Évariste Galois

(1811–1832)

HIS LIFE AND WORK

When you are young, your world knows no bounds. Everything is possible. Solutions for all the world's ills, no matter how complex, lie within your grasp, no matter how radical those solutions may be. How ironic that Évariste Galois, the shortest-lived mathematician chronicled in this book, made his mark by proving that there is no general solution by radicals for polynomial equations of the fifth degree or higher.

On October 25, 1811, Nicholas-Gabriel Galois and his wife Adelaide-Marie, née Demante, became parents of a son, Évariste, perhaps the most precocious mathematician of all time. We have no record of mathematical talent on either side of Évariste's family. Nevertheless he came from good intellectual stock. His maternal grandfather and an uncle on that side of his family were jurists at the Faculty of Law in Paris. His father and paternal grandfather were headmasters of a school.

Galois grew up in his birthplace of Bourg-la-Reine, a town about five miles outside of Paris, which his father served as mayor when Napoleon returned to power during the One Hundred Days in 1815. Adelaide-Marie served as her son's only teacher until he turned twelve. She gave him a good foundation in Greek and Latin and passed on the religious skepticism she shared with her husband.

In 1823 at age twelve, Galois' parents enrolled him as a boarder in the fourth class at the prestigious Lycée of Louis-le-Grand in Paris. This famous preparatory school, which still exists, already numbered both Robespierre and Victor Hugo among its alumni. It is likely that Galois' parents thought that Louis-le-Grand would be a liberal environment in which their son would be nurtured amidst a country that was becoming more royalist and more conservative. They turned out to be very mistaken.

During Galois' first few months at Louis-le-Grand, a large number of students rebelled against the headmaster's plan to bring a conservative Jesuit faculty back to the school. Some students refused to recite in class. Some refused to sing at a mandatory chapel service. Many refused to toast the dying King Louis XVIII. Although this behavior was characteristic of Galois' later teenage years, we have no way of knowing whether he was among the rebels. In any case, Galois was not one of the forty students the headmaster summarily expelled in response to the rebellion.

Perhaps Galois did not participate in the rebellious activities after all. He had a sterling record during his first two years at Louis-le-Grand, earning a first prize and several honorable mentions for his academic work. But then Galois became bored with his studies, performed poorly in his third year, and had to repeat it. Fortunately, he took his first mathematics course when he repeated his third year and he flourished. This class introduced him to Legendre's textbook on Geometry, which Galois is said to have read with the speed of someone reading a novel.

Galois did not merely flourish. He engulfed himself in mathematics, doing this at the cost of his other work. Soon he was receiving poor marks in all of his courses except mathematics. His rhetoric instructor described him as "dissipated." Only his mathematics instructor, Vernier, recognized Galois' burning genius. He wrote

> *Mathematics is the passion that dominates him. I think it would be best for him if his parents allowed him to study nothing else. He is wasting his time here and does nothing but torment his teachers, and overwhelm himself with punishments.*

Vernier also wrote that his pupil needed to acquire more method, but Galois would have none of that. Against Vernier's advice, Galois took the entrance examination to the prestigious l'École Polytechnique a year early and without even taking the usual preparatory course for the exam. Not surprisingly, Galois failed to gain admission because he lacked mastery in several basic areas of mathematics. To Galois this was a great injustice, even when Vernier tried to explain that he should not be surprised.

Nevertheless, Vernier encouraged Galois to enroll in a special mathematics class provided by the great teacher Louis Paul Emile Richard. Richard soon recognized

Galois' genius and tried to get his star admitted to l'École Polytechnique without taking their entrance examination. Not surprisingly, l'École refused to consider that approach. In response, Galois drifted more and more from the work in Richard's course and began work on a short paper on continued fractions that he published in the *Annales des mathematiques* in March 1829 at the age of seventeen!

Galois spent the Spring of 1829 working on his first paper on the resolution of algebraic equations to the *Academie des Sciences* and getting ready to retake the entrance examination for l'Ecole Polytechnique in July. Once again, matters did not go smoothly. Some time in June of that year, a priest forged Galois' father's name on a number of scurrilous notes that greatly offended many members of the larger Galois family. Shamed by the scandal that followed, Galois' father committed suicide on July 2. Not surprisingly, Galois disastrously failed the entrance examination for l'École Polytechnique. Consequently, he had to settle for l'École Normale, a school for training secondary school teachers!

The paper fared little better. The *Academie* appointed the great mathematician Cauchy to review the paper. However, Cauchy, absorbed as always in his own researches, took his time reviewing it. In January 1830, Cauchy wrote to a colleague that he had been too ill to present to the *Academie* his report on Galois' paper as well as a paper of his own. A month later, Cauchy presented his own paper but not his report on Galois' paper. Instead, it appears as though Cauchy encouraged Galois to revise his paper and resubmit it for the *Academie*'s Grand Prize in Mathematics to the mathematician Fourier, the *Academie*'s perpetual secretary for mathematics and physics. Alas, Fourier died in April 1830 and there is no record of his having distributed Galois' paper to other members of the Prize committee.

Galois and France experienced a momentous year in 1830. King Charles X, who had ascended to the throne in 1824, was in many ways even more autocratic than the French kings of the eighteenth century who had preceded the revolution of 1789. On July 26, 1830, Charles and his ministers issued ordinances suspending freedom of the press and greatly curtailing the powers of the legislature. By the end of the day, the citizens of Paris rose in revolt. Three days later they had deposed Charles and replaced him with his cousin Louis-Philippe, the Duke of Orleans.

As revolutionary, anti-monarchist sentiments fomented in Paris during June and July, the Director of l'École Normale locked his students inside to prevent them from taking to the streets. Galois became so angry with this that he tried to escape from l'École by climbing over its walls. When he failed there was nothing left to do but take his examinations in calculus and physics. On July 22, Galois placed fourth out of nine students who took the calculus exam. Two and a half weeks later on August 9, he placed third out of eight students who took the physics examination. One can

only presume that Galois was rather distracted by the events going on outside the walls of l'École Normale.

With examinations finished and the July Revolution over, the director could no longer keep his students locked inside l'École. Galois quickly took advantage of the new atmosphere and joined the Society of Friends of the People, an extremist republican secret society that sought the abolishment of the monarchy altogether. His political activities soon got Galois into deep trouble with l'École, so deep that he quit l'École in early December before the Director's expulsion notice became effective.

On leaving l'École, Galois immediately joined the Artillery of the National Guard, a branch of the militia composed mostly of rabidly anti-monarchist republicans. On December 21, a Paris court was scheduled to pronounce sentence on four former ministers of Charles X who had been convicted of treason against the state. Radical republicans thought that the ministers deserved nothing less than the death sentence. The Artillery of the National Guard, including Galois, stationed themselves in front of the Louvre planning to start a revolt in case the court handed down a life sentence. Fearful of the mayhem that might ensue, the new King's ministers moved more regular troops near the Louvre. Both sides eyed each other suspiciously when a distant cannon shot indicated that life sentences had been pronounced. Fighting did not erupt even though tensions ran high. When the Marquis de Lafayette, hero of both the American and French Revolutions, called for peace, the crowd seemed to be placated. Nevertheless, fearing a threat to the throne, a royal decree abolished the Artillery of the National Guard on December 31.

Having dropped out of school, Galois decided to offer a weekly mathematics course of his own. The announcement in the *Gazette des écoles* stated that the course would cover mathematical topics that were new, some so new that they had never before been presented in public lectures. When the class met for the first time on January 13, 1831, in a bookshop near the Sorbonne, nearly forty students attended. Perhaps some of them wanted to see the fiery radical at the front of the class rather than at the back. In any case, the class only met a few times. Galois' political activities occupied him anew.

During the unrest of December 1830, nineteen officers of the Artillery of the National Guard had been arrested on a charge that they had conspired to give their cannons to the mob. Their imprisonment and trial consumed Galois. Following their acquittal in April 1831, Galois was one of the organizers of a celebration banquet to be held on May 9 at the restaurant of the *Vendanges des Bourgogne*. Alexandre Dumas, author of *The Count of Monte Cristo* and *The Three Musketeers* wrote in his diary, "It would be difficult to find in all of Paris two hundred persons more hostile to the government than those to be found reunited at five o'clock in the afternoon in the long hall on the ground floor above the garden."

