Galois's Version of Galois Theory

Talk Presented at the Galois Bicentennial
Insitut Henri Poincaré, Paris, October 24, 2011

I expect that a great deal will be said at this conference about Galois's role as a harbinger of modern abstract algebra, the creator of group theory who made the first great steps toward abstract groups, rings, and fields. However, what I admire most and want to praise here is a very different aspect of Galois's contribution. I am a lifelong proponent of constructive mathematics, and for me Galois is the mathematician who pushed the notion of a mathematical construction to a level of abstraction that left actual computation far behind, while continuing to rely on the *idea* of computation as the foundation of his thought. What I mean by this is clearly stated in my favorite quote from Galois. In the "*Discours Préliminaire*" that he wrote for a projected but never completed revision of the *Premier Mémoire* he wrote:

> Si maintenant vous me donnez une équation algébrique que vous aurez choisie à votre gré, et que vous désiriez connaitre se elle est ou non résoluble par radicaux, je n'aurai rien à y faire que de vous indiquer le moyen de répondre à votre question, sans vouloir charger ne moi ni personne de le faire. (And then the punch line:) En un mot les calculs sont impraticables.

This passage shows that Galois saw his theory as dealing with algebraic computations. He promised to tell his reader exactly what computation needed to be done to decide whether a given polynomial had a root that can be expressed in terms of radicals. He didn't want to do the work it would require to find the answer, though, and, to tell the truth, he *couldn't have* even if he had wanted to, because the computation would be impossibly long, even for quite simple examples. The great message of Galois's work, for me, is that *it doesn't matter that the computations are impossibly long.* As long as the computations are unambiguously prescribed and can be completed in finite time, the theory is constructive. (What is more, in our age of computers, the conception of impossibly long has become far, far longer.)

In understanding the *Premier Mémoire*—and my intention today is to sketch the main ideas of that memoir—it is important to realize that its reasoning is based on an unspoken and unproven assumption, namely, that there is a rigorous way to carry out computations with the roots of a given polynomial. Galois supposes that a polynomial of degree m is given—he gives it no name, referring to it simply as "*la proposée,*" but I will call it $f(x)$. For the sake of simplicity, I will assume that $f(x)$ has integer coefficients, and that its leading coefficient is 1. What I want to emphasize is that Galois assumes, without justification, that computations with the roots a, b, c, … of $f(x)$ are meaningful and can be carried out. You can see what I mean in the context of his Lemma 2.

Lemma 2 states that if a, b, c, … are the m roots of $f(x)$, then there are integers A, B, C, … , with the property that $V = Aa + Bb + Cc + \cdots$ assumes $m!$ distinct values when the positions of the m roots a, b, c, … of $f(x)$ in V are permuted in all $m!$ ways. It is impossible to state this lemma without that unjustified assumption I have mentioned.

What is the meaning of V, and how can you tell whether two values of V, in which the roots appear in a different order, might or might not be equal? You must be able to compute with the roots for these questions to have meaning.

In this light, there is a seriously circular argument in the memoir. I believe that one of Galois's contributions in the memoir, and the one on which all the rest are based, was his description of a computational way—a computational way that is normally impossibly long—in which the roots of a given polynomial can be computed with, even though, ironically, his whole treatment is based on the tacit assumption that such computations are possible in the first place.

But this is not such a serious logical flaw as it might at first seem, because he could justly claim that *if it is possible to do computations with the roots of a polynomial, then the methods he describes show how those computations must be done.* He can leave to others the logical niceties of showing that the method does in fact work. He has done something more practical (if that word can be used in connection with a theory of impractical computations): He has examined the consequences of those calculations and determined what they say about the solution of algebraic equations. So let me leave aside foundational questions, as Galois did, and proceed on the assumption that there is some way to compute with the roots of a given polynomial.

I will take for granted his really easy Lemma 1, which states simply that an irreducible polynomial can have a root in common with another polynomial only if it divides that other polynomial. This is a consequence of the algorithm for computing the greatest common divisor of two given polynomials, which was common knowledge at the time.

Lemma 2 is much more interesting and bears careful examination. Once again, it states that integers A, B, C, $\dots$ can be chosen in such a way that $V = Aa + Bb + Cc + \cdots$ takes on $m!$ distinct values when the roots a, b, c, $\dots$ of $f(x)$ are inserted in V in all $m!$ possible ways. The proof of this lemma involves the following impossibly long but easily imaginable computation.

