Galois for 21st-Century Readers

Harold M. Edwards

The recent bilingual publication of *The Mathematical Writings of Évariste Galois* by Peter M. Neumann [6] will make Galois's own words available to a vast new audience of students of modern algebra. I have long advocated reading the original works of great mathematicians, but even with the advantage of Neumann's extensively annotated transcription and translation it will be difficult for modern readers to connect Galois theory as they know it with Galois's original presentation of it in his famous First Memoir (*Premier Mémoire*), entitled "On the conditions for the solvability of equations by radicals".

The First Memoir was submitted to the Paris Academy of Sciences in January of 1831, only to be rejected. With the benefit of hindsight, it is easy to condemn this rejection as an epic misjudgment. However, anyone who has studied the memoir will sympathize with the decision, especially in view of the fact that the referees recommended that the young author—Galois was just nineteen at the time—make his presentation clearer and more expansive. They could not have imagined that this would be their last chance to recognize the merit of the work of an unparalleled genius.

In this paper, I have tried to explain the First Memoir to modern readers, going through it proposition by proposition. The most important proposition, and the one I most emphasize, is Proposition 2, the one about which Galois wrote in the margin, "There is something to be completed in this proof. I do not have the time" (the sections "Proposition 2" and "Proposed Revision of Proposition 2" below). My interpretation suggests how Galois *might* have stated and proved it given a little more time. This revised Proposition 2, combined with Proposition 1 (which I also revise, but only to make the statement Galois surely intended), contains the equivalent of what is now called the fundamental theorem of Galois theory.

I do not assume that the reader has ready access to the First Memoir and have tried to make the explanations stand on their own, but serious readers would be foolish to be satisfied with my rewarmed version of Galois's theory. The original, however flawed and incomplete it may be, is indisputably one of the most valuable and insightful documents in the history of mathematics.

Harold M. Edwards is emeritus professor of mathematics at Courant Institute of Mathematical Sciences. His email address is edwards@cims.nyu.edu.

DOI: http://dx.doi.org/10.1090/noti869

The Ground Field

At the beginning of the First Memoir, Galois establishes what would be called the *ground field* today. He states that the polynomials (he calls them equations) to be solved may have coefficients that are not rational numbers, but that nonetheless the coefficients of the polynomial to be solved (or, as would be said today, the polynomial to be factored into linear polynomials) will be called rational quantities. Explicitly, he says, "We shall call *rational* every quantity which can be expressed as a rational function of the coefficients of the [polynomial] together with a certain number of quantities *adjoined* to the [polynomial] and agreed arbitrarily."

I will denote by K a field which is the field of rational numbers $\mathbf{Q}$ to which a finite number of irrational quantities, either algebraic or transcendental, are adjoined.[1] This field K, "agreed

[1] *At first, it is simplest to take the ground field K to be* $\mathbf{Q}$*, and this case exhibits all the features of the general case.*

arbitrarily", will be the field of quantities that are considered to be rationally known in Proposition 1. In the course of the solution of a given polynomial, other quantities will necessarily be adjoined.

Lemma 1

Galois's first lemma states that "An irreducible [polynomial] cannot have any root in common with a rational [polynomial] without dividing it." He essentially leaves the proof to the reader, saying only, "For the greatest common divisor of the irreducible [polynomial] and the other [polynomial] will again be rational; therefore, etc. [sic]."

The notion of a greatest common divisor of two polynomials which he cites here is of fundamental importance to the whole theory. Strictly speaking, one can't speak of *the* greatest common divisor of two polynomials in one variable with coefficients in K but only of *a* greatest common divisor, which is a polynomial that divides them both and which, among all such common divisors, has maximum degree. Given one greatest common divisor of two polynomials, the others are all obtained by multiplying by nonzero constants.

The construction of a greatest common divisor of two given polynomials with coefficients in K can be carried out in various ways. Galois gives no hint as to how he would find a greatest common divisor, but all methods come down to the following simple idea, often called the Euclidean algorithm for polynomials.

A common divisor of $f(x)$ and $g(x)$ is obviously a common divisor of $f(x)$ and $r(x)$ when $\deg f(x) \le \deg g(x)$ and $r(x)$ is the remainder when $g(x)$ is divided[2] by $f(x)$ to find polynomials $q(x)$ and $r(x)$, with $\deg r(x) < \deg f(x)$, for which $g(x) = q(x)f(x) + r(x)$, provided, of course, that $f(x) \neq 0$. Conversely, every common divisor of $f(x)$ and $r(x)$ is also a common divisor of $f(x)$ and $g(x)$. If $\deg f(x) > \deg g(x)$, a common divisor of $f(x)$ and $g(x)$ is a common divisor of $r(x)$ and $g(x)$ where $r(x)$ is the remainder when $f(x)$ is divided by $g(x)$, provided, again, that $g(x) \neq 0$. In this way, the common divisors of $f(x)$ and $g(x)$ are found to coincide with the common divisors of two polynomials whose total degree is less than the total degree $\deg f(x) + \deg g(x)$ of $f(x)$ and $g(x)$, provided neither $f(x)$ nor $g(x)$ is zero. When the degree of the zero polynomial is considered to be $-\infty$, this procedure allows one to reduce the problem of finding the common divisors of $f(x)$ and $g(x)$ to the same problem for a pair of polynomials whose total degree is reduced, unless that total degree is $-\infty$. Thus, since the total degree cannot be reduced more than $\deg f(x) + \deg g(x)$ times without reaching $-\infty$, the common divisors of $f(x)$ and $g(x)$ coincide with the common divisors of two polynomials constructed by iterating this algorithm, one of which is zero. Let $d(x)$ denote the one that is not zero. Then the common divisors of $f(x)$ and $g(x)$ coincide with the divisors of $d(x)$. In particular, $d(x)$ is a greatest common divisor of $f(x)$ and $g(x)$.

As for the proof of Galois's Lemma 1, note first that Galois is certainly including roots that are not in the ground field K, because a polynomial that is irreducible over K has no roots in K unless its degree is one, in which case the lemma is elementary. If there is an extension of K in which $f(x)$ and $g(x)$ have a common root, then there is an extension of K over which $f(x)$ and $g(x)$ have a common divisor of degree greater than zero. The algorithm for finding a greatest common divisor of $f(x)$ and $g(x)$ does not make any use of the extension of K, so in this case there must be a common divisor of $f(x)$ and $g(x)$ of degree greater than zero with coefficients in K. When $f(x)$ is irreducible, it follows that this common divisor is a nonzero multiple of $f(x)$ (the only divisors of $f(x)$ are nonzero constants and nonzero multiples of $f(x)$), so $f(x)$ divides $g(x)$, as was to be shown.

The Precious Galois Principle

As will be explained below, Galois's Lemmas 2 and 3 combine to prove that, for any given polynomial $f(x)$ with coefficients in K, there is an irreducible polynomial $G_0(X)$ with coefficients in K with the property that the field $K(V)$ obtained by adjoining one root V of $G_0(X)$ to K is a field over which both $f(x)$ and $G_0(X)$ can be written as products of linear factors. That is, *Lemmas 2 and 3 imply a construction of a normal extension of K which is a splitting field of $f(x)$.*

Galois's proof—or, rather, the proof indicated by Galois, because an indication is all he gives—presents a somewhat circular argument, insofar as he tacitly assumes that there is such a thing

---

The possible inclusion of transcendental quantities is indicated by Galois's reference to "algebraic equations" in the remarks that precede his proof of Proposition 1. He surely means polynomials whose coefficients are transcendental or, to put it colloquially, whose coefficients are letters, not numbers.