During the banquet, Galois took out a pocket knife, raised a wine glass and made a toast that invoked the name of the new king, Louis-Philippe. Some people at the banquet thought they heard Galois make a threatening remark about the king. Others thought that someone else had made the remark while Galois was making his toast. The authorities chose to believe the worst of Galois and arrested him the next day while he was visiting his mother. He was jailed at Saint-Pélagie prison in Paris to await his trial.

The trial began on June 15. Galois' lawyer told the jury that Galois had said, "To Louis-Philippe, *if he betrays*," as he was wielding his knife and that many in the crowd had not heard him say "if he betrays" because of the noise. Galois became his own worst witness when the prosecutor interrogated him. When the prosecutor asked him if he really meant to kill the King, Galois responded, "Yes, if he betrays." He went on to predict that the King would, in fact, betray the people if he had not done so already. Fortunately for Galois, the judge charged the jury to decide what Galois had said and meant at the feverish banquet, not what he had said under oath in the more sedate courtroom. The jury may have been moved by Galois' tender years. They acquitted him after only a few minutes of deliberation.

Galois could not keep himself out of trouble. Many years later, celebrating Bastille Day would have been considered an ordinary act of French patriotism. In 1831, celebrating it by wearing the uniform of the outlawed Artillery Guard, as Galois and his republican friend Duchatelet chose to do, was an extremely seditious act. The two friends were imprisoned in Saint-Pélagie prison for their behavior.

The end of July marked the first anniversary of the July Revolution of 1830. To commemorate the fallen heroes, the Warden of Saint-Pélagie arranged for a Mass to be held in their memory. Not surprisingly, the atmosphere at the Mass was very tense. As the prisoners were being locked in their cells, cries of "Help, murder!" were heard. A shot rang out from the garret of a prison guard who lived across the street. One of the prisoners fell wounded. Enraged, Galois accused the Warden of having arranged the shooting. The Warden responded by throwing Galois into the dungeon.

Galois languished there for more than three months until he was formally charged and then sentenced to an additional six month in prison. While in prison, he learned that the *Academie* had rejected his latest manuscript. Its secretary, François Arago, wrote that the mathematician Poisson had reported

> *We have made every effort to understand Galois' proofs. His argument is neither sufficiently clear nor developed sufficiently to allow us to judge its rigor. It is not even possible for us to give an idea of his paper.*

> *The author claims that the manuscript contains propositions that are part of a general theory having rich applications. Quite often different parts of a theory clarify each other and can be understood more easily when taken together than when taken in isolation. We would prefer to wait for the author to publish a more complete account of his work before forming a more definite opinion.*

Reading this crushed Galois. He decided to publish the papers himself with the help of his friend Auguste Chevalier. Two of them are presented here. Here is a brief description of the mathematics they cover.

A ***polynomial equation*** has the form

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x^1 + a_n = 0$$

The value n is called the *degree* of the polynomial. The simplest polynomial equation is the linear equation

$$ax + b = 0$$

a *first* degree polynomial equation, which obviously has

$$x = -b/a$$

as its solution.

As Europe slumbered through its Dark Ages, Indian and then Arabic mathematicians, began to study ***quadratic equations***, that is equations of the form

$$ax^2 + bx + c = 0$$

a *second* degree polynomial equation. About the year 900, the Indian mathematician Sridhara (c.870–930), generalizing solutions found in Diophantus' *Arithmetica,* found that when such an equation has a solution, it will have

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a}$$

as a solution. Although Sridhara does not present his result in this format, his algebraic methods are nearly identical to the ones in the proof in contemporary algebra textbooks. For Sridhara, the quantity $(b^2 - 4ac)$ had to be non-negative in order for the quadratic equation to have a solution. Imaginary and complex numbers have been introduced into mathematics in the millennium since Sridhara's time and we now recognize that a quadratic equation always has two solutions

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{and} \quad \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

regardless of the value of $(b^2 - 4ac)$. (When $(b^2 - 4ac) = 0$ the two solutions are said to be redundant.)

As the Renaissance bloomed in the sixteenth century, European mathematicians began to attack the problem of finding solutions to higher degree polynomial equations.

In 1545, the Italian mathematician Girolamo Cardano (1501–1576) published a general solution for the *cubic equation*

$$x^3 + ax^2 + bx + c = 0$$

(i.e. a polynomial equation of the *third* degree) in his book *Ars Magna* (*The Great Art*). The general solution for this equation is

$$\sqrt[3]{\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

where

$$p = b - \frac{a^2}{3} \quad \text{and} \quad q = c + \frac{2a^3 - 9ab}{27}.$$

The *Ars Magna* also contains the general solution to the *quartic equation* (i.e. a polynomial equation of the *fourth* degree)

$$Ax^4 + Bx^3 + Cx^2 + Dx + E = 0$$

that had been discovered by Cardano's student Ludovico Ferrari (1522–1565). Ferrari's general solution has the form

$$-\frac{B}{4A} + \frac{\pm_s W \pm_t \sqrt{-(3\alpha + 2y \pm_s \frac{2\beta}{W})}}{2}.$$

This formula is complicated enough. I will spare you the more than one page it would take to express W, β, β, and y.

Given the fact that Cardano and Ferrari were teacher and student it is not surprising that their proofs each begin by substituting for x the expression

$$t - (b/na)$$

where

n is the degree of the polynomial (i.e. 3 or 4)

a is the coefficient of term in the n^{th} degree

b is the coefficient of the term in the $n - 1^{st}$ degree

(This method can also be applied to derive the general solution of the quadratic equation.)

For the next 250 years, mathematicians tried this method and other methods to find a solution for the *quintic* (i.e. *fifth* degree) and higher degree polynomials *by means of radicals*, i.e. by an expression involving just a finite number of terms and the operations of addition, subtraction, multiplication, division, exponentiation, and roots (i.e. *radicals*).

In 1821, the young Norwegian mathematician Niels Henrik Abel (1802–1829) believed that he had found the long-sought solution to the general quintic by means of radicals. Although Abel soon found a fatal flaw in his proof, his work was not in

vain. By 1824, Abel was able to prove that there is no solution to general quintic by means of radicals.

And then Evariste Galois attacked the problem of the quintic while still in his teens. At first, Galois, like Abel, believed that he had found a solution to the quintic. Like Abel, he soon recognized that he had made a mistake, perhaps by reading Abel's 1824 paper. Rather than move on to the problem of finding a solution for sixth degree polynomial equations, Galois stepped back from the immediate problem of finding a solution for the quintic or any particular class of polynomial equations and asked a much deeper question.

> *Supposing a class of polynomial equations has a general solution by means of radicals, what properties must that general solution have?*

Once again, we see a mathematician *supposing* a solution exists in order to find that solution or else prove that no such solution can exist.

Galois noticed that the roots of a polynomial themselves satisfy a variety of equations. Consider $(23 + \sqrt{3})$ and $(23 - \sqrt{3})$, the two roots of the quadratic equation

$$x^2 - 46x + 526$$

These two roots satisfy the following equations

$$A + B = 46$$
$$A^*B = 526$$
$$A^2 + B^2 = 1064$$

for example. Galois further noticed that *any* algebraic equations satisfied by the roots of the polynomial in question will satisfy the algebraic equations *regardless* of the order in which the roots are substituted. In the equations shown above it doesn't matter whether

$$A = (23 + \sqrt{3}) \text{ and } B = (23 - \sqrt{3})$$

or

$$A = (23 - \sqrt{3}) \text{ and } B = (23 + \sqrt{3}).$$

The key element of Galois' insight is considering the rearrangements, more properly called the *permutations*, of the roots having the property that *any* algebraic equation satisfied by the roots *remains* satisfied after the roots have been permuted.

Of course, that raised the question of when the permutation of the roots would have the property just described. In order to answer that question, Galois developed the branch of mathematics known as *Group Theory*. At first, he focused on *permutation groups*. Consider the ordered set of four elements $<a,b,c,d>$. Now rearrange it, say to $<b,d,c,a>$. The action that maps $<a,b,c,d>$ to $<b,d,c,a>$

is one of the permutations belonging to the group of permutations on ordered sets of four elements. In modern parlance this particular permutation is written as (1,4,2)(3) since it takes the 1st element to the 4th element, the 4th element to the 2nd, the 2nd to the 1st, and leaves the 3rd in place. The permutation that returns these four elements to their original order is (2,4,1)(3). It is called the *inverse* of (1,4,2)(3). Notice that it does not matter which of (1,4,2)(3) and (2,4,1)(3) is performed first and which second.

