Évariste Galois's memoir on the conditions for the solubility of equations by radicals (1831)

by Caroline Ehrhardt
History of Education Department,
National Institute for Pedagogical Research (INRP)

Évariste Galois submitted his *Mémoire sur les conditions de résolubilité des équations par radicaux* (Memoir on the conditions for the solubility of equations by radicals) to the French Academy of Sciences, one year before his death at the age of 21. This was the third version of Galois's research on this subject: the first two manuscripts, which had already been communicated to the Academy, had been lost. This last work did not receive the Academy's approval, despite an encouraging report in which Poisson and Lacroix invited the young mathematician to pursue his research with a view to honing his results. However, Galois devoted the final months of his life to another area of research – elliptic functions. He was killed in a duel in 1832, his memoir on equations still unfinished. This memoir would be published only in 1846, in the *Journal de Liouville*.

***Figure 1*: Portrait of Évariste Galois by his brother.**

In this memoir, Évariste Galois sought a necessary and sufficient condition for an equation to be solvable by radicals, *i.e.* for it to be possible to express its roots through algebraic operations involving the coefficients. In the early 19th century, mathematicians knew how to solve fourth-degree equations or less by explicitly calculating their roots. In 1826, the Norwegian mathematician Abel had succeeded in demonstrating a theorem, the exactitude of which had been anticipated since the work of Lagrange: an algebraic solution is impossible for fifth-degree equations or higher.[1] In this context, Galois did not seek to obtain a formula that would make it possible to calculate roots, but rather a criterion to establish whether this calculation was possible or not.

Second-degree equations

For example, all second-degree equations (in the form $ax^2 + bx + c = 0$) can be solved algebraically in the field of complex numbers. This involves calculating their discriminant: $\Delta = b^2 - 4ac$.

The two roots are then given by the formula:

$$\frac{-b \pm \sqrt{\Delta}}{2a} \text{ si } \Delta > 0 \text{ ou } \frac{-b \pm i\sqrt{\Delta}}{2a} \text{ si } \Delta < 0$$

We see here that the roots are calculated using algebraic operations involving the coefficients a, b and c of the equation. The criterion given by Galois in his article does not make it possible to obtain these formulas; it simply guarantees that all second-degree equations are solvable in the field of complex numbers.

@@@@@@@

1) The "principles"

Galois's memoir begins by setting out the principles on which the analysis is based: the notion of adjunction and substitutions. According to the definition given by Galois, to adjoin a quantity to an equation means that it is considered known for the solution (see panel below); the rational functions thus used to express the roots are functions of the coefficients of the equation and of that quantity. This notion, traces of which can be found in the earlier work of Abel, was innovative compared to the research conducted in the 18th century: the

1. Niels Henrik Abel, "Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degree", *Crelle's Journal*, vol. 1, 1826; Joseph-Louis Lagrange, "Réflexions sur la théorie algébrique des equations", *Mémoire de l'Académie royale des sciences et belles-lettres de Berlin*, 1770, p. 134–215, 1771, p. 238–253.

reasoning of Lagrange and Ruffini[2] was confined to numbers that could be formed from the coefficients of the equation. For Galois, the irreducibility of an equation is relative to the quantities that one adjoins to it, which implies that:

> *When we thus agree to regard certain quantities as shown, we shall say that we adjoin them to the equation which it is required to solve … The adjunction of a quantity can render an irreducible equation reducible*.[3]

Adjoining a quantity

Let's take an example to shed light on this notion of adjunction. A second-degree equation with negative discriminant does not admit a real root (see previous panel). We say that it is irreducible in the field of real numbers. On the other hand, the equation becomes reducible if we move to the field of complex numbers, *i.e*. if we adjoin the quantity i, defined by $i^2 = -1$. The roots are therefore expressed as functions of the coefficients of the equation and the quantity i.