[2] *Unless the divisor is monic, division of polynomials can become cumbersome. Since multiplication of $g(x)$ by a nonzero element of the ground field does not affect its greatest common divisor with $f(x)$, one can simplify the division by multiplying $g(x)$ by a suitable power of the leading coefficient of $f(x)$. In this way, one never needs to do any divisions in the ground field and the algorithm produces a greatest common divisor whose coefficients are in the ring generated in K by the coefficients of $f(x)$ and $g(x)$. If, for example, $K = \mathbf{Q}$ and $f(x)$ and $g(x)$ have integer coefficients, then a greatest common divisor found by this method will have integer coefficients.*

as a splitting field of $f(x)$ before proceeding to construct one! This is the fallacy that Gauss accused his predecessors of having committed when he was explaining the necessity for his new (in 1799) proof that a polynomial with integer coefficients splits into linear factors over the field of complex numbers, the statement that is often called the fundamental theorem of algebra. He said that his predecessors had based their arguments on the assumption that a polynomial with integer coefficients *had* roots in some sense and that it was possible to *compute* with them; for that reason he held the previous proofs to have been invalid.

The same objection applies to Galois's Lemmas 2 and 3. Their proofs assume that the given polynomial has roots and that computations with the roots can be carried out. But in Galois's case the objection is far less damaging, because Galois was not just proving that one could compute with the roots—in which case it would have been fatal to assume at the outset that it was possible to compute with the roots—but he was giving a *construction* that explained exactly *how* to compute with the roots. That is, he proved that *if it is possible to compute with the roots of* $f(x)$ *in a consistent and rigorous way, then the field of rational functions of these roots is isomorphic to a field of the above form* $K(V)$.

Not until several decades later did Kronecker prove the existence of a splitting field for a given polynomial in a way that would suffice to put Galois's construction on a sound footing. When he did so, he built on what he called *das köstliche Galoische Princip* (the precious Galois principle), by which he meant the construction implied by Lemmas 2 and 3 of Galois's memoir.[3]

Galois's Construction

Lemma 2 states that, for any polynomial $f(x)$ with coefficients in K that is without multiple roots, one can find a rational function V of the roots of $f(x)$ with the property that no two values of V that are obtained by permuting the roots of $f(x)$ in V are equal. He even says that the linear function $V = Aa + Bb + Cc + \cdots$ of the roots $a, b, c, \ldots$ of $f(x)$, in which the coefficients $A, B, C, \ldots$ are integers, has this property when the integer coefficients are suitably chosen.

He gives no proof at all, but—provided one does not question what the roots of $f(x)$ are or how one computes with them—the lemma can be proved in the following way. When the integer coefficients $A, B, C, \ldots$ that are to be determined are regarded as variables, $V = Aa + Bb + Cc + \cdots$ becomes a linear polynomial in these variables whose coefficients are the roots of $f(x)$. There are in fact $m!$ such linear polynomials, where (as in Galois's notation) m is the degree of $f(x)$, one for each permutation of $a, b, c, \ldots$. By virtue of the assumption that $f(x)$ has no multiple roots, the difference of any two of these $m!$ linear polynomials is a *nonzero* linear polynomial in $A, B, C, \ldots$. Therefore, the product of all $m!(m!-1)$ such differences is nonzero; call it Δ. The coefficients of Δ are polynomials in the roots of $f(x)$, but they are *symmetric* polynomials in these roots, and, as was well known and understood long before Galois's time, any symmetric polynomial in the roots of a polynomial can be expressed as a polynomial in its coefficients. Therefore, Δ is a nonzero polynomial in m variables $A, B, C, \ldots$ with coefficients in K. It remains only to show that integer values can be assigned to the variables in a nonzero polynomial with coefficients in K in such a way that the polynomial assumes a nonzero value, which is easily done by induction on the number of variables in the polynomial, and Lemma 2 follows.

Lemma 3 then makes the very important statement that each root of $f(x)$ can be expressed rationally in terms of V when V is chosen as in Lemma 2 (and when, as required by Lemma 2, $f(x)$ has no multiple roots). In other words, the field $K(V)$ is a splitting field of $f(x)$. In this case, Galois does sketch a proof:

Let X be a new variable, and let $G(X)$ be the product of all $m!$ factors $X - V$ where V ranges over the $m!$ versions of V. For simplicity, assume V has the form $Aa + Bb + Cc + \cdots$ where the coefficients $A, B, C, \ldots$ are integers. The coefficients of $G(X)$, being symmetric functions of the roots of $f(x)$, are in K.

By the construction of V, $G(X)$ has $m!$ distinct roots. The factors of $G(X)$ can be partitioned into m subsets by putting two of them in the same subset when they have the same root of $f(x)$ in the first position with the coefficient A. Then $G(X)$ becomes a product of m factors, which can be expressed in the form $F(X, a)$, $F(X, b)$, $F(X, c)$, $\ldots$ where $F(X, Y)$ is a polynomial in two variables with coefficients in K, namely, the polynomial $F(X, Y)$ that is found in the following way. First, let the product $(X - Aa - Bb - Cc - \cdots)(X - Aa - Bc - Cb - \cdots)\cdots$ of the $(m-1)!$ factors $X - V$ of $G(X)$ in which a occurs in the first position be written as a polynomial in X and a by making use of the fact that every symmetric polynomial in the roots $b, c, \ldots$ of $f(x)$ other than the root a can be expressed rationally[4] in terms of a. Then

[3] *See* [3].

[4] *This basic fact about symmetric polynomials follows from the formula* $(x - b)(x - c)\cdots = \frac{f(x)}{x-a}$, *in which the coefficients on the left side are the elementary symmetric polynomials in b, c, ..., and the coefficients on the right*

$F(X,Y)$ is the polynomial found by writing Y in place of a in the resulting polynomial. Thus, $G(X) = F(X,a)F(X,b)F(X,c)\cdots$. (The right side is a polynomial with coefficients in K because symmetric polynomials in the roots $a, b, c, \ldots$ of $f(x)$ have values in K.)

Then a greatest common divisor of $F(V,x)$ and $f(x)$ can be written, on the one hand, as a polynomial with coefficients in $K(V)$, because both $F(V,x)$ and $f(x)$ can be regarded as polynomials in x with coefficients in $K(V)$, but, on the other hand, it has exactly one root a because $F(V,a) = 0$ (as follows from the fact that $F(V,a)$ is a product of $(m-1)!$ factors $V - V'$ where V' ranges over all $(m-1)!$ versions of V in which the root a comes first, and just one of these factors is zero), but $F(V,b) \neq 0$ for all other roots b of $f(x)$ (because V is a simple root of $G(X) = F(X,a)F(X,b)F(X,c)\cdots$). Thus, this greatest common divisor has degree one, so it is of the form $\phi(V)x + \psi(V)$ where $\phi(V) \neq 0$. For the quantities $\phi(V)$ and $\psi(V)$ in $K(V)$ that are found in this way, $\phi(V)a + \psi(V) = 0$, which shows that $a = -\psi(V)/\phi(V)$ is in $K(V)$.