Now consider the permutation (1,3,2,4). Applying (1,4,2)(3) *first* and then *(1,3,2,4) second* to the ordered set $<a,b,c,d>$ results in $<b,c,a,d>$. In contrast, applying (1,3,2,4) *first* and (1,4,2)(3) *second* to the ordered set $<a,b,c,d>$ results in $<b,c,a,d>$, a different outcome! In this case order matters.

Galois embedded his study of permutation groups in the broader context of group theory. A group G is specified by a set of elements $\{g\}$ and a group operation, usually denoted by the symbol $^\circ$ that satisfies the following properties

- if g and h are elements of G, then $g^\circ h$ is also an element of G
- if f, g, and h are elements of G, then $(f^\circ g)^\circ h = f^\circ g(^\circ h)$ (this is called the property of association)
- there exists e an element belonging to G, such that for all g that are elements of G, $e^\circ g = g$ (e is called the *identity* element)
- for every element g belonging to G, there is an element h such that $g^\circ h = e$ (h is called the inverse of g and is usually denoted g^{-1})

The group of permutations n elements is now denoted as S_n.

A subgroup N of G is (1) a subset of elements of G (2) whose elements also satisfy the three properties just listed. A subgroup N or a group G is said to be a *normal* if for every element n of N and g of G

$$g^\circ n^\circ g^{-1}$$

is also and element of N.

To be brief, Galois demonstrated that the general polynomial equation of degree n could be solved by radicals if and only every subgroup N of the group of permutations S_n is a normal subgroup. Then he demonstrated that every subgroup of S_n is normal for all $n \leq 4$ but not for any $n > 5$. This demonstrated the impossibility of a finding a solution in radicals for all general polynomial equations of degree greater than 4.

Galois did not live to see his papers published. He remained at Saint-Pélagie prison without further incident until mid-March 1832, when a cholera epidemic forced the authorities to close Saint-Pélagie. Galois was among those transferred to the pension at Sieur Faultrier where he remained until his release on April 29.

Galois died on the morning of May 30 as a result of a duel with a man named Pescheux d'Herbinville. Little remains of the last month of Galois' life aside from letters he wrote the night before the duel. To one republican friend he wrote

> *I die the victim of an infamous coquette and her two dupes. It is in a miserable piece of slander that I end my life.*

To another he wrote "I have been provoked by two patriots . . . It is impossible for me to refuse."

For many years, historians conjectured the reason for Galois' fatal duel. Possible reasons included a royalist plot, a government conspiracy, a female agent provocateur, or a prostitute. In the 1960s, an historian looked at the original copy of the letters Galois wrote and noticed that Galois had erased the name Stéphanie Dumotel from one of them. Further investigation revealed that Stéphanie-Félicie Poterin du Motel was the daughter of the doctor who had treated Galois at Sieur Faultrier. Pescheux d'Herbinville was one of the nineteen republicans who had been acquitted of conspiring to give cannons to the mob. Finally, there was conclusive evidence that Galois had died for love!

The night before he died, Galois also wrote a final letter to his friend Chevalier, printed here, in which he gave an overview of his works. Galois asked his friend to publish it in the *Revue encyclopédique*, which Chevalier did. In the letter Galois wrote, "Ask Jacobi or Gauss to give their opinion, not as to the truth, but as to the importance of the theorems." Neither of the two mathematicians seems to have taken notice.

A decade later, the French mathematician Joseph Liouville did take notice. In 1843, Liouville announced to the *Academie* that he had found in Galois' work a solution "as correct as it was deep of a lovely problem. Given an irreducible equation of prime degree, to determine whether or not it is solvable in radicals." In 1846, Liouville published Galois' complete works in the *Journal de Mathématiques Pures et Appliquées* which he edited.

Galois died in obscurity, with hardly anyone having read or understood his work. He is now recognized by the greatest accolade that mathematics can bestow. A branch of mathematics is named for him: Galois theory!

Memoire on the Conditions for the Solvability of Equations by Radicals[1]

The Memoir[2] given here is taken from a work that I had the privilege of presenting to the *Academy* one year ago. Because this work has not been included, and the propositions that it held are again doubtful, I ought to be content to give the general principles of the theory in a synthetic form, and give *only one* application of my theory. I implore my judges to read at least these few pages with care.

Here we will find a general *condition* which is *satisfied by every equation that is solvable* [soluble] *by radicals*, and that, conversely, assures their solvability [*resolubilite*]. We apply the condition only to equations the degree of which is a prime number. Here is the theorem given by our analysis:

> *For an equation of a prime degree that does not have commensurable divisors to be solvable by radicals, it is necessary and sufficient that all the roots be rational functions of any two of the roots.*

The other applications of the theory are themselves particulars theories in their own right. Moreover, they need to use number theory and a particular algorithm: let us save them for another occasion. In part, they have a relationship to the modular equations of the theory of elliptical functions which we will demonstrate are not able to be resolved [*resoudre*] by radicals.

January 16, 1831

E. GALOIS

PRINCIPLES

I will begin by establishing some definitions and a series of lemmas which are already well known.

Definitions. An equation is said to be reducible when it admits of rational divisors; irreducible in the opposite case.

[1]Translated by John Anders. The translator's understanding of this memoir was greatly enhanced by Edwards' book *Galois Theory* (Springer-Verlag: New York, 1984). Though his translation of this memoir was consulted, in many places this translation differs from his translation in non-trivial ways.

[2]I considered it appropriate to put the following preface at the head of this memoir, even though I found it crossed-out in the manuscript. [Antoine Chevalier, hereafter A. CH.]

It is necessary to explain here what we intend to mean by the word *rational*, for it will be used often.

When *all* the coefficients of an equation are both numerical and rational, when we say this equation can be rationally divided here we simply want to say that the equation can be broken down into factors that have numerical and rational coefficients.

But when not *all* the coefficients of an equation are numerical and rational, then when we say this equation can be rationally divided by a rational divisor we must mean a divisor the coefficients of which are expressed in a rational function with coefficients of the given equation; and in general by a rational quantity, we mean a quantity that is expressed as a rational function of the coefficients of the given equation.

There is more: it could be appropriate to regard as rational every rational function of a certain number of determinate quantities, supposing that these quantities are given beforehand. For example, we could choose a certain root of a whole number and regard as rational every rational function of this radical.

When we come to regard certain quantities as known in this way, we will say that we *adjoin* them to an equation that we want to resolve [*resoudre*]. We will say that these quantities are *adjoined* to the equation.

Having laid this down, we will call *rational* every quantity that is expressed in a rational function of the coefficients of the given equation and of a certain number of quantities that have already been *adjoined* to the equation and have been agreed-upon arbitrarily.

When we help ourselves to auxiliary equations, they will be rational if their coefficients are rational in our sense.

Additionally, we can see that the properties and the difficulties of an equation can be made completely different depending on the quantities which are adjoined to it. For example, the adjunction of a quantity can render an irreducible equation reducible.

Thus when we adjoin a root of one of Gauss' auxiliary equations to the equation $\frac{x^n - 1}{x - 1} = 0$, where n is a prime number this equation breaks down into factors and, consequently, becomes reducible.

Substitutions are the transition from one permutation to another.

The permutation from which we depart in order to indicate the substitutions is totally arbitrary, when it comes to functions; for there is no reason why, in a function of many letters, one letter should occupy one position rather than another.

Nevertheless as we can hardly form for ourselves the idea of a substitution without forming for ourselves that of a permutation, we will frequently talk about

permutations, and we will consider substitutions only as the passage from one permutation to another.

When we come to group the substitutions, we will make them all come from the same permutation.

As it always comes down to questions where the original arrangement of the letters does not influence anything at all, in the groups that we will consider we ought to have the same substitutions, whatever the permutation from which we departed may be. Therefore, if in a group of this sort [*pareil group*] we have the substitutions S and T, we can be confident of having the substitution ST.

These are the definitions that we thought should be recalled.

Lemma I. An irreducible equation cannot have a root in common with a rational equation without dividing it.

For [if an irreducible equation has a root in common with a rational equation] the greatest common divisor of the irreducible equation and the other rational equation will still be rational; therefore, etc.

Lemma II. Given any equation whose roots are $a, b, c, \ldots$, where none of the roots are equal to each other we can always form a function V of these roots, such that none of the values that we obtain in permuting the roots in this function in any way are equal.

For example, one can set

$$V = Aa + Bb + Cc + \cdots,$$

A, B, C being appropriately chosen whole numbers.