The second preliminary notion introduced by Galois is that of substitution, as "the passage from one permutation to another". The idea of linking the study of equations to the study of the permutations of their roots dates back to the work of Lagrange and Vandermonde,[4] published in the late 18th century.[5] Indeed, one of the reports written in 1813 by the Academician Poinsot should be enough to convince us that in the early 19th century this principle was still considered a fruitful avenue of research in the theory of equations:

> *The principles that regard this problem [algebraic solution] reside essentially in the theory of combinations and that of numbers. That is what one may demonstrate by the nature of things and, … if it is possible to advance further, it is only by ideas of the same genre and by a few new elements which are still missing from the theory of permutations.*[6]

Galois's research was thus perfectly consistent with the issues of his day in terms of the means that were to be deployed. The definitions he gives for the terms "substitution" and "permutation" are borrowed from the articles published

2. Paolo Ruffini (1765–1822) was an Italian mathematician who in 1799 published a work in which he demonstrated that fifth-degree equations are not soluble by radicals. The exactitude of the proof he had put forward caused some controversy among mathematicians of the day.
3. --Trans. Translation taken from Peter M. Neumann, *The Mathematical Writings of Évariste Galois*, European Mathematical Society, 2011, p. 109, available here.
4. Alexandre Vandermonde (1735–1796) was a French mathematician close to Gaspard Monge. He was elected to the French Academy of Sciences in 1771.
5. Lagrange, *op. cit.*; Alexandre Vandermonde, "Mémoire sur la résolution des equations", *Histoire de l'Académie royale des sciences, avec les mémoires de mathématiques et de physique tirés des registres de cette Académie*, Paris, 1774, p. 365–416.
6. *Procès-verbaux des séances de l'Académie des sciences*, vol. 5, session of 27 December 1813, p. 294.

by Cauchy in 1815.[7] It should be noted here that the theory of permutations remained little explored at the time, since Abel and Galois were the only two mathematicians to have exploited the results Cauchy had obtained. Furthermore, the articles of 1815 only sketched the outlines of the theory, which Cauchy would not flesh out more fully until 1844.[8] This explains why Galois does not have a perfect mastery of these notions: he seems to know this work, as is shown by the allusion he later makes in Proposition VII, but the terms "groups of permutations" and "groups of substitutions" are often confused in his memoir. Thus Galois defines the group of an equation as the "group of permutations" of the roots, while also stating that:

> *in the group of permutations considered here, the order of the letters is not of importance, but rather only the substitutions of the letters by which one passes from one permutation to another.*[9]

Permutations and substitutions –
Example of a group of substitutions

– A permutation of n distinct letters is an ordered list of these letters. For example: (1,2,3,4,5) and (2,5,3,1,4) are permutations of 5 letters.
– Substitutions are operations that consist in moving from one permutation to another. In 1844, Cauchy introduced a two-line mathematical notation of this process:
For example: the substitution $\begin{pmatrix}1,2,3,4,5\\2,5,3,1,4\end{pmatrix}$ transforms 1 into 2, 2 into 5, 4 in 1 and 5 into 4.
If we confine ourselves to the modern definition of a group, a group is formed by substitutions of n letters and not by permutations.
What Galois calls a "group of permutations" is the set, which he notes in a "matricial" form. This is not a group in the modern sense of the term. On the other hand, the quotation shows that he was also interested in the ("real") group that can be constructed from these permutations, although this is not mentioned explicitly.

@@@@@@@

7. Augustin-Louis Cauchy, "Sur le nombre de valeurs qu'une fonction peut acquérir lorsqu'on y permute de toutes les manières possibles les quantités qu'elles renferment", *Journal de l'École polytechnique*, n° 10, 1815, p. 1–28; Augustin-Louis Cauchy, "Sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment", *Journal de l'École polytechnique*, n° 10, 1815, p. 29–112.
8. Augustin-Louis Cauchy, "Mémoire sur les arrangements que l'on peut former avec des lettres données, et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre", *Exercices d'analyse et de physique mathématique*, vol. 3, 1844, p. 151–252.
9. --Trans. Translation taken from David A. Cox, *Galois Theory*, 2nd ed., John Wiley and Sons, 2012, p. 343, available here.