Similarly, a quotient $-\psi_1(V)/\phi_1(V)$ can be constructed that expresses rationally in terms of V the root of $f(x)$ that occurs in the second place of V, with the coefficient B, by grouping the factors $X - V$ of $G(X)$ according to the root that appears in the second place of V. Thus, b is in $K(V)$. In the same way, one finds that all roots of $f(x)$ are in $K(V)$, from which it follows as well that all roots of $G(X)$ are in $K(V)$ for any root V of $G(X)$ (because these roots are rationally expressible in terms of the roots of $f(x)$).

(Galois scrupulously observes that this conclusion—all roots of $f(x)$ can be expressed rationally in terms of a single quantity—is indicated, without proof, in one of Abel's posthumous works. He is probably referring to [1]. As to the priority of the discovery, however, he wrote in another place ([6], pp. 238–239) that "...it would be easy for me to prove that I did not even know the name of Abel when I presented my first research on the theory of equations to the Institute...").

Computation in $K(V)$

Let $G(X) = G_0(X)G_1(X)G_2(X)\cdots$ be the factorization[5] of $G(X)$ into factors irreducible over K. Each of these irreducible factors is a Galois polynomial—that is, adjunction of one of its roots constructs a field over which it splits into linear factors—because adjunction of any one root V to K gives a field in which $f(x)$ has m roots $a, b, c, \ldots$, which means it gives a field in which $G(X)$ has $m!$ roots $Aa + Bb + Cc + \cdots$.

In particular, a splitting field of $f(x)$ can be constructed by adjoining one root V of one irreducible factor of $G(X)$ to K, an observation that answers the question, *how can one do computations with the roots of a given polynomial* $f(x)$*?*—provided one assumes that such computations are possible in the first place—because computations in the field $K(V)$ are quite simple. If (as in Galois's notation) n is the degree of the irreducible factors of $G(X)$ over K, then every quantity in $K(V)$ can be written in one and only one way as a polynomial in V of degree less than n with coefficients in K. In other words, writing a quantity in $K(V)$ as a polynomial in V of degree less than n with coefficients in K puts that quantity in a *canonical form* with the property that two quantities in $K(V)$ are equal only if their canonical forms are identical. Two quantities in canonical form can be added in the obvious way, and they can be multiplied by multiplying them as polynomials and then using the relation $G_0(V) = 0$ to reduce the degree of the product until it is less than $n = \deg G_0$, where $G_0(X)$ is the irreducible factor of $G(X)$ of which V is a root. Finally, the reciprocal of a quantity $\phi(V)$ in canonical form can be found, provided it is not zero, by combining the algorithm for finding a greatest common divisor of $\phi(X)$ and $G_0(X)$ with the fact that $G_0(X)$ is irreducible to find[6] that a nonzero constant c in K can be written in the form $\alpha(X)\phi(X) + \beta(X)G_0(X)$, which implies that $\frac{1}{\phi(V)} = \frac{\alpha(V)}{c}$; this reciprocal of $\phi(V)$ is in canonical form because $\alpha(X)$ can be assumed to have degree less than $n = \deg G_0(X)$.

Automorphisms

The modern abstract notion of an automorphism of a field may have been far removed from Galois's way of thinking, but the representation of the splitting field of $f(x)$ as a field extension obtained by adjoining one root of $G_0(X)$ provides the equivalent of what is now called the Galois group of that field extension, which is a group of automorphisms.

side are polynomials in a by virtue of the remainder theorem, which states that the remainder when $f(x)$ is divided by $x - a$ is $f(a)$, which is zero.

[5] *The factorization of $G(X)$ into irreducible factors is fairly easy to carry out when K is* $\mathbf{Q}$ *or a field obtained from* $\mathbf{Q}$ *by adjoining transcendental quantities (variables), but the general factorization problem is more difficult. See Part 1 of* [2].

[6] *All polynomials with coefficients in K generated by the algorithm for finding a greatest common divisor of $\phi(x)$ and $G_0(x)$ can be written as linear combinations of $\phi(x)$ and $G_0(X)$, so a greatest common divisor can be so written. In the present case, the greatest common divisors are the nonzero constants, because $G_0(X)$ is irreducible and the degree of $\phi(X)$ is less than $n = \deg G_0(X)$.*

The connection is simply the following. As was seen in the preceding section, every rational function of the roots of $f(x)$ with coefficients in K has a unique representation in the canonical form $\phi(V)$, where ϕ is a polynomial of degree less than $n = \deg G_0(X)$ with coefficients in K. Moreover, since this statement implies that all roots of $G(X)$ can be written in this same canonical form, there are exactly n roots V of $G_0(X)$ in $K(V)$. Galois calls them V, V', V'', ..., $V^{(n-1)}$. The mapping which assigns to a quantity $\phi(V)$ in the extension field $K(V)$ the quantity $\phi(V^{(i)})$, which is another quantity in $K(V)$, is an automorphism of $K(V)$ for each of the n roots $V^{(i)}$ of $G_0(X)$ (because V and $V^{(i)}$ satisfy the same defining relation), and these n automorphisms of $K(V)$ constitute what is called the Galois group of $K(V)$ over K today.

Galois deals only with the action of these automorphisms on the list of roots $a, b, c, \ldots$ of $f(x)$, and he represents that action in a very specific way. What he calls "the group of the equation" (before the first scholium of Proposition 1) is not a group at all in the modern technical sense of the word *group,* but simply an $n \times m$ array (see Figure 1), where the number of rows n is the degree of $G_0(X)$ and the number of columns m is the degree of the polynomial $f(x)$ whose roots are to be constructed. (Galois adds an $(m+1)$st column on the left giving captions for the rows.) The first row contains the roots $a, b, c, \ldots$ of $f(x)$ in $K(V)$, listed in some order, and the subsequent rows list the same roots in the order in which they appear after the automorphism that carries V to $V^{(i)}$ is applied. (Galois writes $\phi(V)$, $\phi_1(V)$, $\phi_2(V)$, ... for the first row, but states at the outset that these are to be seen not as polynomials in V but as roots of $f(x)$. Similarly, the symbols $\phi(V^{(i)})$, $\phi_1(V^{(i)})$, $\phi_2(V^{(i)})$, ... in subsequent rows are no doubt to be seen as roots of $f(x)$.)

In the statement of Proposition 1, something very close to the notion of an automorphism of the splitting field is implied.

Proposition 1

Galois's Proposition 1 characterizes the "group of the equation", represented by the $n \times m$ array above, in the following way:

Let a [polynomial] be given of which the m roots are a, b, c, ... There will always be[7] *a group of permutations of the letters a, b, c, ... which will enjoy the following property:*

1. Every function of the roots invariant under the substitutions of this group will be rationally known, and

2. conversely, every function of the roots that is rationally determinable will be invariant under the substitutions.