At first, let the capital letters A, B, C, $\dots$ be regarded as unknowns, even though they will eventually be integers. Then $V = Aa + Bb + Cc + \cdots$ is a linear polynomial in these unknowns whose coefficients are the roots of the given polynomial. There are $m!$ such linear polynomials $V = Aa + Bb + Cc + \cdots$, one for each ordering of the roots. The difference of any two of them is another linear polynomial in A, B, C, $\dots$ whose coefficients are m *differences* of two of the roots. One must of course assume, as Galois does, that the given polynomial has distinct roots. Then all $m!(m! - 1)$ of these differences of two V's are nonzero linear polynomials in A, B, C, $\dots$. Consider now the product of these differences. It is a polynomial of degree $m!(m! - 1)$ in A, B, C, $\dots$ whose coefficients are polynomials in the roots of $f(x)$. It is not zero, because the factors are all nonzero. Now the coefficients of this gigantic polynomial (if $m = 5$ its degree is 14,280) in A, B, C, $\dots$ are polynomials in the roots, which, by assumption, we know how to compute with. However, they are not *arbitrary* polynomials in the roots but *symmetric* polynomials; as was well known and understood long before Galois's time, the value of any symmetric polynomial in the roots of a given polynomial can be expressed as a polynomial in the *coefficients,* so our assumption that $f(x)$ has integer coefficients implies that the gigantic polynomial in

A, B, C, $\ldots$ is a nonzero polynomial with *integer* coefficients. Therefore, as follows from very elementary considerations, one can assign integer values to the unknowns A, B, C, $\ldots$ that give the polynomial a nonzero value. The use of these integer values for A, B, C, $\ldots$ in V gives a V with the required property that no two values in which the roots are inserted in different orders are equal and Lemma 2 is proved.

(On a more practical plane, since the sets of values of A, B, C, $\ldots$ for which the gigantic polynomial is zero are a set of lower dimension, it is clear that if you just randomly assign integer values to them, you would have to be very unlucky for the resulting V *not* to have the desired property.)

I would like you to reflect on the metaphysics of this argument. We don't really know what the roots a, b, c, $\ldots$ of $f(x)$ are, or how to compute with them, but if we did know what they were and we did know how to compute with them, we would be able to form what I have called the gigantic polynomial and would be able, if we were patient enough, to carry out the required construction. So *if* computations in the roots can be made to make sense, the lemma is true and, what is more, we don't need to *do* any computations with the roots, all we need to do is express symmetric polynomials in the roots of $f(x)$ as polynomials in the coefficients of $f(x)$. Note too that we still don't know what V is or how to compute with it, other than as a formal linear combination of the roots of $f(x)$.

Why should we care whether such a V can be found? In other words, why does Galois put forward Lemma 2? Because V is the whole key. In Galois's language, V has the amazing property that *each of the roots of $f(x)$ can be expressed rationally in terms of V.* This is Lemma 3. Note that, as a consequence, *all* values of V can be expressed rationally in terms of *any one* of them.

Lemma 3, the statement that the roots of $f(x)$ can be expressed rationally in terms of V is proved, of course, by a computation. The argument is subtle and it took me a long time to be sure of it. But now, at last, it appears very clear to me, and I hope it will be clear to you when I explain how I now see it.

The essential idea of the proof is that the elementary symmetric polynomials in the roots b, c, $\ldots$ of $f(x)$ other than a can be expressed as polynomials in a. You may well be familiar with this theorem about symmetric polynomials. It follows from the equation

$$(x-b)(x-c)\cdots = \frac{f(x)}{x-a}$$

in which the coefficients on the left are the elementary symmetric polynomials in b, c, $\ldots$ and the coefficients on the right are polynomials in a by virtue of the remainder theorem.

Now consider the product of the $(m-1)!$ quantities $X - V$, where X is an unknown and where V ranges over those V's in which a remains in the first position while the remaining roots are permuted in all $(m-1)!$ ways. This is a polynomial of degree $(m-1)!$ in X whose coefficients are polynomials in a, b, c, $\ldots$. But, since it is symmetric in b, c, $\ldots$, and, since the elementary symmetric functions in these roots can be expressed as polynomials in a, this product can be written as $F(X, a)$, where $F(X, Y)$ is a polynomial in two variables with integer coefficients.