Lemma III. The function V being chosen as indicated in the previous lemma, it will enjoy the property that each of the roots of the given equation can be expressed rationally in a function of V.

Indeed, let

$$V = \varphi(a, b, c, d, \ldots),$$

or

$$V - \varphi(a, b, c, d, \ldots) = 0$$

Let us multiply with each other all the equations of this sort [*equations semblables*] that we obtain by permuting all the letters, the first letter alone remaining fixed; we will then have the following expression:

$$\big[V - \varphi(a, b, c, d, \ldots)\big]\big[V - \varphi(a, b, c, d, \ldots)\big]\big[V - \varphi(a, b, d, c, \ldots)\big]\cdots,$$

which is symmetric in $b, c, d, \ldots$, and which, consequently, can be written as a function of a. Thus we will have an equation of the form

$$F(V, a) = 0.$$

But I say that we can pull out the value of a from this expression. To do this it is sufficient to find the common solution to this equation and the given equation

[i.e., the equation having roots *a, b, c, d, . . .* from which we constructed V]. This solution is the only common solution to the two equations, for we cannot have, for example,

$$F(V, b) = 0.$$

where this equation has a factor in common with the other equation of this sort [*equation semblables*], unless one of the functions $\varphi(a, \dots)$ were equal to one of the functions $\varphi(b, \dots)$; but this is contrary to the hypothesis [in Lemma II].

It follows from this that a is expressed in a rational function of V, and it is the same for the other roots.

This proposition[3] is cited without demonstration by Abel in his posthumous memoir concerning elliptical functions.

Lemma IV. Let us suppose that we have formed the equation in V [viz., F(V,a)], and that we have taken one of its irreducible factors such that V is a root of an irreducible equation. Let $V, V', V'', \dots$ *be the roots of this irreducible equation. If* $a = f(V')$ *is one of the roots of the given equation,* $f(V')$ *itself will be a root of the given equation.*

Indeed, in multiplying together all the factors of the form $V - \varphi(a, b, c, \dots, d)$, [sic. $V - \varphi(a, b, c, \dots)$] where we have made every possible permutation of all the letters except one we will have a rational equation in V, which will necessarily be found to be divisible by the equation in question; thus V' ought to be obtained by exchanging the letters in the function V. Let $F(V, a) = 0$ be the equation that we obtain by permuting all the letters in V except the first letter. Thus we will have $F(V', b) = 0$, where b could be equal to a, but must be one of the roots of the given equation; consequently, just as it results from the given equation and $F(V, a) = 0$ that $a = f(V)$, so also when the given equation and $F(V', b) = 0$ are combined, it follows that $b = f(V')$.

PROPOSITION I.

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

(1) every function of roots which is invariant[4] *under the substitutions of this group, is known rationally;*

[3]It is remarkable that from this proposition we can conclude that every equation depends on some auxiliary equation such that all the roots of this new equation are rational functions of on another; for the auxiliary equation is in V in this case.

Let me add that this remark is merely a curiosity. Indeed, an equation that has this property is not, in general, easier to solve than another that does not have this property.

[4]Here we call a function invariant not only when the form is invariant under the substitutions of its roots for each other, but also when the numerical value of the function does not vary under these substitutions. For example, if $Fx = 0$ is an equation, Fx is a function of roots that does not vary under any permutation [sic. substitution]. When we say that a function is known rationally, we mean to say that [its] numerical value is expressible as a rational function with coefficients of the equation and of the adjoined quantities.

(2) conversely, every function of roots that is rationally determinable, is invariant under the substitutions of this group.

(In the case of algebraic equations, this group is nothing other than the collection of $1 \cdot 2 \cdot 3, \ldots, m$ possible permutations of the m letters, because, in this case the symmetric functions alone are determinable rationally.)

(In the case of the equation $\frac{x^n - 1}{x - 1} = 0$, if we let $a = r$, $b = r^g$, $c = r^{g^2}, \ldots,$ where g is a primitive root, the group of permutations will simply be these:

abcd . . . . . k

bcd . . . . . ka

cd . . . . . kab

. . . . . .

kabc . . . . . i; [sic. *j*]

in this particular case, the number of permutations is equal to the degree of the equation and the same thing will obtain in the case of an equation all the roots of which are rational functions of one another.)

Demonstration: Whatever the given equation is, we will be able to find a rational function V of its roots, such that all the roots are rational functions of V. Given these equations, let us consider the irreducible equation of which V is a root (Lemmas III and IV). Let the roots of this equation be V, V', V'', $\ldots V^{(n-1)}$.

Let the roots of the proposed equation be φV, $\varphi_1 V$, $\varphi_2 V, \ldots, \varphi_{m-1} V$. Let us write the following n permutations of the roots:

$$\begin{array}{cccccc}
(V) & \varphi V & \varphi_1 V & \varphi_2 V & , \ldots, & \varphi_{m-1} V \\
(V') & \varphi V' & \varphi_1 V' & \varphi_2 V' & , \ldots, & \varphi_{m-1} V' \\
(V'') & \varphi V'' & \varphi_1 V'' & \varphi_2 V'' & , \ldots, & \varphi_{m-1} V'' \\
..... & ..... & ..... & ..... & ..... & ..... \\
(V^{(n-1)}) & \varphi V^{(n-1)} & \varphi_1 V^{(n-1)} & \varphi_2 V^{(n-1)} & , \ldots, & \varphi_{(m-1)} V^{(n-1)}
\end{array}$$

and I say that this group of permutations enjoys the mentioned property.

(1) Every function F of roots which is invariant under the substitutions of this group, can be written thus: $F = \psi V$, and we will have

$$\psi V = \psi V' = \psi V'' = \cdots = \psi V^{(n-1)}.$$

Thus the value of F can be determined rationally.

(2) Conversely, if a function F is rationally determinable and we set $F = \psi V$, we must have

$$\psi V = \psi V' = \psi V'' = \cdots = \psi V^{(n-1)},$$

because the equation in V does not have a commensurable divisor and since V satisfies the equation $F = \psi V$, F being a rational quantity. Thus the function F will necessarily be invariant under the substitutions of the group written down above.

Thus, this group enjoys the double property with which the given theorem is concerned. The theorem is thus demonstrated.

We will call the group in question the group of the equation.

Scolium 1. It is evident that in the group of permutations with which we are here concerned, the arrangement of letters should not at all be regarded, but only the substitutions of the letters under which we pass from one permutation to another.

Thus we can arbitrarily give ourselves a first permutation, provided that the other permutations are always derived by the same substitutions of letters. Thus the new group formed in this way will obviously enjoy the same properties as the first group, because in the preceding theorem, we were concerned only with the substitutions that we can make in the functions.

Scolium 2. The substitutions are independent even of the numbers of roots.

PROPOSITION II.

Theorem[5]*. If we adjoin the root, r, of an irreducible auxiliary equation [of prime degree p] to a given equation*

(1) one of two things will come to pass: either the group of the equation will not change or it will be partitioned into p groups each belonging to the given equation respectively when we adjoin each of the roots of the auxiliary equation to it;

(2) [if the group is partitioned, then] these [p] groups will enjoy the remarkable property that we will pass from the one to the other by putting-to-work the same substitution of the letters in all the permutations of the first group.

(1) If, after the adjunction of r, the equation in V (which is talked about above) [viz. $F(V,a)$] remains irreducible, it is clear that the group of the equation will not be changed. If, on the contrary, the equation in V is reduced, then the equation in V will be broken down into p factors, all of the same degree and of the form

$$f(V, r) \times f(V, r') \times f(V, r'') \times \cdots,$$

r, r', r'', being the other values of r. Thus the group of the given equation will also be broken down into groups each with the same number of permutations, because one permutation corresponds to each value of V. These groups will be those of the given equation, respectively, when we successively adjoin to it r, r', r'', …

[5]In the statement of the theorem, after the words "the root of an irreducible auxiliary equation, r''", Galois had initially put there "of prime degree p" which he later erased. So that in the demonstration in place of "r, r', r'', . . . being the other values of r", the first redaction carried, "r, r', r'', . . . being the different values of r." Finally we find the following note of the author in the margin:

"There is still something left to complete in this demonstration. I do not have time."

This line was thrown on the paper with great haste; a circumstance, together with the words, "I do not have time", makes me think that Galois had reread the Memoir in order to correct it before returning to the earth [*aller sur le terrain*]. [A.Ch.]