In both 1 and 2, the manuscript shows that Galois first wrote "permutations" and changed it to "substitutions", but he let "permutations" stand in the phrase "group of permutations," which strongly suggests that the group he had

[7] *Galois first wrote, "One will always be able..." and crossed it out to write, "There will always be...". His approach to algebra led to many more such conflicts between constructive and nonconstructive formulations.*

$$
\begin{array}{llll}
(V) & \phi(V) & \phi_1(V) & \ldots \quad \phi_{m-1}(V) \\
(V') & \phi(V') & \phi_1(V') & \ldots \quad \phi_{m-1}(V') \\
(V'') & \phi(V'') & \phi_1(V'') & \ldots \quad \phi_{m-1}(V'') \\
 & & \ldots\ldots & \\
(V^{(n-1)}) & \phi(V^{(n-1)}) & \phi_1(V^{(n-1)}) & \ldots \quad \phi_{m-1}(V^{(n-1)})
\end{array}
$$

Figure 1. This $m \times n$ array (with an $(m+1)$st column added on the left) is the format in which Galois presented what he called the group of the equation $f(x) = 0$. (However, Galois wrote ϕ's without parentheses as ϕV, $\phi_1 V$, etc. His only parentheses are in the column on the left and the superscripts in the bottom row.) Here V is a quantity with the property that all roots $a, b, c, \ldots$, of $f(x)$ can be expressed rationally in terms of V, and $V', V'', \ldots, V^{(n-1)}$ are the other roots of the irreducible polynomial $G_0(X)$ of which V is a root. Each of the n rows of the array lists the m roots of $f(x)$ in some order. (See examples in the section "Solution of the Quartic".) Every V can be expressed rationally in terms of every other V. The order of the roots in the first row determines their order in all others in the following way. Write each root as a function of V and let these functions be given the names $\phi_i(V)$ shown in the first row, in that order. Then $\phi_i(V')$ is also a root of $f(x)$; this is the root that is to be entered in the ith column of the second row, and the other rows are to be filled in similarly. It should be emphasized, however, that Galois saw the entries of the array as *roots of* $f(x)$, not as polynomials in the various V's. In modern terms, the field $K(V)$ has n automorphisms $V \mapsto V^{(j)}$, and the table shows the way in which these automorphisms act on the roots of $f(x)$.

in mind in the statement of the proposition was simply the $n \times m$ array listing the roots in different orders, which is not a group at all in the modern sense. Very likely this "group of permutations" was for him a constructive presentation of the more abstract notion of a group (in the modern sense) of substitutions of the roots, namely, the substitutions that transform any one row of the array into any other.[8]

The purpose of Proposition 1 is clear, but its statement is somewhat flawed. Galois has constructed the "group of the equation" and he wants to characterize that group in a way that is independent of the choices that were made in the construction. The flaw is that he tries to characterize the substitutions in the group in terms of the way that they act on functions of the roots, when in fact, as the proposition itself implies, a substitution of the roots does *not* act on functions of the roots unless it is in the group. (For example, if a, b, and c are the roots of $x^3 + x^2 - 2x - 1$, numerical approximations to the roots can be used to find that $a^2b + b^2c + c^2a$ is either 3 or -4 depending on the order in which the roots are listed. If an order is chosen in which $a^2b + b^2c + c^2a = 3$, then interchanging a and b changes the version of the function of the roots on left side from 3 to -4, but leaves the version on the right side unchanged, so this interchange does not act on this "function".)

What characterizes the substitutions described by the group is not *the way* that they act on rational functions of the roots, but the fact that they *do* act on rational functions of the roots. In modern terms, they are substitutions that are restrictions of automorphisms of the splitting field, which is to say that they are transformations of the splitting field that preserve its structure. In language closer to Galois's: *A substitution of the roots is in the group of $f(x)$ if and only if any relation $F(a,b,c,\dots) = 0$ among the roots of $f(x)$, where $F(a,b,c,\dots)$ is a rational function of the roots of $f(x)$, remains valid when the substitution is applied to the variables a, b, c, ... in $F(a,b,c,\dots)$.*

In other words, Galois surely meant something like:

Proposition 1 (Revised)**.** *Let a [polynomial] 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. *Every function of the roots $F(a,b,c,\dots)$ that has a rationally known value has the same rationally known value when a substitution of this group is applied, and*

2. *conversely, every function of the roots $F(a,b,c,\dots)$ that satisfies $F(a,b,c,\dots) = F(Sa, Sb, Sc, \dots)$ for all substitutions S in this group will have a rationally known value.*

Proof. When $F(a,b,c,\dots)$ is written in canonical form as a polynomial in V of degree less than n with coefficients in K, the proposition becomes the statement that such a polynomial $\phi(V)$ is unchanged by all substitutions $V \mapsto V^{(i)}$ if and only if it has degree zero. Obviously it is unchanged if it has degree zero. Conversely, if it is unchanged by all substitutions, then it is equal to $\frac{1}{n}\sum_{i=1}^{n} \phi(V^{(i)})$, which is in K because it is a symmetric function of the roots $V^{(i)}$ of $G_0(X)$, a polynomial whose coefficients are in K. □

Proposition 2

Galois's Proposition 2 states:

If one adjoins to a given equation the root r of an irreducible auxiliary equation, (1) *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 equation, and* (2) *these groups will enjoy the remarkable property that one will pass from one to another by operating on all the permutations of the first with one and the same substitution of letters.*

This proposition contains an obvious flaw that results from a hasty reworking of the memoir, probably in the last hours before the duel: In part (1) he refers to p without having said what p is. The manuscript shows that in the original statement p denoted the degree of the auxiliary equation, and it was assumed to be prime. In the revision, Galois was dropping the assumption that the degree of the auxiliary equation was prime and failed to notice that in deleting the words "of prime degree p" before (1) he was deleting the definition of p.

But a less obvious flaw results from the reworking as well. The one-to-one correspondence between the "groups" in the partition and the roots of the auxiliary equation is lost. When p was assumed prime, this equality was already just one of the two possibilities (the other being that "the group of the equation will not be changed"), but when p is not prime the equality is lost altogether, as will be seen in the next section, and the number of "groups" is determined in a quite different way. The removal of the assumption that the degree of the adjoined quantity is prime is an important broadening of the theory, but in the form Galois hastily gave it Proposition 2 garbles the description of the way in which an adjunction partitions the group of $f(x)$. Certainly he knew better.

[8] *See* [6], *pp. 22–23.*

Two other aspects of Proposition 2 pose obstacles for modern readers, because they appear to be flaws even though they are not. First, part (2) suggests to a modern reader that Galois is saying that the subgroup corresponding to the adjunction is a *normal* subgroup, which is not at all the case. In fact, (2) only says that the "groups" in the partition in (1) (which are of course not groups in the modern sense) describe conjugate subgroups (in the modern sense) of the group of $f(x)$. When it is stated in this way, the property described in (2) seems far less "remarkable", at least to a modern reader.

Second, when he says in (1) that adjoining *one* root partitions the group of $f(x)$ into p groups, each belonging to the adjunction of a different root of the auxiliary equation, a modern reader is naturally confused. If only one root was adjoined, how can the partition involve the adjunction of other roots? This question is answered in the next section.

