic zero, but nonzero characteristic arises frequently in number theory and in algebraic geometry.
- It removes the rather artificial reliance on chasing roots of polynomials. That is, different polynomials may yield the same extension fields, and the modern approach recognizes the connection between these polynomials.

Solvable groups and solution by radicals

The notion of a solvable group in group theory allows one to determine whether a polynomial is solvable in radicals, depending on whether its Galois group has the property of solvability. In essence, each field extension L/K corresponds to a factor group in a composition series of the Galois group. If a factor group in the composition series is *cyclic of order n*, and if in the corresponding field extension L/K the field K already contains a primitive nth root of unity, then it is a radical extension and the elements of L can then be expressed using the nth root of some element of K.

If all the factor groups in its composition series are cyclic, the Galois group is called *solvable*, and all of the elements of the corresponding field can be found by repeatedly taking roots, products, and sums of elements from the base field K.

One of the great triumphs of Galois Theory was the proof that for every $n>4$, there exist polynomials of degree n which are not solvable by radicals (this was proven independently, using a similar method, by Niels Henrik Abel a few years before, and is the Abel–Ruffini theorem), and a systematic way for testing whether a specific polynomial is solvable by radicals. The Abel–Ruffini theorem result from the fact that for $n>4$ the symmetric group S_n contains a simple, noncyclic, normal subgroup, namely the alternating group A_n.

A non-solvable quintic example

Van der Waerden[10] cites the polynomial $f(x)=x^5-x-1$. By the rational root theorem this has no rational zeros. Neither does it have linear factors modulo 2 or 3.

The Galois group of $f(x)$ modulo 2 is cyclic of order 6, because $f(x)$ modulo 2 factors into polynomials of orders 2 and 3, $(x^2+x+1)(x^3+x^2+1)$.

$f(x)$ modulo 3 has no linear or quadratic factor, and hence is irreducible. Thus its modulo 3 Galois group contains an element of order 5.

It is known[11] that a Galois group modulo a prime is isomorphic to a subgroup of the Galois group over the rationals. A permutation group on 5 objects with elements of orders 6 and 5 must be the symmetric group S_5, which is therefore the Galois group of $f(x)$. This is one of the simplest examples of a non-solvable quintic polynomial. According to Serge Lang, Emil Artin found this example.[12]

For the polynomial $f(x)=x^5-x-1$, the lone real root $x_1=1.1673\ldots$ is algebraic, but not expressible in terms of radicals. The other four roots are complex numbers.

Inverse Galois problem

The *inverse Galois problem* is to find a field extension with a given Galois group

As long as one does not also specify the ground field, the problem is not very difficult, and all finite groups do occur as Galois groups. For showing this, one may proceed as follows. Choose a field K at will, and a finite group G. Cayley's theorem says that G is (up to isomorphism) a subgroup of the symmetric group S on the elements of G. Choose indeterminates $\{x_g\}$, one for each element g of G, and adjoin them to K to get the field $F=K(\{x_g\})$. Contained within F is the field L of symmetric rational functions in the $\{x_g\}$. The Galois group of F/L is S, by a basic result of Emil Artin. G acts on F by restriction of action of S. If the fixed field of this action is M, then, by the fundamental theorem of Galois theory, the Galois group of F/M is G.

On the other hand, it is an open problem whether *every* finite group is the Galois group of a field extension of the field $\mathbf{Q}$ of the rational numbers. Igor Shafarevich proved that every solvable finite group is the Galois group of some extension of $\mathbf{Q}$. Various people have solved the inverse Galois problem for selected non-Abelian simple groups. Existence of solutions has been shown for all but possibly one (Mathieu group M_{23}) of the 26 sporadic simple groups. There is even a polynomial with integral coefficients whose Galois group is the Monster group.

