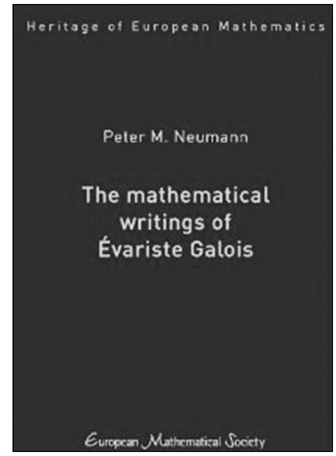
The Mathematical Writings of Évariste Galois

Reviewed by Charles W. Curtis



The Mathematical Writings of Évariste Galois
Peter M. Neumann
European Mathematical Society, October 2011
Hardcover, 421 pages, 78.00 euros
ISBN-13:978-3-03719-104-0

The name Évariste Galois and the subject known today as Galois theory are familiar to anyone who has studied modern algebra. In his short life of twenty years, ended following a duel in May 1832, Galois created the foundations of a large part of algebra as it is studied today, together with individual results that have never lost their sparkle.

There were several French editions of his published work and other writings. These include the testamentary letter to his friend Auguste Chevalier, written on the eve of the fatal duel and published as Galois had requested in the *Revue Encyclopédique* in September 1832. Chevalier served as Galois's literary executor, made copies of two of the most important unpublished works of Galois, and gave them to Joseph Liouville in 1843. Liouville published the *Oeuvres Mathématiques d'Évariste Galois* [10] in his *Journal de Mathématiques pures et appliquées* in 1846. Other editors of the Galois manuscripts were Jules Tannery, who published *Manuscrits et Papiers inédits de Évariste Galois* in 1906, and Robert Bourgne and Jean-Pierre Azra, whose critical edition *Écrits et Mémoires Mathématiques d'Évariste Galois* appeared in 1962.

Translations of the manuscripts into German and Italian have appeared, along with English translations of some of them. The book that is the subject of this review, by Peter M. Neumann, contains an English translation of all of Galois's writings published by Liouville and Tannery and more, with the original on the facing page for purposes of comparison. The author has done a painstaking analysis of the manuscripts, so that the French edition is not simply a reissue of older ones, and has included images of some of the Galois manuscripts from the archives de l'Institut de France. The reproductions provide a fascinating counterpoint to the texts and the translations. The author has also included extensive commentary "focussed on the symbols on the page, on the syntax, on establishing an accurate text." He acknowledges that commentaries "on the semantics, the meaning of what Galois wrote, would be a quite different exercise" and "must be the subject of further studies." Hints of what further mathematical studies might be are included at several places in the notes on individual items. Comments on some of the existing English translations appear, with comparison with the author's version.

The translations begin with the five mathematical articles published in Galois's lifetime, beginning with an article on continued fractions published when he was seventeen in *Annales de Mathématiques pures et appliquées*, edited and published by J. D. Gergonne. In an introductory note, the author states that the article received a friendly review and was cited as recently as 1962 by Davenport, who commented, however, that the material was implicit in earlier work of Lagrange. The fourth, "Sur la théorie des nombres", published when Galois was eighteen, was of great interest and importance, as it contained the original version of a substantial part of the theory of finite fields.

A translation of the testamentary letter of 29 May 1832 addressed to Chevalier appears next. The letter contains a survey of Galois's ideas on the subject of what is now called Galois theory, along with a remarkable new result (with a proof) concerning the simple groups $PSL(2,p)$ and some material on

Charles W. Curtis is emeritus professor of mathematics at the University of Oregon. His email address is cwc@uoregon.edu.

DOI: http://dx.doi.org/10.1090/noti925

integrals of algebraic functions and the theory of elliptic functions.

Several of Galois's works besides the Galois theory of equations led to new developments. A striking example is the result on the simple groups $PSL(2, p)$ contained in the letter to Chevalier. Half a century later Gierster [8] gave a determination of the subgroups of $PSL(2, p)$. This included a new proof of Galois's result. It was taken up again in the last half of the twentieth century by J. H. Conway [4] in connection with exceptional properties of the known simple groups and the discovery of new nonabelian finite simple groups—the sporadic simple groups. Galois's foray into group theory in the letter to Chevalier began with a summary of some properties of the group of linear fractional transformations

$$x \to \frac{ax + b}{cx + d}$$

with x in the finite field F of p elements, for an odd prime p and $ad - bc \neq 0$, which can be identified with the quotient $PSL(2, p)$ of the finite group $SL(2, p)$ of 2×2 matrices of determinant one by its center, of order 2. Galois stated (Neumann's translation), "Thus simplified, the group has