Proposed Revision of Proposition 2

It was in connection with the proof of Proposition 2 that Galois made the marginal note, "Il y a quelque chose à compléter dans cette démonstration. Je n'ai pas le temps". (There is something to be completed in this proof. I do not have the time.) This statement and the apparent haste of the handwriting have led editors of the memoir to conclude that the revision of Proposition 2 was made on the night before the duel ([6], pp. 158–159). Neumann calls the note a *cri de coeur* ([6], p. 161); it is certainly a major part of the drama and tragedy of the Galois story.

As is explained above, there is indeed something to be completed in Proposition 2. When the degree of the auxiliary equation is a prime p, the proposition is correct and plays an important role in the later propositions relating to solution by radicals. However, Galois's hasty revision shows that he was ready to drop the assumption of primality and felt he needed only a little more time to do it accurately.

The scholium (a word that is rarely used today, meaning an amplification of the proposition under discussion) that ends Proposition 1 states that "the substitutions are independent even of the number of roots," which implies that Galois contemplated changing the number of roots of $f(x)$. What could he have meant by this?

Changing the number of roots would mean changing the degree of $f(x)$. Surely there would be no point in saying that Proposition 1 is independent of the degree of $f(x)$, so he cannot have meant this. On the other hand, what could it mean to say that the substitutions are independent of the number of roots when the substitutions are substitutions of these very roots?

The most convincing interpretation, it seems to me, is that Galois was contemplating adding more columns to the $n \times m$ array that describes the "group" (m is of course the number of roots), which would mean changing $f(x)$ to a polynomial with coefficients in K that is *divisible* by $f(x)$. This suggests that, in order to study $f(x)$ as a polynomial to which a root of an irreducible auxiliary polynomial $g(x)$ is adjoined, one might find the group of $f(x)g(x)$ instead of the group of $f(x)$ (unless $f(x)$ and $g(x)$ have a root in common, in which case, by Lemma 1, $g(x)$ is already a factor of $f(x)$ and the quantity to be adjoined is already a root of $f(x)$). Since, as the scholium points out, Proposition 1 means that the substitutions in the "group of $f(x)$" depend only on the roots $a, b, c, \ldots$ themselves, they can be read off from the enlarged array (which may also contain more rows but which, by Proposition 1, can indicate no additional substitutions of the roots of $f(x)$) as well as from the original one.

In short, the question that is answered by Proposition 2, "how is the group of $f(x)$ reduced if the field of known quantities K is extended to include a new quantity?" will be answered in the general case if it is answered in the special case in which the quantity that is adjoined is a root of $f(x)$. In this case, however, the answer can be seen clearly in terms of the $n \times m$ array that describes the group of $f(x)$, as the proof below shows. I believe that Galois would have used an argument like this one to "complete" his proof of the proposition.

Proposition 2 (Revised)**.** *If one adjoins to a given equation one of its roots a,* (1) *the group of the equation will be partitioned into k groups, each belonging respectively to the proposed equation when one adjoins to it one of the roots to which the substitutions of the group carry a, and* (2) *these groups will enjoy the* (remarkable?) *property that one will pass from one to another by operating on all the permutations of the first with one and the same substitution of letters.*

The proof that follows is suggested by the proof Galois indicated for Lemma 3 (see above), as well as the one he indicated for Proposition 2.[9]

Proof. Since rearranging the rows or columns of the $n \times m$ array does not change the substitutions that it describes, there is no loss of generality in assuming that the root a that is adjoined is the

[9] *Proposition 2 posed difficulties for Joseph Liouville as he worked through Galois's memoir to validate it. His proof of it departed substantially from Galois's indications. See* [6]*, pp. 159–161.*

root in the upper left corner of the array. Let k be the number of different roots of $f(x)$ that occur in the first column, and let them be a, a', a'', ..., $a^{(k-1)}$. Again, since the order of the rows is immaterial, the rows can be arranged as k blocks of rows, listing first all rows that begin with a, then all rows that begin with a', and so forth. The proposition will be proved by showing that each block presents "the group of $f(x)$" after the corresponding $a^{(i)}$ is adjoined.

Part (2) of the proposition is simply the observation that a substitution which carries a row beginning with $a^{(i)}$ to a row beginning with $a^{(j)}$ carries all rows beginning with $a^{(i)}$ to rows beginning with $a^{(j)}$. In particular, k divides n, and the quotient, call it n', is the number of rows in each of the k blocks.

In the above proof of Lemma 3, a polynomial $F(X,Y)$ in X and Y with coefficients in K was constructed with the property that, for any root V of $G_0(X)$, the polynomials $F(V,Y)$ and $f(Y)$ have only one root in common, namely, the root a of $f(x)$ that is in the first position of $V = Aa + Bb + Cc + \cdots$. Let $H(X,Y)$ be the monic greatest common divisor of $G_0(X)$ and $F(X,Y)$ when they are treated as polynomials in X whose coefficients are rational functions in Y with coefficients in K. (The greatest common divisors are polynomials in X whose coefficients are rational functions of Y. The monic greatest common divisor is the one whose leading coefficient is 1.) For any root $a^{(i)}$ that appears in the first column of the $n \times m$ array, the roots V of $H(X,a^{(i)})$ are the roots that $G_0(X)$ and $F(X,a^{(i)})$ have in common, which are simply the roots of $G_0(X)$ that correspond to rows in which $a^{(i)}$ appears in the first column. Thus, $G_0(X)$ has the factorization $H(X,a)H(X,a')H(X,a'')\cdots$, which partitions the rows of the $n \times m$ array into k blocks, each $n' \times m$, as above. What is to be shown is that each factor $H(X,a^{(i)})$, which of course has coefficients in $K(a^{(i)})$, is irreducible over this field, so that it is a factor of $G(X)$ irreducible over $K(a^{(i)})$ and its roots V therefore determine the rows of "the group of $f(x)$" when the known quantities are those in $K(a^{(i)})$.

Adjunction of $a^{(i)}$ gives an extension of K of degree k because $a^{(i)}$ is a root of a polynomial of degree k with coefficients in K (namely, $\prod_{i=0}^{k-1}(x - a^{(i)})$, which has coefficients in K by Proposition 1) that is irreducible over K (because leaving out any factor of $\prod(x - a^{(i)})$ gives a polynomial whose coefficients are not in K by Proposition 1). Therefore, $K(V)$, which is an extension of degree n of K that contains $a^{(i)}$, is an extension of $K(a^{(i)})$ of degree $\frac{n}{k} = n'$, which is the degree of $H(X,a^{(i)})$. If $H(X,a^{(i)})$ were reducible, then V would be a root of a polynomial with coefficients in $K(a^{(i)})$ whose degree was less than n', and the degree of $K(V)$ over K would be less than n. Therefore, $H(X,a^{(i)})$ is irreducible over $K(a^{(i)})$, as was to be shown. □

The Fundamental Theorem of Galois Theory

In the previous section, the device of changing $f(x)$ to a polynomial of higher degree that is divisible by $f(x)$ served two purposes. First, it created a universe—the splitting field of the new polynomial—that contained the adjoined quantity along with the roots of $f(x)$, and, second, it made possible the simple description of the proposition in terms of the partition of the $n \times m$ array into k subarrays, each $n' \times m$.