See also

- Differential Galois theory
- Grothendieck's Galois theory

Notes

1. Stewart, Ian (1989). *Galois Theory*. Chapman and Hall. ISBN 0-412-34550-1.
2. (Funkhouser 1930)
3. Cardano 1545
4. Tignol, Jean-Pierre (2001). *Galois' Theory of Algebraic Equations*. World Scientific. pp. 232–233. 302. ISBN 978-981-02-4541-2.
5. Stewart, 3rd ed., p. xxii
6. Clark, Allan (1984) [1971]. *Elements of Abstract Algebra*. Courier Corporation. p. 131. ISBN 978-0-486-14035-3.
7. Wussing, Hans (2007). *The Genesis of the Abstract Group Concept: A Contribution to the History of the Origin of Abstract Group Theory*. Courier Corporation. p. 118. ISBN 978-0-486-45868-7.
8. Scharlau, W., ed. (1981). *Richard Dedekind, 1831–1981: Eine Würdigung*. Braunschweig, Vieweg.
9. Galois, Evariste; Neumann, Peter M. (2011). *The Mathematical Writings of Evariste Galois*. European Mathematical Society. p. 10. ISBN 978-3-03719-104-0.
10. van der Waerden, Modern Algebra (1949 English edn.), Vol. 3, Section 61, p.191
11. V. V. Prasolov, *Polynomials* (2004), Theorem 5.4.5(a)
12. Lang, Serge (1994). *Algebraic Number Theory* (https://books.google.com/books?id=uSeGtAIWgjQ&pg=PA). Graduate Texts in Mathematics. **110**. Springer. p. 121. ISBN 9780387942254.

References

- Artin, Emil (1998). Galois Theory. Dover Publications. ISBN 0-486-62342-4. *(Reprinting of second revised edition of 1944, The University of Notre Dame).*
- Bewersdorff, Jörg (2006). *Galois Theory for Beginners: A Historical Perspective*. American Mathematical Society. doi:10.1090/stml/035 (https://doi.org/10.1090%2Fstml%2F035). ISBN 0-8218-3837-2. .
- Cardano, Gerolamo (1545). *Artis Magnæ* (http://www.filosofia.unimi.it/cardano/testi/operaomnia/ed_4_4.pdf) (PDF) (in Latin).
- Edwards, Harold M. (1984). Galois Theory. Springer-Verlag. ISBN 0-387-90980-X. *(Galois' original paper, with extensive background and commentary.)*
- Funkhouser, H. Gray (1930). "A short account of the history of symmetric functions of roots of equations". *American Mathematical Monthly*. **37** (7): 357–365. doi:10.2307/2299273 (https://doi.org/10.2307%2F2299273). JSTOR 2299273 (https://www.jstor.org/stable/2299273).
- Hazewinkel, Michiel, ed. (2001) [1994], "Galois theory" (https://www.encyclopediaofmath.org/index.php?title=p/g043160), *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- Jacobson, Nathan (1985). *Basic Algebra I* (2nd ed.). W. H. Freeman and Company. ISBN 0-7167-1480-9. *(Chapter 4 gives an introduction to the field-theoretic approach to Galois theory.)*
- Janelidze, G.; Borceux, Francis (2001). Galois Theories. Cambridge University Press. ISBN 978-0-521-80309-0. (This book introduces the reader to the Galois theory of Grothendieck, and some generalisations, leading to Galois groupoids.)
- Lang, Serge (1994). *Algebraic Number Theory*. Berlin, New York: Springer-Verlag. ISBN 978-0-387-94225-4.
- Postnikov, M. M. (2004). *Foundations of Galois Theory*. Dover Publications. ISBN 0-486-43518-0.
- Rotman, Joseph (1998). Galois Theory (2nd ed.). Springer. ISBN 0-387-98541-7.
- Völklein, Helmut (1996). *Groups as Galois groups: an introduction*. Cambridge University Press. ISBN 978-0-521-56280-5.
- van der Waerden, Bartel Leendert (1931). *Moderne Algebra* (in German). Berlin: Springer. . **English translation** (of 2nd revised edition): *Modern Algebra*. New York: Frederick Ungar. 1949. *(Later republished in English by Springer under the title "Algebra".)*

External links

Some on-line tutorials on Galois theory appear at:

- http://www.math.niu.edu/~beachy/aaol/galois.html
- http://mich.maths.org/public/viewer.php?obj_id=1422
- http://www.jmilne.org/math/CourseNotes/ft.html

Online textbooks in French, German, Italian and English can be found at:

- http://www.galois-group.net/