$$\frac{(p + 1))p(p - 1)}{2},$$

permutations. But it is easy to see that it is not further decomposable properly unless $p = 2$ or $p = 3$." In modern terminology, Galois stated that $PSL(2, p)$ is a simple group if $p \neq 2, 3$. As the group $PSL(2, p)$ has a subgroup of index $p + 1$, it has a transitive permutation representation on $p + 1$ elements. Galois raised the question as to whether $PSL(2, p)$ has a transitive permutation representation on a set of fewer than $p + 1$ elements, first pointing out that this is not possible for a set of fewer than p elements. He then stated and gave an outline of a proof of the theorem that the group $PSL(2, p)$ has a transitive permutation representation on a set of p elements when $p = 5, 7, 11$ and does not have a nontrivial permutation representation on a set of fewer than $p + 1$ elements if $p > 11$. The theorem applies to the simple groups $PSL(2, p)$ for $p \geq 5$. It can also be mentioned that the group $PSL(2, 3)$ of order 12 has a transitive permutation representation on a set of 3 elements. Conway examined more closely the cases $p = 3, 5, 7, 11$ in Galois's theorem, leading to exceptional properties of the groups $PSL(2, p)$ in these cases. For example, these include isomorphisms $PSL(2, 3) \cong A_4, PSL(2, 5) \cong A_5$, and a presentation of the sporadic Mathieu simple group M_{12} of order $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ related to a presentation of the simple group $PSL(2, 11)$. Conway continued with an illustration of the way the exceptional permutation representations of the small simple groups $PSL(2, p)$ can arise in other situations by considering the permutation representation of Janko's sporadic simple group J of order 175560 on 266 letters, involving the simple group $PSL(2, 11)$.

In a note preceding the translation of the article "Mémoire sur les conditions de résolubilitié des équations par radicaux", usually referred to as the First Memoir (Premier Memoir), Neumann states, "The memoir on the conditions for solubility of equations by radicals is undoubtedly Galois's most important work. It is here that he presented his original approach to the theory of equations which has now become known as Galois Theory." Galois had submitted it to the Académie des Sciences on 17 January 1831, only to have it rejected and returned to him on the basis of a referees' report by Lacroix and Poisson. In the notes on the first memoir, Neumann provides a translation of the referees' report on it, with comments on the report by J. Tits and the author and some history of further attempts by Galois to interest the Académie des Sciences in his work. In the testamentary letter, Galois gave his view on the situation: "Le premier est écrit, et malgré ce qu'en a dit Poisson, je le maintiens avec les corrections que j'y ai faites." (Neumann's translation: "The first [memoir] is written, and in spite of what Poisson has said about it, I stand by it with the corrections that I have made on it.")

The purpose of the first memoir was to define a finite group, today called the *Galois group*, associated with a polynomial equation $f(x) = 0$ and to derive the necessary and sufficient conditions the group must satisfy in order for the equation to be solvable by radicals. The basic ideas about finite groups needed to carry this out were developed in the memoir for the first time and are part of the early history of finite group theory.

In his book *Galois Theory* [6], Harold Edwards gave an account of the subject "in a way that would not only explain it, but explain it in terms close enough to Galois's own to make his memoir accessible to the reader." With Neumann's translation and commentary on the first memoir now available, Edwards has given a step-by-step presentation, addressed to "modern readers", of the main results in the first memoir [7].

A modern approach to Galois theory (see for example [1]) is based on a study of the splitting field of a separable polynomial with coefficients in a base field. The Galois group of the field extension is the set of automorphisms of the splitting field that leave elements of the base field fixed. The main theorem of Galois theory is the statement that there is a one-to-one correspondence between subgroups of the Galois group and intermediate fields, which are subfields of the splitting field containing the base field. An intermediate field is a normal extension of the base field if and only if the corresponding subgroup of the Galois group is a normal subgroup.

The ideas involved in Galois's description of the subfields of the splitting field of a polynomial in terms of the subgroups of the Galois group have appeared later in other parts of mathematics. For example, they were acknowledged in Chevalley's approach to the notion of a covering space of a topological space and the Poincaré group (or fundamental group) associated with the simply connected covering space. Chevalley stated in his book *Theory of Lie Groups* [2, p. 27]: "The Poincaré group is the group of automorphisms of the simply connected covering space, playing therefore a role similar to that played by the Galois group of an algebraic extension."

The comments I make in this review about Galois's result in group theory in the testamentary letter and the reference to Chevalley's comment about Galois in his *Theory of Lie Groups* represent my own expanded appreciation of Galois beyond the Galois theory of equations. This began when I heard Conway's lecture on exceptional groups at Oxford (where I had been lecturing about Chevalley groups and thinking about simple groups) and realized that, at least for me, Galois's result put his overall contribution in a new light. The reference to Chevalley's book comes from a course on Lie groups which I gave at Wisconsin in the 1950s to an audience including students of R. H. Bing who all knew more topology than I did and were rather dismissive of Chevalley's treatment of covering spaces. I developed the parallel with Galois theory in more detail than Chevalley and found it quite satisfying, even though the topologically inclined students were probably not impressed.