Clearly $F(V, a) = 0$ because it is a product in which one of the factors is $V - Aa - Bb - Cc - \cdots$, which is zero.

Let $G(X) = \prod(X - V)$ be the product of $X - V$ over all $m!$ values of V. Then clearly $G(X) = F(X, a)F(X, b)F(X, c)\cdots$ when use is made of the fact that the right hand side is symmetric in the roots of $f(x)$ and is therefore a polynomial in X with integer coefficients. Since V was chosen in such a way that V would be a simple root of $G(X)$, and since it is a root of $F(X, a)$, it cannot be a root of $F(X, b)$ for any root b of $f(x)$ other than a.

That is the hard part of the proof of Lemma 3. The fact that $F(V, a) = 0$ while $F(V, b) \neq 0$ for all other roots b of $f(x)$, means that a is a root of the greatest common divisor of the two polynomials $F(V, x)$ and $f(x)$ and is the *only* root of this greatest common divisor. But the determination of the greatest common divisor of two polynomials is a basic algebraic operation that results in a polynomial whose coefficients are rational functions of the coefficients of the given polynomials. In the case at hand, the result is a polynomial of degree one, with the single root a, whose coefficients are rational in V. In short, $\beta a + \gamma = 0$ where β and γ are rational functions of V, so a itself is $-\gamma/\beta$, a rational function of V.

Since a was an arbitrary root of $f(x)$, this means that *all roots of $f(x)$ can be expressed rationally in terms of V.* So the central problem I spoke about before, "How can you compute with the roots of $f(x)$?" is reduced to the problem, "How can you compute with V?" Ah, but this has an easy answer from basic polynomial algebra. Since V is a root of the polynomial $G(X)$ of degree $m!$ with integer coefficients, it is a root of one of the *irreducible factors* of this polynomial with integer coefficients, call that factor $G_0(X)$. And computation with a *single* root of an *irreducible* polynomial with integer coefficients is easy. This is a simple algebraic extension of the rationals, or, to put it another way, it is the field which is the quotient of the integral domain $\mathbf{Q}[x]$ (polynomials in x with rational coefficients) with respect to a prime ideal, namely, the ideal generated by the irreducible polynomial $G_0(X)$ of which V is a root. Operationally, it just means that you compute with polynomials in V with rational coefficients, using the relation $G_0(V) = 0$ to reduce the degree whenever it goes above the degree of $G_0(X)$, and doing division by rationalizing the denominator.

To summarize, in the preliminary lemmas leading up to his Propositions 1 and 2, Galois establishes (at least he established it for himself, even though he didn't give the reader a lot of help in following his argument) that for any given $f(x)$ one can find an irreducible polynomial $G_0(X)$ with integer coefficients that has the property that the field obtained by adjoining one root V of $G_0(X)$ to $\mathbf{Q}$ constructs a field in which $f(x)$ has n roots. In short, he has sketched a construction of what is now called the splitting field of $f(x)$.

A casual reading of Proposition 1 gives the modern reader—or at any rate gave me when I read it for the first time many years ago—a false feeling of familiarity and understanding. It sounds very much like the modern definition of the Galois group as the group of automorphisms of the splitting field of $f(x)$ that leave the constants unmoved. But that reading of it brings to the proposition the entire modern culture of abstract set theory, group theory, and field theory that are, in my opinion, much less concrete than the conception of the matter that Galois intended to convey in Proposition 1.

As I said at the outset, I don't at all understand how Galois justified or understood computations with the roots of $f(x)$ at a foundational level, but his proof of Proposition 1 indicates clearly that he was in fact computing with rational functions of V making use of the irreducible polynomial of degree n of which V is a root. In particular, the second part of his proof of Proposition 1 makes clear that what he meant when he said that a rational function of the roots had a value that could be determined rationally was that when it was expressed as a polynomial in V of degree less than the degree n of $G_0(X)$ it became a polynomial of degree zero, i.e., a rational number. In short, he was making use of $\mathbf{Q}[V]$ mod $G_0(V)$ as a splitting field of $f(x)$.