To give an example of a group of substitutions in the modern sense of the term, the group S_3 of the substitutions of three elements 1, 2, 3 is composed of the six following substitutions: the identity Id, the circular substitution s_1 $\begin{pmatrix}1,2,3\\3,1,2\end{pmatrix}$, the circular substitution s_2 $\begin{pmatrix}1,2,3\\2,3,1\end{pmatrix}$, the transposition t_1 $\begin{pmatrix}1,2,3\\1,3,2\end{pmatrix}$, the transposition t_2 $\begin{pmatrix}1,2,3\\3,2,1\end{pmatrix}$, and the transposition t_3 $\begin{pmatrix}1,2,3\\2,1,3\end{pmatrix}$. The table of this group is as follows:

	ID	**s_1**	**s_2**	**t_1**	**t_2**	**t_3**
ID	ID	s_1	s_2	t_1	t_2	t_3
s_1	s_1	s_2	ID	t_3	t_1	t_2
s_2	s_2	ID	s_1	t_2	t_3	t_1
t_1	t_1	t_2	t_3	ID	s_1	s_2
t_2	t_2	t_3	t_1	s_2	ID	s_1
t_3	t_3	t_1	t_2	s_1	s_2	ID

Another thing that can be noted is that Galois does not adopt the two-line notation for substitutions introduced by Cauchy. For the modern-day reader, the abstruseness of Galois's memoir is mainly due to its rather approximate use of the notions of substitution and permutation. The same must have been true for the mathematicians of the early 19th century, who were unaccustomed to using them in an abstract sense: though Lagrange had used them in his research on equations, this was more as a calculatory method than as a conceptual tool.

The statement of "Principles" ends with four lemmas relating to the theory of equations. The first is stated as follows:

> *Lemma I. An irreducible equation cannot have any root in common with a rational equation without dividing it.*[10]

This lemma signifies that if an irreducible polynomial P has a root in common with another polynomial f, f can thus be written as: $f(x) = P(x) \times Q(x)$
It might be useful here to give an example from the field of real numbers.
The polynomial $P(x) = x^2 + 1$ is irreducible in R. Its roots in C are *i* and $-i$.
The polynomial $f(x)= x^3 - x^2 + x - 1$ is not irreducible in R (since 1 is its root). In C, its roots are 1, *i* and $-i$.
We can write: $f(x)= P(x) \times (x-1)$

10. Peter M. Neumann, *op. cit.*, p. 111.

This result was not unprecedented: it had already been demonstrated by Abel in his *Mémoire sur une classe particulière d'équations résolubles algébriquement* (Memoir on a particular class of soluble algebraic equations), published in *Crelle's Journal* in 1829.

@@@@@@@

For the second and third lemmas, Galois takes up the fundamental idea of similar functions that Lagrange had developed in his *Réflexions sur la résolution algébrique des équations* of 1770: he seeks a function V of the roots taking *n!* distinct values by permutations of the roots. This function will thus be similar to a function that gives the *n* roots of the initial equation:

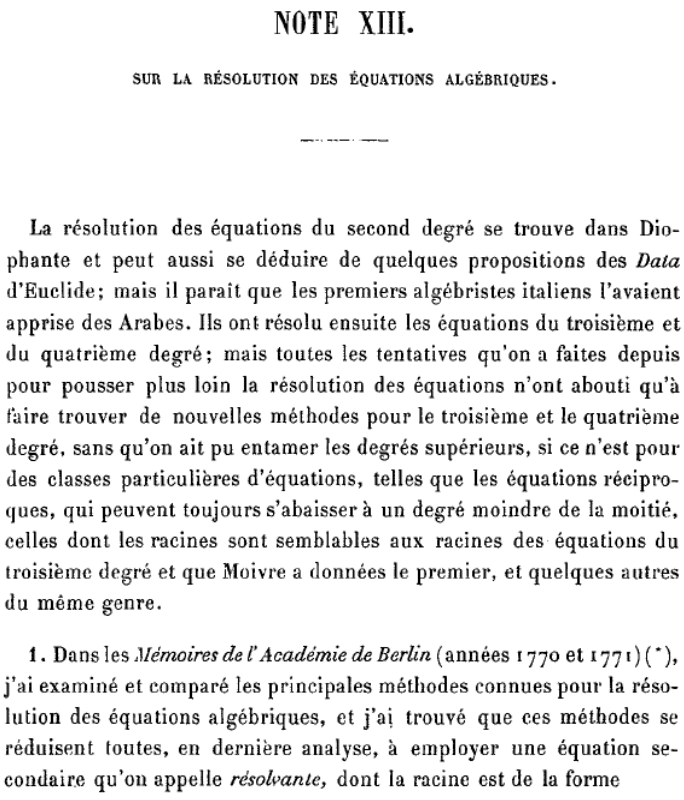
> *Lemma II. Given an arbitrary equation which has no equal roots, of which the roots are a, b, c, …, one can always form a function V of the roots, such that none of the values that are obtained by permuting the roots in this function in all possible ways will be equal.*
>
> *Lemma III. The function V being chosen as is indicated in the preceding article, it will enjoy the property that all the roots of the proposed equation will be rationally expressible as a function of V.*[11]