In modern Galois theory, the universe is described as a normal extension of K—that is, the splitting field of some unspecified $f(x)$—and the elements of the Galois group are regarded as abstract automorphisms of that normal extension without any specified way of describing them. In these abstract terms, Proposition 2 says simply that *the adjunction of a quantity in a normal extension of K to the ground field reduces the Galois group to the subgroup that contains just those automorphisms that leave the adjoined quantity unmoved.* Since, by Proposition 1, a quantity in the extension field is "known" if and only if it is unmoved by the permutations of the Galois group, and since the "known" quantities become those in the subextension $K(a)$, where a is the adjoined quantity, the proposition takes the form:

Proposition 2 (Modernized)**.** *The subextension $K(a)$ of a normal extension of K obtained by adjoining a to K contains precisely those quantities of the normal extension that are unmoved by the same automorphisms that leave a unmoved. Moreover, the number n′ of such automorphisms is $\frac{n}{k}$, where n is the order of the Galois group and k is the number of distinct images of a under the Galois group.*

This proposition can be applied several times, expanding the ground field with each step, to find:

Proposition. *A subextension $K(a_1, a_2, \ldots, a_t)$ of a normal extension obtained by adjoining t quantities $a_1, a_2, \ldots, a_t$ to K contains precisely those quantities of the normal extension that are unmoved by the automorphisms that leave all of $a_1, a_2, \ldots, a_t$ unmoved. Moreover, the number n′ of such automorphisms is $\frac{n}{k_1 k_2 \cdots k_t}$, where n is the order of the original Galois group and each k_i is the number of distinct images of a_i under automorphisms that leave $a_1, a_2, \ldots, a_{i-1}$ unmoved.*

This proposition constructs the smallest subextension that contains a given (finite) set of quantities $a_1, a_2, \ldots, a_t$ in the extension. In this way,

it establishes a correspondence between subextensions of a normal extension and subgroups of its Galois group, the correspondence that is called the fundamental theorem of Galois theory. This version of the fundamental theorem underlies the treatment of Galois theory that I gave in my book *Essays in Constructive Mathematics* [2].

Proposition 3

Galois's Proposition 3 states that *if all roots of an auxiliary equation are adjoined to K, then the "groups" in Proposition 2 all describe the same substitutions of the roots.* In modern terms, this is the statement that normal extensions correspond to normal subgroups, an observation that is often included, appropriately enough, in the statement of the fundamental theorem of Galois theory. Galois offers no proof, saying a proof "will be found," and indeed the proof is not difficult.

Let $a_1, a_2, \ldots, a_t$ be the roots of a polynomial with coefficients in K, and let them all lie in the splitting field of some $f(x)$. By Lemmas 2 and 3, integers $A_1, A_2, \ldots, A_k$ can be chosen in such a way that adjoining $v = A_1a_1 + A_2a_2 + \cdots + A_ta_t$ adjoins each a_i and therefore adjoins each v' obtained from v by permuting the a_i. Adjoining $a_1, a_2, \ldots, a_t$ is the same as adjoining any of the quantities v' obtained by permuting the a_i in v. The "groups" in Proposition 2 in this case give the substitutions that leave all quantities in $K(v')$ unmoved, where the v' are the other roots of the irreducible polynomial of which v is a root. Since $K(v') = K(v)$ for all these v', the proposition follows.

Proposition 4

Proposition 4 makes a strange statement about adjoining a "numerical" value of a [rational] function of the roots. Perhaps Galois saw Proposition 4 as necessary when Proposition 2 was still restricted to adjunctions of prime degree, or perhaps he had some conception of "numerical" values that I am failing to understand, but in any case Proposition 4 seems to me to be a special case of Proposition 2 and does not seem to be important to what follows.

Proposition 5

Galois adopted the classical Euclidean style[10] in which propositions could be either *theorems* or *problems.* His first four propositions are labeled "theorem", but the fifth and seventh are "problems", while the sixth is a "lemma", and the eighth is again a "theorem". In Euclid, theorems are distinguished from problems by the fact that the discussion of a problem concludes with "as was to be done," while a theorem ends with "as was to be shown." Galois does not follow Euclid in this, but his discussions of problems are different from his discussions of theorems. For example, Proposition 5 is stated as the problem, "Under what circumstances is an equation solvable by simple radicals?" and his discussion of it ends with an indication of a constructive method for determining whether a given $f(x)$ is solvable by radicals by analyzing the group of $f(x)$. The method, essentially, is to determine whether the group contains a normal subgroup of prime index and, if so, to determine whether that subgroup has a normal subgroup of prime index, and so forth. The equation [polynomial] is solvable if and only if one can find a succession of such normal subgroups of prime index until a group of order one is reached.

The ideas and methods here are near enough to the modern ones that they probably require no further comment to be understandable to a 21st-century reader.

Solution of the Quartic

In his scholium to Proposition 5, Galois applies his method to the solution of the general quartic, the quartic polynomial $f(x) = x^4 + Ax^3 + Bx^2 + Cx + D$ in which the coefficients A, B, C, and D are *letters.* In other words, the ground field K is the field $\mathbf{Q}(A, B, C, D)$ of rational functions in A, B, C, and D with integer coefficients. In Proposition 1 he already stated, without proof, that the group of the general (or, as he calls it there, the algebraic) equation of degree m contains all $m!$ permutations of the roots. Therefore, it is to be shown that the symmetric group S_4 of permutations of the four roots has a normal subgroup of prime index, which in turn has a normal subgroup of prime index, and so forth, until a group of order one is reached. Galois accomplishes this by exhibiting the successive normal subgroups.

The first subgroup, normal in S_4, is the alternating group A_4 of index 2. In Galois's formulation, it is described by a decomposition of the 24 permutations of the roots a, b, c, d into two 12×4 arrays, namely,

abcd	*bacd*
badc	*abdc*
cdab	*cdba*
dcba	*dcab*
acdb	*bcda*
cabd	*cbad*
dbac	*dabc*
bdca	*adcb*
adbc	*bdac*
dacb	*dbca*
bcad	*acbd*
cbda	*cadb*

[10] *See* [5], *vol. 1, pp. 124–129.*

although he does not write them explicitly. What makes this a decomposition that corresponds to a normal subgroup is the fact that one array is obtained from the other by the same substitution of letters (namely, the interchange $a \leftrightarrow b$) at the same time that they represent the same substitutions of letters (namely, the even permutations).

The 12×4 array on the left can be decomposed into three 4×4 arrays, namely,

$$\begin{array}{lll} abcd & acdb & adbc \\ badc & cabd & dacb \\ cdab & dbac & bcad \\ dcba & bdca & cbda. \end{array}$$

Again, one passes from any one of these three to any other by the same substitution of letters (for example, from the first to the second by leaving a fixed and changing b to c, c to d, and d to b), and all three represent the same substitutions of the letters (namely, a 4-group, consisting of the identity and the three compositions of two disjoint 2-cycles). The first 4×4 array decomposes as

$$\begin{array}{ll} abcd & cdab \\ badc & dcba \end{array}$$

which again is a normal decomposition, and finally the 2×4 array on the left decomposes as

$$\begin{array}{ll} abcd & badc \end{array}$$

and the group is now a 1×4 array.