The second memoir, "Des équations primitives qui sont solubles par radicaux", contains further development of the theory of permutation groups in connection with the problem stated in the title. As Neumann says, "That this is an old unfinished piece of work that Galois had intended to amplify, polish and publish seems clear." With reference to the second memoir, the author says in an epilogue "Myths and Mysteries" (p. 386): "The *Lettre testamentaire* bears witness to the fertility of his mind and very strongly suggests that he had created much mathematics that goes a long way beyond what he had published and what he had drafted in the *Premier Mémoire*. One can—and many writers do—build an edifice of conjecture on the brief sketch he gave there. Much, though not all, of what he wrote about primitive soluble equations (or groups) and about the groups now known as $PSL(2, p)$ is supported in part in the *Second Mémoire*."

The remaining translations, in a chapter entitled "The Minor Mathematical Manuscripts", include what are often fragments relating to the first and second memoirs and other topics, such as Galois's explanation of how his work was independent of Abel's work on the general equation of the fifth degree. On this point Galois stated (in Neumann's translation), "but he has left nothing on the general discussion of the problem which has occupied us. Once and for all, what is remarkable in our theory is to be able to answer yes or no in all cases" (with the last few words crossed out and replaced by the single word "répondre"). This is surely an indication of Galois's anticipation of the modern approach to parts of the mathematics of today, characterized by the search for general solutions to problems.

The items in the chapter are organized into dossiers from a volume of manuscripts in the library of the Institut de France. Neumann has "sought to reproduce [each] manuscript as accurately as possible in print, with all its crossings-out, emendations, additions, and quirks of writing." Notes are included before and after each item, with detailed comparisons to corresponding parts of the material in the editions of Tannery and of Bourgne and Azra, and occasionally mathematical topics the author plans to explore. This part of the book with the texts and the accompanying notes fills in the sketchy picture we have of Galois's mathematical persona in a particularly satisfying way and will be an important reference for further studies of Galois's mathematics.

The collected works show that Galois's thinking was not restricted to his group-theoretic approach to the theory of equations, complete and satisfying as it was. His results on exceptional permutation representations of the simple groups $PSL(2, p)$ put him in the company of twentieth-century group theorists in their search for new nonabelian finite simple groups. Another topic that started with Galois and which would require a long and multifaceted article in order to describe its place in today's mathematics is the theory of finite fields. I shall mention here only a few things about finite fields and linear groups. The starting point is the great book of C. Jordan [9], *Traité des substitutions et des équations algébriques*, published in 1870, on linear groups over the finite field of p elements for a prime p, with applications to Galois theory. In the preface the author mentions works he consulted, beginning with the works of Galois, on which, he states, his book (of over 600 pages) is a commentary! He credits Galois for calling attention to the distinction of whether a group is simple or not. He defines what are now called the classical groups—the general linear group, the orthogonal group and the symplectic group—on a finite dimensional vector space over the finite field of p elements. For each type of group, he calculates the order and the composition factors. In 1900 L. E. Dickson published *Linear Groups, with an Exposition of the Galois Field Theory* [5]. The first part of the book contains a thorough presentation of Galois's theory of finite fields. The main point of the book is to carry over Jordan's work on the classical groups over the field of p elements to the corresponding theory for classical groups over a general finite field. The nonabelian finite simple groups obtained as composition factors of the classical groups, along with twisted versions of them and the alternating groups, were the only known infinite families of nonabelian simple groups until Chevalley's paper "Sur certains groupes simples" [3] gave new infinite families of nonabelian finite simple groups associated with the exceptional simple Lie algebras.

The book, in the author's words, "is conceived as a contribution to the history of mathematics." It also gives a mathematically knowledgeable reader a chance to follow a series of groundbreaking mathematical events, from Galois's invention of what he needed from group theory in order to solve the problem stated in the title of the first memoir to his first steps towards establishing group theory as an independent subject, beginning with the second memoir and continuing with his determination, in the letter to Chevalier, of the exceptional permutation representations of the linear fractional groups. It's quite a story.

References

[1] E. Artin, *Galois Theory*, Notre Dame Mathematical Lectures, Number 2, University of Notre Dame, 1946.

[2] C. Chevalley, *Theory of Lie Groups*, Princeton University Press, 1946.

[3] C. Chevalley, Sur certains groupes simples, *Tôhoku Math. J.* (2) **7** (1955), 14–66.

[4] J. H. Conway, Three lectures on exceptional groups, Chapter VII in *Finite Simple Groups*, M. B. Powell and G. Higman, eds., Academic Press, London, 1971.

[5] L. E. Dickson, *Linear Groups, with an Exposition of the Galois Field Theory*, Dover Publications, New York, 1958.

[6] H. M. Edwards, *Galois Theory*, Springer-Verlag, New York, 1984.

[7] H. M. Edwards, Galois for 21st century readers, *Notices Amer. Math. Soc.* **59**, no. 7 (2012), 912–923.

[8] J. Gierster, Die Untergruppen der Galois'schen Gruppe der Modulargleichungen für den Fall eines primzahligen Transformationsgrades, *Math. Annalen* **18** (1881), 319–365.

[9] C. Jordan, *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris, 1870.

[10] J. Liouville (ed.), Oeuvres Mathématiques d'Évariste Galois, *Journal de Mathématiques pures et appliquées* **XI** (1846), 381–444.