Rational and resolvent expression

A rational function is the quotient of two polynomials.
In the sense that Galois intends, to say that the roots can be expressed rationally as a function of V means that each root x_i can be written in the form $x_i = \frac{P(V, \sqrt{a}, \sqrt{b}...)}{Q(V, \sqrt{a}, \sqrt{b}...)}$, where P and Q are two polynomials.
The following can be given as an example of a resolvent: $V(x,y) = x^2 + y^2$, where x and y are solutions to a second-degree equation $X^2 + PX + Q = 0$, is invariant by the two substitutions of the group S_2, and Id and s substitution of the roots. In this case it can be shown that V can be rationally expressed as a function of the coefficients of the equation: $V(x,y) = (x+y)^2 - 2xy = P^2 - 2Q$.

Here again, Galois adopts a solution schema that is consistent with the algebraic practices of his time, and which consists in deploying an intermediary stage by defining a resolvent function.

11. Peter M. Neumann, *op. cit.*, p. 111.



NOTE XIII.

SUR LA RÉSOLUTION DES ÉQUATIONS ALGÉBRIQUES.

La résolution des équations du second degré se trouve dans Diophante et peut aussi se déduire de quelques propositions des *Data* d'Euclide; mais il paraît que les premiers algébristes italiens l'avaient apprise des Arabes. Ils ont résolu ensuite les équations du troisième et du quatrième degré; mais toutes les tentatives qu'on a faites depuis pour pousser plus loin la résolution des équations n'ont abouti qu'à faire trouver de nouvelles méthodes pour le troisième et le quatrième degré, sans qu'on ait pu entamer les degrés supérieurs, si ce n'est pour des classes particulières d'équations, telles que les équations réciproques, qui peuvent toujours s'abaisser à un degré moindre de la moitié, celles dont les racines sont semblables aux racines des équations du troisième degré et que Moivre a données le premier, et quelques autres du même genre.

1. Dans les *Mémoires de l'Académie de Berlin* (années 1770 et 1771)(*), j'ai examiné et comparé les principales méthodes connues pour la résolution des équations algébriques, et j'ai trouvé que ces méthodes se réduisent toutes, en dernière analyse, à employer une équation secondaire qu'on appelle *résolvante*, dont la racine est de la forme

***Figure 2*: The famous "Note XIII" in Lagrange's work on equations**. *Galois studied these equations as a lycée student.*

2) THE THEORY

The original parts of Galois's research, which he calls his "theory", only start after he reiterates these principles, which, according to him, are too well known for it to be necessary to provide new demonstrations.

Many demonstrations are barely sketched out, or are simply absent from the *Mémoire sur les conditions de résolubilité des équations par radicaux*. On this point, it is often said that Galois died too young and suddenly to perfect his theory.
However, it is highly likely that the absence of demonstrations for these lemmas was a choice and not a necessity. Indeed, in the preface that he had written to the *Mémoire*, and which was not published in the *Journal de Liouville*, Galois explains that it is not useful to "to repeat the rudiments of the whole theory, on the pretext of presenting it in an intelligible form".[12]

Proposition I defines the "group of an equation" as a group of permutations of the roots:

12. Évariste Galois, "Préface à deux mémoires d'analyse pure".

Let an equation be given of which the m roots are a, b, c, … . There will always be a group of permutations of the letters a, b, c, … which will enjoy the following property:

1. *That every function of the roots invariant under the substitutions of this group will be rationally known;*
2. *Conversely, that every function of the roots that is rationally determinable will be invariant under the substitutions.*[13]

Galois's demonstration consists in exhibiting the "group" and showing that it satisfies the required properties. It should be noted, however, that Galois has no intention of proving that this is a group in the modern sense of the term: for him, the group of an equation is an organised set – i.e. one that can be written in the form of a table – and not a set for multiplication.