According to Proposition 5, this analysis shows that the general quartic is solvable by radicals. Also according to Proposition 5, one can determine actual adjunctions that reduce the group to a single permutation. According to that proposition, what is needed for the first step is a quantity that is unchanged by even permutations of the roots but not by all permutations of the roots. Such a quantity, well known to algebraists long before Galois's time, is $(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$, a quantity[11] often denoted by $\sqrt{\Delta}$ (where Δ is its square, a symmetric polynomial in the roots and therefore a polynomial in A, B, C and D with integer coefficients) which is unchanged by even permutations and whose sign is changed by odd permutations. Therefore, by Proposition 5, an adjunction that effects the first reduction of the group from one in which $n = 24$ to one in which $n = 12$ is the adjunction of a square root of $(\sqrt{\Delta} - (-\sqrt{\Delta}))^2 = 4\Delta$, or, what is the same, adjunction of a square root of Δ.

For the next adjunction, what is needed is a quantity that is unmoved by the 4-group (the substitutions that are represented by each of the three 4×4 arrays above) but has three distinct images under the group A_4. As is easily seen, the three quantities $(a+b-c-d)^2$, $(a-b+c-d)^2$, and $(a-b-c+d)^2$ are invariant under the 4-group and are permuted cyclically by A_4. Therefore, one can adjoin $\sqrt{-3}$ to $\mathbf{Q}(A, B, C, D, \sqrt{\Delta})$ and then a cube root of $(p + \alpha q + \alpha^2 r)^3$, where p, q, and r are these quantities and $\alpha = \frac{-1+\sqrt{-3}}{2}$ is a cube root of unity, to effect the needed reduction.

Next, $a+b-c-d$ is unchanged by the two elements of the 4-group represented by the two 2×4 arrays, but its sign is reversed by the other two elements, so the recipe of Proposition 5 calls for adjoining a square root of 4 times its square or, what is the same, a square root of $(a+b-c-d)^2$ itself.

Finally, the sign of $a-b+c-d$ is reversed by the element other than the identity of the 2-element group that remains, so the group is reduced to a single element by adjoining a square root of $(a-b+c-d)^2$.

Galois's assertion that "in this way one finds the solution of Descartes or that of Euler" is generous to Descartes and Euler. According to Neumann ([6], p. 163), it is unclear exactly which versions of which methods Galois is referring to, but the method of solving quartic equations that Euler presents in [4], calling it "new", is the following.

Normalize the given quartic to make $a+b+c+d = 0$, say it is $x^4 - Ax^2 - Bx - C$. First solve the cubic $z^3 - \frac{A}{2}z^2 + (\frac{A^2}{16} + \frac{C}{4})z - \frac{B^2}{64} = 0$, say the roots are p, q, and r. The roots of the given quartic are $\sqrt{p} + \sqrt{q} + \sqrt{r}$ when the signs of the square roots are correctly chosen.

Elegant and effective as Euler's explanation of his method is, he does not show the underlying principle in the way that Galois does. When the quartic is normalized as Euler instructs, the cubic is in fact the one whose roots are the three quantities $p = \frac{1}{16}(a+b-c-d)^2$, $q = \frac{1}{16}(a-b+c-d)^2$, and $r = \frac{1}{16}(a-b-c+d)^2$. The first step in the solution of this cubic is to adjoin a square root of $(p-q)^2(p-r)^2(q-r)^2$, which, when it is expressed in terms of a, b, c, and d, can be found to be $2^{12}(a-b)^2(a-c)^2(a-d)^2(b-c)^2(b-d)^2(c-d)^2$. Thus Galois's first step, which is to adjoin a square root of the rational quantity $(a-b)^2(a-c)^2(a-d)^2(b-c)^2(b-d)^2(c-d)^2$, accomplishes the same objective as Euler's first step, which is to adjoin a square root of the rational quantity $(p-q)^2(p-r)^2(q-r)^2$. Similarly, Galois's second step, which is to adjoin a cube root of $(p + \alpha q + \alpha^2 r)^3$, accomplishes the same objective as Euler's second step, namely, to adjoin a quantity p or q or r that is invariant under the subgroup of index 3 in the group of even permutations of the four roots of the quartic

[11] *It can be written as the determinant* $\sqrt{\Delta} = \begin{vmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^3 & b^3 & c^3 & d^3 \end{vmatrix}$. *In this form, it gives a convenient definition of even and odd permutations.*

but not invariant under the whole group, because the whole group permutes p, q, and r cyclically. Finally, as Galois charitably points out, although Euler extracts three square roots $\sqrt{p}$, $\sqrt{q}$, and $\sqrt{r}$, only two are in fact necessary; this follows from the observation that, in Euler's notation, $\sqrt{pqr} = \frac{B}{8}$ is rational (this quantity is $\sqrt{h}$ in Euler), so $\sqrt{r}$ is known once $\sqrt{p}$ and $\sqrt{q}$ are adjoined. Combining $\sqrt{p} = \frac{1}{4}(a + b - c - d)$, $\sqrt{q} = \frac{1}{4}(a - b + c - d)$ and $\sqrt{r} = \frac{1}{4}(a - b - c + d)$ with $0 = \frac{1}{4}(a + b + c + d)$ then shows that $a = \sqrt{p} + \sqrt{q} + \sqrt{r}$ and that the four roots are $\pm\sqrt{p} \pm \sqrt{q} \pm \sqrt{r}$ when the sign of $\sqrt{r}$ is determined by the first two signs. (The rule is that the number of minuses is even.) In short, the steps are essentially the same in the two methods, but Galois's steps are dictated in a simple way by his Proposition 5 *and* they do not require the normalization $a + b + c + d = 0$.

Proposition 6

It is somewhat surprising that Galois found worthy of special mention the lemma that *an irreducible equation of prime degree cannot become reducible by the adjunction of a radical,* especially so because his formulation is inaccurate. His proof and the final statement in his discussion of the proposition make clear, however, that he meant to say that an adjunction of a radical can reduce an irreducible polynomial of prime degree only if it factors it into linear factors, because a radical adjunction necessarily factors $G_0(X)$ into factors of equal degree (provided, as Galois assumes, that the radical is of prime degree p and that the pth roots of unity have already been adjoined) by Propositions 2 and 3.

Proposition 7

Proposition 7 is the second "problem" in the memoir, and it is in fact an elaboration of the first "problem", namely, Proposition 5, which was to determine whether a given equation [polynomial] was solvable by radicals. Proposition 7 is the special case in which the polynomial to be solved has prime degree. Galois's answer is that *an irreducible polynomial of prime degree p is solvable by radicals if and only if its roots x_k can be ordered in such a way that the substitutions of the roots in its group all have the form $x_k \mapsto x_{ak+b}$ for some integers a and b,* where it is understood that subscripts on the roots are to be interpreted as integers mod p.

The lemma of Proposition 6 implies by a fairly easy argument that the next-to-last subgroup in the reductions, the one before the subgroup containing just one element is reached, must be cyclic of order p. Since Proposition 5 states that the sequence of reductions can only include reductions to *normal* subgroups, Proposition 7 follows from: Let S_p be the group of all permutations of the integers mod p, and let C_p be the subgroup generated by the permutation $k \mapsto k + 1$. *The normalizer of C_p in S_p is the group of permutations of the form $k \mapsto ak + b$.* The proof is an exercise in elementary group theory; Galois of course proves it using his own terminology.