Proposition 1 indeed describes a particular "group of permutations" of the roots of $f(x)$ by characterizing it in terms of the way that it acts on rational functions of the roots, but the detailed explanation of this characterization runs into problems. First, since the word "group" had no place in the mathematical vocabulary at the time, it must be interpreted in a non-technical way, and it is far from clear how Galois meant for us to understand it. Second, Galois seems always to have struggled unsuccessfully to use the words "permutations" and "substitutions" in different and consistent ways. It is not at all clear when he uses the word "permutation" here whether he means the operation of permuting or whether he means simply an arrangement in a certain order. Finally, and most problematically, it is far from clear in what way substitutions of the roots act on rational functions of the roots. A rational function of the roots can be represented in many different ways—the essence of "computing with the roots" lies in being able to determine when two rational functions of the roots are *equal* when they are not *identical*—so one can't say that you just perform the substitution of the roots in the rational function because that could depend on the choice of the particular representation of the rational function that you chose to use.

But there is a simple way out of these quandaries. At the conclusion of his proof of Proposition 1, Galois says "this group has ... the required properties," so in the course of the proof he has *specified* what he means by this group, and it is in fact a very clearly described $n \times m$ array, where n is the degree of $G_0(X)$ and m is the degree of $f(x)$. The entries are roots of $f(x)$, and each row of the array contains each root of $f(x)$ exactly once. In other words, in a completely colloquial way, the $n \times m$ array is a group of n permutations of the m roots of $f(x)$.

The interpretation of the $n \times m$ array depends on Lemma 4, which states that if $\phi(V)$ is a root of $f(x)$ in $\mathbf{Q}[V]$ mod $G_0(V)$, and if V' is another root of $G_0(X)$, then $\phi(V')$ is also a root of $f(x)$ in $\mathbf{Q}[V]$ mod $G_0(V)$. This, to use our modern vocabulary, is a simple consequence of the statement that mapping V to V' is an automorphism of $\mathbf{Q}[V]$ mod $G_0(V)$, so it carries roots of $f(x)$ to roots of $f(x)$. With this lemma in mind, the way in which the explicit $n \times m$ array that Galois writes (with an $(m+1)$st column on the left to serve as captions for the rows) is, in an obvious way, a straightforward list of n permutations of the roots of $f(x)$.

Thus, Galois describes what he is going to call "the group of $f(x)$" quite explicitly. The job of Proposition 1 is to give a characterization of it that shows it is independent of the choices that were made in its construction. I certainly recognize the merit of this characterization, but I think that for a first understanding of the group of $f(x)$ it is better to stick with the following more direct interpretation of the $n \times m$ array.

The formula $V = A \cdot \phi(V) + B \cdot \phi_1(V) + C \cdot \phi_2(V) + \cdots$ shows that the order $\phi(V)$,

$\phi_1(V)$, ... , $\phi_{m-1}(V)$ of the roots of $f(x)$ in the row of the array that corresponds to V is simply the order in which they appear in V itself. Therefore, since the array describes a group of n permutations of these roots in the modern sense, it is clear that the array tells how to find all n roots of $G_0(X)$ given any one of them, just by using the group to permute the order of the roots of $f(x)$ in the given V. In other words, the array gives a recipe—I think of it as being like DNA replication—for grouping the $m!$ factors $X - V$ of $G(X)$ into sets of n each, in such a way that the product of the factors in each set is an irreducible polynomial with integer coefficients. And you don't even have to know what the integer coefficients A, B, C ... are.

Armed with this very concrete description of what Galois calls "the group of $f(x)$," as well as the precise meaning of the statement that a rational function of the roots has a rationally known value, I hope you will be able to prove Proposition 1 for yourself, once you are given some time to think about it. (You may want to look at Galois's proof, but I'm afraid it provides very limited help.) In this hope, I will go on to Proposition 2, which is the heart of the matter.

Proposition 2 addresses the all-important question: If the "known" quantities are augmented, how is the factorization of $G(X)$ into factors that are irreducible *in the new sense* affected? Specifically, do factors that were irreducible become reducible, and if so in what way? This is the crucial step in the process of solving an equation by radicals, or, to put it in modern terms, the process of constructing the splitting field of a given $f(x)$ using radicals alone. You adjoin new quantities—preferably radicals—one by one to increase the known quantities at your disposal, and you hope to be able to do it in such a way that the roots themselves become known—that is, in such a way that $G(X)$ becomes a product of *linear* factors so that all values of V, and with them all values of the roots, become known quantities. In terms of the $n \times m$ array, this means that n is reduced to 1. So it is of the essence to know how—and whether—the adjunction of a new constant reduces the number of rows in the $n \times m$ array that is the group of $f(x)$.