Propositions II and III then establish the link between the group of the equation and the adjoined quantities: the adjunction of a new magnitude entails the group of the equation being divided into a certain number of smaller and comparable groups (in modern language, these are normal sub-groups of the initial group). We can then recommence this reasoning with the new group thereby obtained, and so and so forth. The demonstration of Proposition III is incomplete: in fact, the form of the factorisation after the adjunction of a new quantity of the equation, of which the resolvent V is a root, is not as "clear" as Galois says it is, and this point would receive attention from many of Galois's successors. As for Proposition III, it is stated without any demonstration.

In Proposition II, Galois states that if the adjunction of a root r of an auxiliary equation renders the given equation reducible, then the polynomial P of which the resolvent is the root can be factorised as follows:
$P(V) = f(V,r) \times f(V,r') \times f(V,r'')\ldots$, where r, r', r'', … are the different roots of the auxiliary equation of the resolvent, and where function f remains the same.
However, this decomposition is far from obvious since, after the adjunction of a quantity r, if one applies the usual results of the factorisation of polynomials, one obtains a decomposition in the following form:
$P(V) = f(V,r) \times f_1(V,r) \times f_2(V,r)\ldots$, where the functions f_i are different but involve the same variables V and r.

13. Peter M. Neumann, *op. cit.*, p. 114– 115.

In Proposition V in the memoir, Galois shows that the initial equation is solvable by radicals, if, at the end of the process, one obtains a group that now contains only one element:

> *To solve an equation, it is necessary to reduce its group successively to the point where it does not contain more than a single permutation*.[14]

Example of Propositions II and V applied to a particular fourth-degree equation

Take the equation $x^4 - 5x^2 + 6 = 0$; it factorises into $(x^2 - 2)(x^2 - 3) = 0$ and its roots are $\pm\sqrt{2}$ et $\pm\sqrt{3}$. There originally exists a group of 4 substitutions permuting these roots: Id, X (inversing $\sqrt{2}$ and $-\sqrt{2}$, leaving $\sqrt{3}$ and $-\sqrt{3}$) fixed, Y (inversing $\sqrt{3}$ and $-\sqrt{3}$, leaving $\sqrt{2}$ and $-\sqrt{2}$ fixed), Z = XoY (inversing $\sqrt{2}$ and $-\sqrt{2}$, inversing $\sqrt{3}$ and $-\sqrt{3}$). This is the Galois group specific to this equation.

By applying Proposition II, and by successively adjoining the quantities $\sqrt{2}$ and $\sqrt{3}$, the Galois group is gradually reduced (mathematicians also say "unscrewed"). For example, in the field of rationals to which one adjoins $\sqrt{3}$ (the set of "quadratic integers" $a + b\sqrt{3}$, noted as $\mathbb{Q}[\sqrt{3}]$), there exist new relations between roots within $\mathbb{Q}[\sqrt{3}]$, made possible by this extension of Q (for example, $2\sqrt{3} \times \sqrt{\mathbf{3}} + \sqrt{3} \times \mathbf{(-\sqrt{3})} = 3$, the polynomial of the roots $\sqrt{3}$ and $-\sqrt{3}$, in bold, which remains in $\mathbb{Q}[\sqrt{3}]$). In this extension, the substitutions Y and Z no longer preserve this polynomial, while X (inversion of the roots $\sqrt{2}$ and $-\sqrt{2}$) continues to preserve it: the initial Galois group Id, X, Y, Z has been reduced to its sub-group Id, X. When one adjoins $\sqrt{2}$, in the field $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ composed of numbers of the type $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3}$, the only substitution that conserves the polynomial is Id: to take Galois's expression, we have "reduced" the group "to the point where it does not contain more than a single permutation". The equation is therefore solvable by radicals.

This example illustrates Proposition II – *"If one adjoins to a given equation the root r of an irreducible auxiliary equation, one of two things will happen: either the group of the equation will not be changed, or it will be partitioned into p groups each belonging respectively to the proposed equation when one adjoins to it each of the roots of the auxiliary questions"* – as well as Proposition V mentioned above – *"To solve an equation, it is necessary to reduce its group successively to the point where it does not contain more than a single permutation"*.

14. Peter M. Neumann, *op. cit.*, p. 121.

However, instead of stating his result as a theorem, Galois algorithmically describes the mechanism connecting the process of adjunction to that of the decomposition of the group.