(2) We have seen above that all the values of V are rational functions of each other. Following this let us suppose that while V is a root of $f(V, r) = 0$, $F(V)$ is another root of $f(V, r) = 0$; it is clear that likewise if V' were a root of $f(V, r') = 0$, $F(V')$ will be another root of $f(V, r') = 0$; for we will have

$$f\big[F(V'), r\big] = \textit{a function divisible by } f(V, r)$$

Thus (Lemma I) [sic. Lemma IV]

$$f\big[F(V'), r'\big] = \textit{a function divisiblee by } f(V', r')$$

Having laid this down, I say that we obtain the group relative to r' by putting-to-work the same substitution of letters throughout the group relative to r.

Indeed, if we have, for example,

$$\varphi_\mu F(V) = \varphi_\nu(V)$$

we then have (Lemma I) [sic. Lemma IV]

$$\varphi_\mu F(V') = \varphi_\nu(V').$$

Therefore, in order to pass from the permutation $\big[\mathrm{F(V)}\big]$ to the permutation $\big[F(V')\big]$, it is necessary to make the same substitution that we make in order to pass from the permutation (V) to the permutation (V').

Thus the theorem is demonstrated.

PROPOSITION III.

Theorem. If we adjoin all the roots of an auxiliary equation to a given equation, the groups in question in Theorem II will also enjoy this property viz., that the substitutions are the same in each group.

One will find the demonstration[6].

PROPOSITION IV.

Theorem. If to a given equation we adjoin the numerical value of a certain function of its roots, the group of the equation will be lowered in such a way as to have no permutations other than those permutations under which this function is invariant.

Indeed, following Proposition I, every known function must be invariant under the permutations of the group of the equation.

[6]In the manuscript, the annunciation of the theorem that we come to read here is found in the margin and in place of it we find another that Galois had previously written with his demonstration under the same heading. Here is the original text:

Proposition III

Theorem. If the equation in r is of the form $r^p = A$, and the p^{th} roots of unity find themselves with the name of precisely adjoined quantities, the p groups in question in Theorem II will also enjoy this property viz., that the substitutions of letters by which we pass from one permutation to another in each group would be the same for all the groups.

Indeed, in this case, it comes to the same thing to adjoin this or that value of r to the equation. Consequently, the properties must be the same after the adjunction of this or that value. Thus the group must be the same value with respect to the substitutions. Therefore, etc.

All of this is erased with care; the new annunciation carries the date 1832, and shows by the manner in which it was written that the author was extremely pressed, which confirms the assertion that I advanced in the preceding note. [A. CH.]

PROPOSITION V.

Problem [1]. In which case is an equation solvable [soluble] by simple radicals?

First I will observe that, in order to resolve [*resoudre*] an equation, it is necessary to lower [*abaisser*] its group successively up until it contains no more than one single permutation. For when an equation is solved [*resolue*], every function of its roots is known, even when it is invariant under no permutations whatsoever.

Having laid this down, let us search for which condition must be satisfied by the group of an equation in order that it would be able to be lowered in this way by the adjunction of radical quantities.

Let us follow the sequence of possible operations in this solution, considering the extraction of each root of a prime degree as a distinct operation.

Let us adjoin to the original equation the first radical extracted [*extrait*] in the solution. Two situations are possible: either, by the adjunction of this radical, the group of permutations of the equation will be diminished, or, the group will remain the same if this extraction of the root is only a simple preparation for the resolution of the equation.

There must always be a diminution of the group after only a certain *finite* number of extractions, unless the equation is not solvable [*soluble*].

If, having arrived at this point [i.e., an extraction which diminishes the size of the group], there should be many ways to diminish the group of the given equation by a simple extraction of a root, it will be necessary, for what we are going to say, to consider only one radical of the least highest possible degree among all the simple radicals which are such that the knowledge of each of them diminishes the group of the equation.

Thus let p be the prime number which represents this minimum degree in a situation where we diminish the group of the equation by an extraction of a root of degree p.

We can always suppose, at least with respect to the group of the equation, that a p^{th} root of unity, α, is to be found among the quantities previously adjoined to the equation. For, since this expression is obtained by the extractions of roots of degree less than p, its being-known will not alter the group of the equation at all.

Consequently, after Theorems II and III, the group of the equation must be decomposed into p groups enjoying this double property with respect to each other:

(1) that we pass from the one to the other by one single substitution

(2) that all of them contain the same substitutions.

I say, conversely, that if the group of the equation can be partitioned into p groups that enjoy this double property, we will be able to reduce the group of the equation to one of the partial groups [*groupes partiels*] by a simple extraction of the p^{th} root and by the adjunction of this p^{th} root.

Indeed, let us take a function of the roots which is invariant under all the substitutions of one of the partial groups [*group partiel*], and varies according to every other substitution. (For this it suffices to choose a symmetric function of the different values that are taken by a function which is invariant under no substitution by any permutation of one of the partial groups.)

Let θ be this function of the roots.

Let us put-to-work on the function θ one of the substitutions of the whole group [*group total*] that is not shared by the partial group [*group partiel*]. Let θ_1 be the result of this substitution. Let us put-to-work the same substitution on the function θ_1, and let θ_2 be the result, and so forth.

Because p is a prime number, this series will be able to stop only at term θ_{p-1}, after which we will have $\theta_p = \theta_1$, [sic. θ] $\theta_{p+1} = \theta_1$, and so forth.

Having put this down, it is clear that the function

$$(\theta + \alpha\theta_1 + \alpha^2\theta_2 + \cdots + \alpha^{p-1}\theta_{p-1})^p$$

will be invariant under all the permutations of the whole group [*group total*], and, consequently, will be actually known.

If we extract the p^{th} root of this function, and adjoin it to the given equation, then, by Proposition IV, the group of the equation will contain no substitutions other than those substitutions of the partial group [*group partiel*].

Thus, in order for the group of an equation to be able to be lowered by a simply extraction of a root, this very condition is necessary and sufficient.

Let us adjoin to the original equation the radical in question; now we will be able to reason about the new group as about the previous one, and it will be necessary that it itself be broken-down in the way we indicated just above, and so forth, up until a certain group that will contain no more than one single permutation.

Scolium. It is easy to observe this sequence in the already known resolution [*resolution*] of the general equation of the fourth degree. Indeed, these equations are resolved by means of an equation of the third degree, which itself requires the extraction of a square root for its resolution. In the natural series of ideas, it is necessary to begin with this square root. But, in adjoining this square root to the given equation of the fourth degree, the group of the equation, which contains twenty four total substitutions [sic. permutations], is broken-down into two groups each of which contain only twelve. Designating the roots by *a, b, c, d*, one of these two smaller groups is:

abcd,	*acdb*,	*adbc*,
badc,	*cabd*,	*dacb*,
cdab,	*dbac*,	*dcad*,
dcba,	*bdca*,	*cbda*.

Now this group can itself be partitioned into three groups, as is indicated in Theorems II and III. Thus, by the extraction of a single radical of the third degree, there simply remains the group

abcd,
badc,
cdab,
dcba;

this group is partitioned anew into two groups:

abcd, *cdab*,
badc *dcba*.

Thus, after a simple extraction of a square root, there will remain

abcd,
badc;

which will be resolved [*resoudre*] in the end by a simple extraction of a square root.

In this way we obtain either Descartes' solution or Euler's solution; for, although after the resolution of the auxiliary equation of third degree Euler extracts three square roots, we know that two are sufficient, because then the third can be deduced rationally.

We will now apply this condition to irreducible equations of prime degree.

Application to Irreducible Equations of Prime Degree

PROPOSITION VI.

Lemma. An irreducible equation of prime degree cannot become reducible by the adjunction of a radical the index of which is anything other than the very degree of the given irreducible equation.

For if r, r', r'', … are the different values of the radical and $Fx = 0$ is the given irreducible equation of prime degree, it is necessary for Fx to be partitioned into factors

$$f(x, r) \times f(x, r') \times \cdots,$$

each of the same degree, which is not possible unless $f(x,r)$ is an equation of a prime degree in x.

Thus an irreducible equation of prime degree cannot become reducible unless its group is reduced to a single permutation.

PROPOSITION VII.

Problem. What is the group of an irreducible equation of prime degree n if it is solvable by radicals?