At the end of the memoir, following Proposition 8, Galois gave what he labeled an "Example of Theorem VII" (even though Proposition 7 is a problem, not a theorem). It is a 20×5 array showing, in Galois's format, the largest possible group of a solvable quintic. Since he already stated in Proposition 1 that the general quintic has a group of order 120, it follows—although Galois makes no mention of it—that the general quintic is not solvable by radicals. (Note that the simplicity of the alternating group A_5, so often invoked in textbook proofs of this fact, is not needed.)

Questions about Proposition 7

I am unable to explain several points in the latter part of Proposition 7.

First, I am puzzled by his reference to "the method of M. Gauss", which he invokes to conclude that the quantities he denotes $X_1, X_a, X_{a^2}, \ldots$ can be found [by radical adjunctions] even though the desired conclusion follows immediately from his own Proposition 5. (A nontrivial cyclic group contains a subgroup of prime index, and every subgroup of a cyclic group is both normal and cyclic.) He is referring, almost certainly, to Section 7 of the *Disquisitiones Arithmeticae,* where Gauss treats in detail the algebraic solution of $x^n - 1$, primarily for prime values of n. To modern readers, it is natural to regard Gauss's solution of $x^n - 1 = 0$ as an application of Galois theory published ten years before Galois was born, but Galois himself, instead of using his own Proposition 5 to prove that a cyclic equation is solvable, cites Gauss—a reference that appears to call for some nontrivial intermediate steps, namely, the reduction of a cyclic equation to a binomial equation and the reduction of a general binomial equation to $x^p - 1 = 0$ for prime p. One explanation of this choice on Galois's part would be that he was acknowledging having profited from reading Gauss's treatment of this important special case of the solution of algebraic equations. Another would be that he hoped to win approval of his work from Gauss, who at the time was in his early fifties and widely regarded as the prince of mathematicians. (In his famous testamentary letter, Galois would ask his friend Chevalier to bring his work to the attention of Gauss and Jacobi.)

Secondly, I am unable to reconstruct what Galois had in mind when he wrote, "Therefore,

etc." at the end of this argument, as though the rest of the argument were routine. He has proved that the X_{a^i} he defines can be expressed in terms of radicals, but his goal is to prove that the x_i can be expressed in terms of radicals. Most probably, he intended to use the formula $x = \frac{1}{n}(c + \sqrt[n]{X_1} + \sqrt[n]{X_a} + \cdots + \sqrt[n]{X_{a^{n-2}}})$, where c is the sum of the roots, but this formula, instead of representing the n desired roots of the given equation, represents n^{n-1} quantities, only n of which are roots, because there are n choices for each of the nth roots. His assertion that any $f(x)$ whose group has the specified form is solvable by radicals is correct, but his proof seems inadequate. What is needed is a formula to connect the choices of nth roots in the formula $x = \frac{1}{n}(c + \sqrt[n]{X_1} + \sqrt[n]{X_a} + \cdots \sqrt[n]{X_{a^{n-2}}})$ so that it describes just the n required roots. Galois may well have had an answer to this question, but no answer is apparent. (Also, he may have been satisfied with a formula involving radicals that *included* the n roots in a set of n^{n-1} possibilities, but I am inclined to doubt it.)

Finally, I am unsure what Galois means by "the method that would have to be used in practice." His formula $\prod(X_{a^i} - X)$ defines a polynomial $F(X)$ of degree $n-1$ with coefficients in the splitting field of the given polynomial. It has $(n-2)!$ conjugates under the action of S_n, because $n(n-1)$ permutations of the form $x_k \mapsto x_{ak+b}$ leave it unchanged. Let these conjugates be $F^{(i)}(X)$ for $i = 1, 2, \ldots, (n-2)!$. The product $G(X,Y) = \prod(Y - F^{(i)}(X))$ over all $F^{(i)}(X)$ is a polynomial in two variables with coefficients in K. If the original polynomial is solvable, then there is a j for which $F^{(j)}(X)$ has coefficients in K; the corresponding factor $Y - F^{(i)}(X)$ of $G(X,Y)$ has coefficients in K, so $G(X,Y)$ has a root $Y = F^{(j)}(X)$ in K for any value of X in K. Galois seems to say that this necessary condition is also sufficient and that "one knows how to" determine whether it is satisfied.

Proposition 8

The final proposition is again a theorem, namely, the corollary of Proposition 7 that results when one notes that the groups of the form described by Proposition 7 leave at most one root fixed unless they leave all roots fixed or, what is the same, unless they consist of the identity alone.

This theorem, stating that *an irreducible polynomial of prime degree is solvable by radicals if and only if all roots can be expressed rationally in terms of any two of them,* will doubtless seem peculiar to 21st-century readers. It seemed peculiar as well to the referees Lacroix and Poisson, who recommended the rejection of Galois's memoir, because, as is natural, they wanted a solvability criterion that could be applied to a given polynomial. Its advantage, it seems to me, is that it requires no group theory or field theory, and no special constructions, for its statement. If one knows what it means for a polynomial to be solvable by radicals, one knows more than enough to understand what it means to say that all roots can be expressed rationally in terms of any two. I believe that is why Galois chose it as his concluding proposition.

Again, Study the Masters

The introduction to my 1974 book *Riemann's Zeta Function* was an exhortation to "Read the classics!" A few years later I discovered Niels Henrik Abel's remark that "It appears to me that if one wants to make progress in mathematics one should study the masters and not the pupils," which then became my constant refrain. Abel's contrast of "masters" to "pupils" is an important addition to the message. "Read the classics" doesn't just mean read good texts; it means read the texts that gave birth to the subjects or gave them their most vivid statements—those written by the "masters"—not the ones written by later "pupils", who themselves learned the ideas from the masters and are trying to make presentations that are more accessible or that conform to newer styles.

I have tried to show here that the ideas expressed by what is now called the fundamental theorem of Galois theory are all contained, in a very effective but terse form, in the first few pages of Galois's First Memoir. In the course of the writing, I have been forcefully reminded of the extent to which Galois is the master and I the pupil.

Once again, I advise students to *Study the masters!* Thanks to Peter Neumann's meticulous reexamination of all of Galois's works—not just of the First Memoir—many more students will now be able to do so.

References

[1] N. H. Abel, Précis d'une théorie des fonctions elliptiques, §1 of Chapter 2, *Jour. f. reine u. angew. Math.* **4** (1829), 236–277, 309–348. Also, *Oeuvres,* vol. 1, 518–617.

[2] H. M. Edwards, *Essays in Constructive Mathematics*, Springer-Verlag, New York, 2005.

[3] ———, Kronecker's fundamental theorem of general arithmetic, in *Episodes in the History of Modern Algebra*, Gray and Parshall, eds., AMS-LMS, 2007.

[4] Leonhard Euler, Vollständige Anleitung zur Algebra, *Opera Omnia*, Series 1, Vol. 1.

[5] Thomas L. Heath, *The Thirteen Books of Euclid's Elements*, 2nd edition, Cambridge Univ. Press, 1925; Dover reprint, 1956.

[6] Peter M. Neumann, *The Mathematical Writings of Évariste Galois*, European Mathematical Society, Zürich, 2011.