Such a writing technique was unusual in the early 19th century, since it provides a narrative in which the intermediary results are not explained, rather than a calculatory proof. Thus, although Proposition V makes it possible to understand *why* some equations will be soluble, and others not, it does not say *how* one should go about solving it in practical terms, using a specific equation to respond to the question. According to the criteria of the early 19th century, where the utility of mathematics still lay above all in its practical applicability to concrete phenomena, such a conclusion was in no sense satisfactory. In essence, this was what Poisson wrote in his report:

> *[The memoir] does not contain the condition of solvability of equations by radicals … The condition of solvability, if it exists, should have an external character, that can be tested by examining the coefficients of a given equation, or, at most, by solving other equations of a lesser degree than that proposed.*[15]

In Propositions VII and VIII, Galois applies the preceding results to irreducible first-degree equations. Proposition VII states the criterion in the language of groups:

> *If an irreducible equation of a prime degree is soluble by radicals, the group of this equation must contain only substitutions of the form* x_k, x_{ak+b}, *a and b being constants.*

Finally, the criterion of solvability is translated in the traditional language of equations in Proposition VIII:

> *In order that an irreducible equation of prime degree should be soluble by radicals, it is necessary and sufficient that any two of its roots being known, the others may be deduced from them rationally.*

The solution group of an equation

The notion of the group appears in Galois's memoir. He writes "if in a group one has the substitutions S and T then one is sure to have the substitution ST". One hundred years later, Gustave Verriest, in a text of 1934 entitled *Évariste Galois et la théorie des équations*

15. *Procès-verbaux des séances de l'Académie*, session of 4 July 1831, t. 9, p. 660; --Trans. Translation taken from Laura Toti Rigatelli, *Évariste Galois 1811–1832*, trans. John Denton, Birkhäuser Verlag, 1996, p. 90.

algébriques,[16] suggested that Galois had enabled the discovery that "the crux of the problem lies not in the direct search for the magnitudes to adjoin, but in the study of the nature of the group of the equation. This group expresses the degree of indiscernibility of the roots: it thus characterises not what we know of the roots, but that which we do not know … thus it is that two equations of different degrees, but with similar groups, are solved in the same way. Therefore, it is no longer the degree of an equation that measures how difficult it is to solve, but the nature of its group." In fact, the solution group of a given equation measures the degree of indiscernibility of its solutions, or, put differently, the symmetries of the equation.

3) Architecture and conception of the *Mémoire*

The *Mémoire sur les conditions de résolubilité des équations par radicaux* is written in a very concise style; some demonstrations are absent and others incomplete. This incompleteness is often put down to the tragic circumstances of Galois's life and his premature death, which, it is argued, prevented him from writing up his research after the early versions were lost. Yet analysis of the original manuscript shows that this work, although incomplete, had already been corrected and reread several times over. Moreover, Galois judged it sufficiently complete to submit to the Academy. It is therefore a fully-fledged piece of research, and not a summary of results previously obtained: although the memoir existed in a more complete state in previous versions submitted to the Academy, the explanations that are presumed missing are *not there* precisely because Galois deliberately decided not to include them in the last version, or because he himself did not yet possess the necessary demonstrations. If we overlook the impression of incompleteness and the imprecise vocabulary that characterise the entire first memoir, and give a wholesale impression of obscurity, we notice that Galois treated the three different parts in noticeably different ways. These reveal the manner in which he conceived his research.

The "Principles" with which the memoir begins consist in "a few definitions and a series of lemmas known to all". The first four lemmas are separated from the rest of the presentation, and Galois does not attach any importance to their

16. Quoted by Norbert Verdier, *Pour la science- les Génies de la science, Evariste Galois,* February–May 2003 (see "Pour en savoir plus" tab on *BibNum*).

demonstration: for him they fell within the classical theory of equations and were not part of the theory he wished to establish.

Propositions I to V form the heart of the memoir, setting out what would later be described as "Galois theory". In this part, Galois establishes the principle of correspondence between equations and groups of substitutions. These propositions are the object of abstract proofs, in the sense that the results are described in French and not written in mathematical language, and are pursued without an explicit explanation of the calculations from which they result or in which they culminate. The idea is to set out "the functioning of the analysis", to use one of Galois's expressions, that is to say, to describe how the process must unfold, and not to go through all the operations.