After the preceding proposition we can say that the smallest possible group before the group which has only a single permutation, will contain n permutations. But a

group of permutations of a prime number, n, of letters, cannot be reduced by n permutations, unless each of these permutations can be deduced from another by a cyclic substitution of order n (See the memoir of M. Cauchy, *Journal de l'Ecole* Polytechnique *xvii*th volume.) Thus the penultimate group will be

$$\text{(G)}\qquad \begin{array}{cccccccc} x_0, & x_1, & x_2, & x_3, & ,\ldots, & x_{n-3}, & x_{n-2}, & x_{n-1}, \\ x_1, & x_2, & x_3, & x_4, & ,\ldots, & x_{n-2}, & x_{n-1}, & x_0, \\ x_2, & x_3, & \ldots & \ldots & ,\ldots, & x_{n-1}, & x_0, & x_1, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{n-1}, & x_0, & x_1, & \ldots & ,\ldots, & x_{n-4} & x_{n-3} & x_{n-2}, \end{array}$$

$x_0, x_1, x_2, \ldots, x_{n-1}$ being the roots of the given irreducible equation.

Now the group that will immediately precede this group in the order of being-broken-down must be composed of a certain number of groups having all the same substitutions as this group. But I observe that these substitutions can be expressed in this way: (In general, let us set $x_n = x_{n+1} = x_i, \ldots$. It is clear that each of the substitutions of a group (G) can be obtained by putting x_{k+c} in place of x_k, c being a constant.)

Let us consider one of the groups similar to the group (G). Following Theorem II, the similar group will be obtained by putting-to-work the same substitution everywhere in this group; for example, in putting $x_{f(k)}$ in the place of x_k everywhere in group (G), f being a certain function.

Because the substitutions of these new groups must be the same as those of group (G), we must have

$$f(k + c) = f(k) + C$$

C being independent of k.

Thus

$$f(k + 2c) = f(k) + 2C$$
$$\ldots$$
$$f(k + mc) = f(k) + mC.$$

If $c = 1$, $k = 0$, we will find

$$f(m) = am + b$$
$$f(k) = ak + b,$$

a and b being constants.

Thus the group that immediately precedes the group (G) must contain only substitutions such as

$$x_k, \quad x_{ak+b},$$

and will not contain, consequently, any cyclic substitution other than those of group (G).

We will reason about this group as about the previous one, and it will follow that the first group in the order of being-broken-down, that is to say, the *actual* group of the equation, can contain substitutions only of the form

$$x_k, \quad x_{ak+b}.$$

Thus

if an irreducible equation of prime degree is solvable by radicals, the group of this equation can contain only substitutions of the form

$$x_k, \quad x_{ak+b},$$

a and b being constants

Conversely, if this condition is in place, I say that the equation will be solvable by radicals. Indeed, let us consider the functions

$$\begin{aligned}
&(x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1})^n = X_1,\\
&(x_0 + \alpha x_a + \alpha^2 x_{2a} + \cdots + \alpha^{n-1} x_{(n-1)a})^n = X_a\\
&(x_0 + \alpha x_{a^2} + \alpha^2 x_{2a^2} + \cdots + \alpha^{n-1} x_{(n-1)a^2})^n = X_{a^2}\\
&\qquad\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}$$

α being an n^{th} root of unity, a a primitive root of n.

In this case it is clear that every function that is invariant under the cyclic substitutions of the quantities $X_1, X_a, X_{a^2}, \ldots$ will be immediately known. Thus we will be able to find $X_1, X_a, X_{a^2}, \ldots$ by Mr. Gauss's method for binomial equations. Therefore, etc.

Thus in order for an irreducible equation of prime degree to be solvable by radicals, it is necessary and sufficient that every function invariant under the substitutions

$$x_k, \quad x_{ak+b}.$$

be rationally known.

Thus the function

$$(X_1 - X)(X_a - X)(X_{a^2} - X)\ldots$$

must be known, whatever X is.

It is necessary and sufficient, therefore, that the equation which gives this function of roots admit a rational value whatever X is.

If the given equation has all rational coefficients, the auxiliary equation that gives this function will also have all rational coefficients, and it will be sufficient to recognize whether or not this auxiliary equation of degree $1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-2)$ has a rational root—and we know how to do that.

Here there is the means necessary for use in practice. But we will present the theorem again under another form.

PROPOSITION VIII.

Theorem. In order for an irreducible equation of prime degree to be solvable by radicals, it is necessary and sufficient that when any two of its roots are known, the others can be deduced rationally.

In the first place, it is necessary because, since the substitution

$$x_k, \quad x_{ak+b}.$$

does not allow any two letters to be put in the same place, it is clear by Proposition IV that in adjoining two roots to the equation its group must be reduced to only one permutation.

In the second place, this is sufficient; for, in this case, any other substitution of this group will not allow two letters to remain in the same place. Consequently, the group will contain at most $n(n-1)$ permutations. Thus it will contain only a single cyclic substitution (without which it would have at least n^2 permutations). Thus every substitution of the group, x_k, x_{fk}, must satisfy the condition

$$f(k+c) = fk + C$$

Therefore, etc.

The Theorem is thus demonstrated.

Example of Theorem VII

Let $n = 5$; the group will be the following:

abcde
bcdea
cdeab
deabc
eabcd

acebd
cebda
ebdac
bdace
daceb

aedcb
edccb
edcba
dcbae
cbaed
baedc
adbec
dbeca
becad
ecadb
cadbe

———.

Fragment of a Second Memoir
Concerning Primitive Equations that are Solvable by Radicals

Let us try to find out when a primitive equation is, in general, solvable by radicals. Now, we can quickly establish a general characteristic based on the very degree of these equations. This characteristic is this: in order for a primitive equation to be solvable [*resoluble*] by radicals, it is necessary that its degree be of the form, p^{ν}, p being prime. And from this is will immediately follow that, when we have to resolve [*resoudre*] by radicals an irreducible equation the degree of which could admit of unequal prime factors, we will be able to do so only by Mr. Gauss's method of decomposition; otherwise the equation will be unsolvable [*insoluble*].

In order to establish the general property that we will come to annunciate with respect to the primitive equations that we can resolve [*resoudre*] by radicals, we can suppose that the equation that we want to resolve [*resoudre*] is initially primitive, but ceases to be after the adjunction of a simple radical. In other words, we can suppose that, n being prime, the group of the given equation is partitioned into n conjugate, irreducible but not primitive groups. For, unless the degree of the equation is prime, a group of that sort [*un pareil group*] will always be presented in the series of decompositions.

Let N be the degree of the given equation, and let us suppose that after an extraction of a root of a prime degree n, the given equation becomes non primitive and is partitioned into Q primitive equations each of degree P, by means of a single equation of degree Q.

If we name the group of the given equation G, this group must be partitioned into n non primitive, conjugate groups, in which the letters that designate the roots will be arranged in systems composed of P letters each conjoined. Let us see how many ways this can be done.

Let H be one of the non primitive, conjugate groups. It is easy to see that, in this group, any two letters taken at will will form part of a certain system of P conjoined letters and will form part only of one single system.

For, in the first place, if there were two letters which were not able to form part of the same system of P conjugate letters, the group G, which is such that any one of these substitutions transforms all the substitutions of group H into each other, would be non primitive: which is contrary to the hypothesis.

In the second place, if two letters were to form part of many different systems, it would follow that the groups which answer to different systems of P conjoined letters would not be primitive: which is still contrary to the hypothesis.

Having laid this down, let

$$\begin{array}{ccccc} a_0, & a_1, & a_2, & \ldots, & a_{p-1} \\ b_0, & b_1, & b_2, & \ldots, & b_{p-1} \\ c_0, & c_1, & c_2, & \ldots, & c_{p-1} \end{array}$$

be the N letters: let us suppose that each horizontal line represents a system of conjoined letters. Let P conjoined letters

$$a_0, \quad a_{0.1}, \quad a_{0.2}, \quad \ldots, \quad a_{0.P-1},$$

be all situated in the first vertical column. (It is clear that we will be able to make it be such by switching the order of the horizontal lines.)