Just as the factorization of $G(X)$ into factors that are irreducible over the integers is described by Galois's $n \times m$ array, its factorization over the expanded domain of "known" quantities is described by an $n' \times m$ array, where n' is the degree of the new irreducible factors of $G(X)$—which you hope will be less than n and which is in any case a factor of n. How is this $n' \times m$ array found?

To simplify its description, I am going to alter the statement of Proposition 2 somewhat, by changing the question it answers from "how does the adjunction of a new quantity alter the group of $f(x)$?" to "how does the adjunction of *one particular root of* $f(x)$ alter the group of $f(x)$?" Since $f(x)$ is not required to be irreducible, this added assumption on the quantity to be adjoined involves no loss of generality. In my opinion, this alteration of Galois's statement of Proposition 2 stays pretty close to his conception of the matter, as evidenced by his hint in the Scholium preceding Proposition 2, that more roots might be added to $f(x)$, and by the indication that he gives of a proof of the proposition, which deals directly with the factorization of the polynomial I have been calling $G_0(X)$. But even if it does not accurately describe Galois's exact approach, it is an alteration worth making for the sake of explaining Proposition 2 more simply.

Neither the order of the rows nor the order of the columns is important to the meaning of the $n \times m$ array, so there is no loss of generality in assuming that a is the first entry in the first row or that all the rows whose first entries are a follow it before any rows with other first entries are listed. Then Proposition 2 states simply that when the "rationally known" quantities are extended to include not just rational numbers but all quantities that are expressible as rational functions of a, then the new "group of $f(x)$" that characterizes the "rationally known" quantities is reduced to the $n' \times m$ array that remains after all rows that do not have a in the first column are dropped.

Furthermore, the same is true for any other $a^{(i)}$ that occurs in the first column. Each of these roots of $f(x)$—they are the roots of the irreducible factor of $f(x)$ over the integers of which a is a root—determines an $n' \times m$ array. Therefore, $n = kn'$ where k is the number of different entries in the first column. Galois notes that not only are these $n' \times m$ arrays all the same size, but, as he expresses it, one passes from one of these arrays to another by a single substitution of letters.

As always, Galois's indication of a proof of Proposition 2 is scant. I propose the following reconstruction. Recall that $F(X, Y)$ is a polynomial with integer coefficients for which $F(V, a) = 0$. The statement that n' of the rows have a as their first entry implies that n' of the n roots of $G_0(X)$ are roots of $F(X, a)$. In other words, the greatest common divisor of $G_0(X)$ and $F(X, a)$, which is a polynomial whose coefficients are rational in a, has as its roots precisely those V's that correspond to rows that start with a. Let $H(X, a)$ denote this greatest common divisor. On the other hand, a is a root of an irreducible polynomial with integer coefficients of degree k, where $k = n/n'$ is the number of distinct entries in the first column. Again, this polynomial is irreducible over $\mathbf{Q}$ by virtue of Proposition 1, as is easy to see. Therefore, V can be adjoined to $\mathbf{Q}$ in two steps: First adjoin a, an extension of degree k, and then adjoin a root of $H(X, a)$. Since this extension is of degree $n = n'k$ and the first step is of degree k, it follows that the second step is of degree n', which means that $H(X, a)$ must be irreducible over $\mathbf{Q}(a)$. Computations in this extension field—over which both $f(x)$ and $G(X)$ split into linear factors—easily prove Proposition 2, i.e., that the $n' \times m$ array is the group of $f(x)$ when the known quantities are $\mathbf{Q}(a)$, and that the k arrays corresponding to the k values of a differ from one another by a single substitution of letters.

In this way, as early as Proposition 2 of the *Premier Mémoire,* we have arrived at what is usually called the fundamental theorem of Galois theory. Well, not quite, but near enough. Specifically, given a root a of a polynomial $f(x)$, we have found a necessary and sufficient condition for a rational function of the roots of $f(x)$ to be rationally expressible in terms of a alone, namely: It must be left fixed by all substitutions of the group of $f(x)$ that leave a fixed.