The concision of this section was not due to lack of time. Among Galois's papers one finds a first version of Proposition I on the group of an equation, very probably dating from June 1830, and including a demonstration more detailed than that found in the final version. The same is true of Proposition III, of which the initial version – crossed out during the correction stage – is in fact an application of the previous proposition to equations in the form "$x^p = a$", with which Galois must have familiarised himself by reading Gauss's *Disquisitiones Arithmeticæ*. In the final version of the manuscript, it was replaced by a much more general theorem, which also seems to derive from Proposition II but is stated without a demonstration.

The aim of Galois's editing work seems to have been to get right to the essential points. Indeed, the memoir of the conditions for the solubility of equations offers a fine example of mathematical thought under construction. Galois did not leave us the genealogy of his work, but it was most probably by familiarising himself with the traditional theory of equations, and by learning to manipulate substitutions and permutations on the basis of specific equations, using the traditional calculating method of Lagrange or Abel, that he formulated his initial ideas on the link between solvability and the group of substitutions of roots. Some of the extant drafts contain numerous algebraic calculations, sometimes juxtaposed on the same sheet with manipulations of the permutations of integers: it was by dint of practice and training – in a sense, by immersing himself in classical theory – that Galois arrived at his initial results. However, none of these calculations was retained in the definitive draft of his work.

***Figure 3*: An example of one of Galois's extant drafts**
(some are much clearer).

These few examples show that Galois was not expressly trying to avoid calculations, nor to strive for the greatest possible degree of generality. Concrete algebraic manipulations of specific cases of equations are an integral part of his research. It was only once he had inductively understood the principles governing these calculations that he removed them from his work. As Galois explains in the preface which Liouville did not publish,[17] these are mere "details" over which "the mind no longer has time to pause". They would remain in draft form and were ultimately absent from the drafting of this – very sparse – memoir. Once he was sufficiently at ease with the calculations, Galois's approach was to extract their essence in his attempt to understand what makes an equation soluble. His general theory was thus formulated through a permanent to-ing and fro-ing between this theory and concrete cases, which became its applications.

The third part of the memoir, comprising Propositions VI to VIII, is an illustration of the preceding theory in the case of irreducible first-degree equations (i.e. where the degree is a prime number). This application is approached in a more "calculatory" manner, although that term may seem surprising when talking about Galois's mathematics. However, while the operations are not always set out in the text, their result appears in the text in algebraic language and not in French. For example, Galois makes the effort to

17. This preface is included in Galois's Complete Works: Évariste Galois, *Ecrits et mémoires mathématiques, édition critique intégrale des manuscrits et publications d'Evariste Galois par Robert Bourgne et Jean-Pierre Azra, Paris*, Gauthier-Villars, 1962 (reed. Jacques Gabay, 1997).

write the last group involved in the solution of irreducible first-degree equations, and to express the substitutions he uses: the presentation is therefore more concrete than for Propositions I to V. However, the application here does not have any practical purpose, since Galois does not provide an algorithm that would make it possible to decide if a given equation is soluble by radicals: the final result remains theoretical. Rather than providing a practically exploitable criterion, the aim of this application to first-degree equations thus seems to be to elucidate the general principles according to which Propositions I to V are formulated (indeed, Galois was aware that he had not managed to express these principles with as much precision as would have been desirable). His indifference to the practical feasibility of his reasoning is clear when, to conclude, he gives the example of the fifth degree: he writes down the group of substitutions that such an equation must have in order to be soluble, rather than showing how to decide on the solubility of a given equation of which the numerical coefficients have been determined in advance.

@@@@@@@

The *Mémoire sur les conditions de résolubilité des équations* is often described as a prophetic text, one too ahead of its time to be understood by its contemporaries. Nevertheless, it is based on knowledge and know-how that would have been familiar to mathematicians in the early 19th century, since it draws on a mathematical tradition stretching back to Lagrange and attempts to play on the theory/applications dialectic that was so dear to the Polytechnicians who then dominated Parisian mathematical circles. Recognising that Galois's *Mémoire* was not inaccessible to his contemporaries and that it engaged with the issues of its day is not to deny its mathematical value; it simply entails taking the historical value of this document seriously as well.

■

(December 2008)

(Translated by Helen Tomlinson, published October 2016)