Likewise, let

$$a_{1\cdot 0}, \quad a_{1\cdot 1}, \quad a_{1\cdot 2}, \quad a_{1\cdot 3}, \ldots, \quad a_{1\cdot P-1}$$

be P conjoined letters all situated in the second vertical column such that

$$a_{1\cdot 0}, \quad a_{1\cdot 1}, \quad a_{1\cdot 2}, \quad a_{0\cdot 3}, \ldots, \quad a_{1\cdot P-1}$$

respectively, belong to the same horizontal lines as

$$a_{0\cdot 0}, \quad a_{0\cdot 1}, \quad a_{0\cdot 2}, \quad a_{0\cdot 3}, \ldots, \quad a_{0\cdot P-1};$$

likewise, if we let the systems of conjoined letters be

$$\begin{array}{ccccc} a_{2\cdot 0}, & a_{2\cdot 1}, & a_{2\cdot 2}, & a_{2\cdot 3}, \ldots, & a_{2\cdot p-1} \\ a_{3\cdot 0}, & a_{3\cdot 1}, & a_{3\cdot 2}, & \ldots, & a_{3\cdot p-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

in this way we will obtain, in the end, P^2 letters. If the total number of letters is not exhausted, we will take a third index such that

$$a_{m\cdot n\cdot 0}, \quad a_{m\cdot n\cdot 1}, \quad a_{m\cdot n\cdot 2}, \quad a_{m\cdot n\cdot 3}, \ldots, \quad a_{m\cdot n\cdot P-1}$$

are, in general, a system of conjoined letters; and in this way we will reach the conclusion that $N = P^{\mu}$, μ being a certain number equal to that of the different indices about which we are concerned. The general form of the letters will be

$$a_{\underset{1}{k}\cdot\underset{2}{k}\cdot\underset{3}{k}\cdot\ldots\cdot\underset{\mu}{k}}$$

$\underset{1}{k}, \underset{2}{k}, \underset{3}{k}, \ldots, \underset{\mu}{k}$ being the indices which can take each of the P values 0, 1, 2, 3, . . ., P-1.

Through the way in which we have proceeded we can also see that, all the substitutions in the group H will be of the form

$$\left[a_{\underset{1}{k}\cdot\underset{2}{k}\cdot\underset{3}{k}\cdot\ldots\cdot\underset{\mu}{k}}, \quad a_{\underset{1}{\varphi}(k)\cdot\underset{2}{\psi}(k)\cdot\underset{3}{\chi}(k)\cdot\ldots\cdot\sigma(k)}\right],$$

because each index corresponds to a system of conjoined letters.

If P is not a prime number, we will reason about the group of permutations of any one of the systems of conjoined letters, as we reasoned about the group G, when we replaced each index by a certain number of new indices, and we will find $P = R^{\alpha}$, and so forth; whence, finally, $N = p^{\nu}$, p being a prime number.

Concerning Primitive Equations of Degree P^2

Let us stop a moment to discuss the series of primitive equations of degree p^2, p being an odd prime number. (The case of $p = 2$ has already been investigated.) If an equation of degree p^2 is solvable [*soluble*] by radicals, let us in the first place suppose it to be such that it becomes non primitive by an extraction of a radical.

Thus let G be a primitive group of p^2 letters which are partitioned into n non primitive groups conjugate to H.

The letters in the group H must necessarily be arranged in this way

$$\begin{array}{cccccc}
a_{0\cdot 0}, & a_{0\cdot 1} & a_{0\cdot 2} & a_{0\cdot 3} & ,\ldots, & a_{0\cdot p-1}, \\
a_{1\cdot 0}, & a_{1\cdot 1} & a_{1\cdot 2} & a_{1\cdot 3} & ,\ldots, & a_{1\cdot p-1} \\
a_{2\cdot 0}, & a_{2\cdot 1} & a_{2\cdot 2} & a_{2\cdot 3} & ,\ldots, & a_{2\cdot p-1} \\
\ldots & \ldots & \ldots & \ldots & ,\ldots, & \ldots \\
a_{p-1\cdot 0}, & a_{p-1\cdot 1}, & a_{p-1\cdot 2}, & a_{p-1\cdot 3} & ,\ldots, & a_{p-1\cdot p-1}
\end{array}$$

each horizontal and each vertical line being a system of conjoined letters.

If we permute the horizontal lines among themselves, the group that we will obtain, being primitive and of prime degree, must contain only substitutions of the form

$$\left(a_{k\cdot k}, a_{mk+n\cdot k}\right),$$
$$_1\quad _2 \qquad\quad _1 \qquad _2$$

the indices being taken relative to the modulus p.

It will be the same for the vertical lines which will be able to yield only substitutions of the form

$$\left(a_{k\cdot k}, a_{k\cdot qk+r}\right)$$
$$_1\quad _2 \qquad _1 \quad _2$$

Therefore, finally, all the substitutions of group H will be of the form

$$\left(a_{k\cdot k}, a_{mk+n\cdot mk\cdot q}\right).$$
$$_1\quad _2 \qquad _1 \quad _2 \qquad _2$$

If a group G is partitioned into n groups conjugate to those that we have just described, all the substitutions of the group G must transform into one another the cyclic substitutions of the group H which are concisely written as follows:

$$(a) \qquad \left(a_{k\cdot k},\ldots, a_{k+\alpha\cdot k+\alpha},\ldots\right)$$
$$_1\quad _2 \qquad _1 \quad _1 \quad _2 \quad _2$$

Therefore let us suppose that one of the substitutions of group G is formed by respectively replacing

$$\begin{array}{c} k \\ _1 \\ k \\ _2 \end{array} \text{ by } \begin{array}{l} \varphi_1(k, k) \\ \varphi_2(k, k) \end{array}$$
$$\qquad\qquad\quad _1\ _2 \qquad\quad _1\ _2$$

If, in the functions φ_1, φ_2, we substitute the values $k + \alpha, k + \alpha$ for k and k, there must come as a result something of the form
$$_1 \quad _1 \ _2 \quad _2 \qquad _1 \qquad _2$$

$$\varphi_1 + \zeta_1, \quad \varphi_2 + \zeta_2,$$

and from this it is easy to conclude immediately that the substitutions of the group G must all be contained in the following expression [*formule*]

(A) $$\left(a_{k\cdot k}, a_{mk+nk+\alpha\cdot mk+nk+\alpha}\right).$$

But we know by (n)[7], that the substitutions of group G can contain only p^2-1 or p^2-p letters.

But let us recall that it is merely for the demonstration given here that we have assumed that the primitive group G is partitioned into non primitive conjugate groups. As this condition is not at all necessary, in general the groups will be much more complicated.

Thus it is pertinent to recall when these groups will admit of substitutions where only p^2-p letters vary, and this investigation will occupy us for some time.

Thus let G be a group which contains some substitution of the order p^2-p; I say in the first place that all the substitutions of this group will be linear, that is to say of the form (A).

This is recognized to be true for substitutions of the order p^2-1; therefore it is sufficient to demonstrate it for those substitutions of the order p^2-p. Therefore let us consider a group where all m of the substitutions are only of the order p^2 or of the order p^2-p. (See the place cited.)

Then the p letters which do not vary in a substitution of the order p^2-p must be conjoined letters.

Let us suppose that these conjoined letters are

$$a_{0\cdot 0},\quad a_{0\cdot 1},\quad a_{0\cdot 2},\quad ,\ldots,\quad a_{0\cdot p-1}$$

We can deduce all the substitutions where these p letters do not change place, [and] we can deduce the substitutions of the form

$$\left(a_{k\cdot k}, a_{k\cdot \varphi k}\right),$$

and we can deduce the substitutions of the order p^2-p, the period of which is p terms. (See again the place cited.)

Because the group of the primes enjoys the requisite property the primes must necessarily be reduced to the form

$$\left(a_{k\cdot k}, a_{k\cdot mk}\right),$$

according to what we have seen for equations of degree p.

With respect to cyclic substitutions the period of which is p terms, as they are conjugate to the preceding terms, we can assume a group which contains them without

[7]Since this memoir forms a sequel to a work of Galois that I do not have, it is impossible for me to indicate the memoir cited here and below. [A. Ch.]

containing these very ones: thus they must transform the cyclic substitutions (*a*) into one another; thus they will also be linear.

Thus we have arrived at this conclusion, that the primitive group [*primitive groupe*] of permutations of p^2 letters must contain only substitutions of the form (*A*).

Now, let us take the whole group [*groupe total*] that we obtain in applying all possible linear substitutions to the expression [*expression*]

$$a_{k_1 \cdot k_2},$$

and let us try to find out what the divisors of this group are that can enjoy the property requisite for the resolvability [*resolubilite*] of equations.

First, what is the total number of linear substitutions? Initially, it is clear that every transformation of the form

$$k_1 \cdot k_2, \quad mk_{11} + nk_{12} + \alpha \cdot mk_{21} + nk_{22} + \alpha_2$$

will not be a substitution for this; for it is necessary in a substitution that to each letter of the first permutation the substitution gives-back only a single letter of the second, and conversely.