To put this in more general, and more modern, terms, given any normal algebraic extension K of $\mathbf{Q}$, Galois has described a group of automorphisms of K with the property that a quantity b in K can be expressed rationally in terms of another quantity a in K if and only if b is unmoved by all of the automorphisms that leave a unmoved. You just have to choose a monic polynomial $f(x)$ with integer coefficients whose splitting field is K; the $n \times m$ array described by Galois describes explicitly the needed group of n automorphisms of K. (To apply the form of Proposition 2 that has been proved, which assumes that a is a root of $f(x)$, one only needs to replace $f(x)$, if necessary, with $f(x)g(x)$ where $g(x)$ is the irreducible polynomial of which a is a root, which makes the $n \times m$ array wider, but changes nothing else.) It should be noted, by the way, that Galois's substitutions of the roots are much more specific and concrete and constructive than the transfinite notion of an automorphism of K.

What is usually called the fundamental theorem of Galois theory states that the subfields of a normal extension correspond one-to-one to subgroups of the Galois group, with larger extensions corresponding to smaller subgroups. (For the sake of simplicity, I have dealt only with extensions of the rational field $\mathbf{Q}$, but Galois's setting, and his reasoning, include much more general ground fields.) As I have stated Proposition 2, it applies only to extensions of the ground field that are obtained by adjoining a single quantity a, but the more general case can be proved without much more effort, so the only part of the fundamental theorem of Galois theory that is missing is the assertion that normal extensions correspond to normal subgroups, but I think you will agree that that part of the theorem is icing on the cake. (I have omitted it, but Galois did not; see his Proposition 3.)

But of course Galois was not out to discover and prove the fundamental theorem of Galois theory, he was out to answer questions about the solution of algebraic equations. So he didn't stop with Proposition 2 but went on to *apply* his ideas to the solution of algebraic equations. While I admit that his proofs fall a bit short, I say that he is rather too terse than too vague, and that his proofs, when he bothers to give them, are indeed proofs. Had he only lived and been challenged to explain his ideas more fully, I have no doubt that he could have given a complete, constructive proof of this theorem as well as of the others in the memoir. While the theorem about solutions by radicals with which he concludes the *Premier Mémoire* seems a little strange to modern readers, I think that both its statement and its proof are under-appreciated today.

The theorem states that an irreducible polynomial of prime degree is solvable by radicals if and only if *all* of its roots can be expressed rationally in terms of just *two* of them. What I admire about the statement of the theorem is that it doesn't depend on any technical explanations about group theory. If you know what it means for an equation to be solvable by radicals, you know far more than enough to understand what it means to say that all roots can be expressed rationally in terms of any two of them. And although this theorem might appear to cover only a peculiar special case of solvability by radicals, the fact is that in the lead-up to it he has—as promised—explained what computations must be done to determine whether any given $f(x)$ is solvable by radicals, but these computations do involve technicalities of group theory.

As for his proof, I think it deserves a place in courses in Galois theory that it seldom has. The standard treatment of the unsolvability of the quintic depends on proving that A_5 is a simple group. This means that one is starting with the Galois group of the original polynomial and analyzing it. Galois comes at it from the opposite end. Once the equation is solved by radical adjunctions, its group has been reduced to the trivial group with one element. Galois asks, what about the next-to-last step? He shows that just before it is reduced to the trivial group the group must be cyclic of order p, where p is the prime degree. In other words, the roots q_1, q_2, $\ldots$, q_p can be ordered in such a way that the substitutions of the group are generated by the single substitution $q_i \mapsto q_{i+1}$, where, of course, subscripts on the roots are considered to be integers mod p. He then shows, in a completely straightforward way, that each earlier subgroup in the sequence of groups in the reduction by adjunction of radicals can *only* contain substitutions of the form $q_i \mapsto q_{ai+b}$. His theorem then follows from the fact that such substitutions can leave at most one root fixed unless they leave them all fixed.

In conclusion, I would like to say how pleased and grateful I am to have been invited to participate in this homage to the genius of Évariste Galois on his bicentennial. Without wanting in any way to disparage my own book on Galois theory, published in 1984, I will say that the part of my book that was its greatest contribution, and to which I refer most often myself, is the English translation of Galois's *Premier Mémoire* that is in Appendix 1. As I have tried to explain in this talk, Galois's own exposition offers in many ways the most insightful one of what *we* call, and future generations will certainly continue to call, Galois theory.