Therefore if we take any letter $a_{l_1 \cdot l_2}$ of the second permutation, and if we restore [*remonte*] it to the letter corresponding to it in the first permutation, we must find a letter $a_{k_1 \cdot k_2}$ where the indices $k_1 \cdot k_2$ are completely determinated. Therefore it is necessary that, whatever l_1 and l_2 are, we have finite and determinate values of k_1 and k_2 by the two equations

$$m_1 \cdot k_1 + n_1 \cdot k_2 + \alpha_1 = l_1, \; m_2 \cdot k_1 + n_2 \cdot k_2 + \alpha_2 = l_1 .$$

Thus the condition for a transformation of this sort [*pareille transformation*] to be a real substitution, is that $m_1 \cdot n_2 - m_2 \cdot n_1$ are neither zero nor divisible by the modulus *p*, which is the same thing.

Now I say that unless this group of linear substitutions does not always belong [*appartienne*], as we will see, to the equations which are solvable by radicals, it will always enjoy this property that if in any one of its substitutions there are *n* letters which are fixed, then *n* will divide the number of the letters. And, in fact, whatever the number of letters is which remains fixed, we will be able to express this circumstance by linear equations which give all the indices of one of the fixed letters, by means of a certain number of those among them. Giving *p* values to each of these indices as they remain arbitrary, we will have p^m systems of values, *m* being a certain number. In the case with which we are concerned, *m* is necessarily < 2, and, consequently, is found to be between 0 and 1. Therefore the number of substitutions is known to be no greater than

$$p^2 (p - 1) (p^2 - p).$$

Now let us consider only the linear substitutions where the letter $a_{0.0}$ does not vary; if, in this case, we find the total number of permutations of a group which contains all the possible linear substitutions, it will be sufficient to multiply this number by p^2.

But, firstly, when we substitute p for the index k_2, all the substitutions of the form

$$\left(a_{\underset{1}{k}\cdot\underset{2}{k}},\ a_{\underset{1}{m}\underset{1}{k}\cdot\underset{2}{k}}\right)$$

will give $p-1$ substitutions in all. We will have p^2-p when we join the term $\underset{2}{mk}$ to the term k_2, so that it follows that:

(m') $$(\underset{1}{k}\cdot\underset{2}{k},\ \underset{1}{m}\underset{2}{k}\cdot\underset{2}{m}\underset{1}{k}+\underset{2}{k}).$$

On the other hand, it is easy to find a linear group of p^2-1 permutations, such that in each of these substations all the letters, with the exception of $a_{0.0}$, vary. For, when we replace the double index $\underset{1}{k}\cdot\underset{2}{k}$ by the simple index $\underset{1}{k}+i\underset{2}{k}$, i being a primitive root of

$$x^{p^2-1}-1=0 \text{ (mod. } p),$$

it is clear that every substitution of the form

$$\left[a_{\underset{1}{k}+\underset{2}{ki}},\ a_{(\underset{1}{m}+\underset{2}{mi})(\underset{1}{k}+\underset{2}{ki})}\right]$$

will be a linear substitution; but, in these substitutions no letter remains in the same place, and they are of the number of p^2-1.

Therefore we have a system of p^2-1 permutations such that in each of these substitutions all the letters change with the exception of $a_{0.0}$. Combining these substitutions with the p^2-p substitutions which are spoken of above, we will have $(p^2-1)(p^2-1)$ substitutions.

But we have seen beforehand that the number of substitutions where $a_{0.0}$ remains fixed cannot be greater than $(p^2-1)(p^2-1)$. Therefore it is precisely equal to $(p^2-1)(p^2-p)$, and the whole linear group would have in total $p(p^2-1)(p^2-1)$ permutations.

It remains to search out the divisors of this group, which can enjoy the property of being solvable by radicals. For this we will have to make a transformation which has for its goal to lower as much as possible the general equation of degree p^2, the group of which is linear.

Firstly, as the cyclic substitutions of a group of this sort [*pareil groupe*] are such that every other substitution of the group transforms them into one another, we will be able to lower the equation by one degree and to consider an equation of degree p^2-1, the group of which will have only substitutions of the form

$$\left(b_{\underset{1}{k}\cdot\underset{2}{k}},\ b_{\underset{1}{m}\underset{1}{k}+\underset{1}{m}\underset{2}{k}\cdot\underset{2}{m}\underset{1}{k}+\underset{2}{n}\underset{2}{k}}\right),$$

the $p^2 - 1$ letters being

$$\begin{array}{ccccc} & b_{0\cdot1}, & b_{0\cdot2}, & b_{0\cdot3}, & ,\ldots, \\ b_{1\cdot0}, & b_{1\cdot1}, & b_{1\cdot2}, & b_{1\cdot3}, & ,\ldots, \\ b_{2\cdot0}, & b_{2\cdot1}, & b_{2\cdot2}, & b_{2\cdot3}, & ,\ldots, \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

Now I observe that this group is not primitive such that all the letters are conjoined letters when the ratio of the two indices is the same. If we replace each system of conjoined letters by a single letter, we will have a group all the substitutions of which are of the form

$$\left(b_{\frac{k_1}{k_2}}, b_{\frac{m_1k_1+n_1k_2}{m_2k_1+n_2k_1}}\right),$$

$\frac{k_1}{k_2}$ being new indices. When we replace this ratio with a single index k, we see that the $p + 1$ letters will be

$$b_0, \quad b_1, \quad b_2, \quad b_3, \quad ,\ldots, \quad b_{p-1}, \quad b_{\frac{1}{0}}, \text{ [sic.]}$$

and the substitutions will be of the form

$$\left(k, \frac{mk + n}{rk + s}\right).$$

Let us try to find out how many letters remain in the same place in each of the substitutions; it is necessary for this to resolve [*resoudre*] the equation

$$(rk + s)k - m(mk + n) = 0,$$

which will have two, or one, or no roots, depending on whether $(m - s)^2 + 4nr$ is a quadratic residue, zero, or not a quadratic residue. For the third case, the substitution will be of the order $p - 1$, or p, or $p + 1$.

For the sort of case that involves two primes we can take substitutions of the form

$$(k, mk + n),$$

where the single letter $b_{\frac{1}{0}}$ [sic.] does not vary, and here we can see that the total number of substitutions of the group is reduced to

$$(p + 1)\, p(p - 1).$$

It is after we have reduced this group in this way that we will treat it more generally. We will first search-out in which case a divisor of this group which contains substitutions of the order p would be able to belong to an equation that is solvable [*soluble*] by radicals.

In this case, the equation will be primitive and it should not be solvable by radicals unless we do not have $p + c(?) = 2^n$ [*sic.*] n being a certain number.

We can suppose that the group contains only substitutions of the order p and the order $p + 1$. All the substitutions of the order $p + 1$ will, consequently, be of this sort, and their period will be two terms.

Therefore let us take the expression

$$\left(k, \frac{mk + n}{rk + s}\right),$$

and let us see in which case this substitution is able to have a period of two terms. It is necessary for this situation that the inverse substitution be joined-together-with it. The inverse substitution is

$$\left(k, \frac{-sk + n}{rk - s}\right).$$

Thus we should have $m = -s$, and all the substitutions in question will be

$$\left(k, \frac{mk + n}{k - m}\right)$$

or yet

$$k,\ m + \frac{N}{k - m},$$

N being a certain number which is the same for all the substitutions, because these substitutions must be transformed into one another the ones into the others by all the substitutions of the order p, $(k,\ k + m)$; but these substitutions must, moreover, be conjugate to one another. Therefore if

$$\left(k,\ m + \frac{N}{k - m}\right),\quad \left(k,\ n + \frac{N}{k - n}\right)$$

are two substitutions of this sort, it is necessary that we have

$$n + \frac{N}{\dfrac{N}{k - m} + m - n} = m + \frac{N}{\dfrac{N}{k - n} + n - m},$$

to know,

$$(m - n)^2 = 2N.$$

Therefore the difference between two values of m can acquire only two different values; therefore m can have no more than three values; therefore, in the end, $p = 3$. Thus it is only in this case that the reduced group can contain substitutions of the order p.

And, indeed, the reduced equation will then be of the fourth degree, and, consequently, solvable by radicals.

From this we know, in general, that substitutions of the order p must not be found among the substitutions of our reduced group. But could there be substitutions of the order $p - 1$? That is what I will investigate[8].

[8]I have searched in vain through Galois' papers for the continuation of this text. [A. Ch.]