APPENDIX 1

Memoir on the Conditions for Solvability of Equations by Radicals

by Evariste Galois

Translated by Harold M. Edwards

PRINCIPLES

I shall begin by establishing some definitions and a sequence of lemmas, all of which are known.

Definitions. An equation is said to be reducible if it admits rational divisors; otherwise it is irreducible.

It is necessary to explain what is meant by the word rational, because it will appear frequently.

When the equation has coefficients that are all numeric and rational, this means simply that the equation can be decomposed into factors which have coefficients that are numeric and rational.

But when the coefficients of an equation are not *all* numeric and rational, one must mean by a rational divisor a divisor whose coefficients can be expressed as rational functions of the coefficients of the proposed equation, and, more generally, by a rational quantity a quantity that can be expressed as a rational function of the coefficients of the proposed equation.

More than this: one can agree to regard as rational all rational functions of a certain number of determined quantities, supposed to be known *a priori.* For example, one can choose a particular root of a whole number and regard as rational every rational function of this radical.

When we agree to regard certain quantities as known in this manner, we shall say that we *adjoin* them to the equation to be resolved. We shall say that these quantities are *adjoined* to the equation.

With these conventions, we shall call *rational* any quantity which can be expressed as a rational function of the coefficients of the equation and of a certain number of *adjoined* quantities arbitrarily agreed upon.

When we make use of auxiliary equations, they will be rational if their coefficients are rational in our sense.

One sees, moreover, that the properties and the difficulties of an equation can be altogether different, depending on what quantities are adjoined to it. For example, the adjunction of a quantity can render an irreducible equation reducible.

Thus, when one adjoins to the equation

$$\frac{x^n - 1}{x - 1} = 0, \quad \text{where } n \text{ is prime,}$$

a root of one of Mr. Gauss's auxiliary equations, this equation decomposes into factors, and consequently becomes reducible.

Substitutions are the passage from one permutation to another.

The initial permutation one uses to describe substitutions is entirely arbitrary when one is dealing with functions, because there is no reason, in a function of several letters, for a letter to occupy one position rather than another.

Nonetheless, since one can hardly comprehend the idea of a substitution without that of a permutation, we shall frequently speak of permutations, and we shall consider substitutions only as the passage from one permutation to another.

When we want to group substitutions we shall make them all proceed from the same permutation.

As it is always a question of problems in which the initial distribution of the letters is immaterial, in the groups which we consider one should have the same substitutions no matter which permutation one starts from. Thus if the substitutions S and T are in such a group, one is certain of having the substitution ST.

These are the definitions that we thought we should recall.

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

Because the greatest common divisor of the given irreducible equation and the other equation will also be rational; therefore, etc.

LEMMA II. Given any equation with distinct roots $a, b, c, \ldots$, one can always form a function V of the roots such that no two of the values one obtains by permuting the roots in this function are equal.

For example, one can take

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

$A, B, C, \ldots$ being suitably chosen whole numbers.

LEMMA III. When the function V is chosen as indicated above, it will have the property that all the roots of the given equation can be expressed as rational functions of V.

In fact,* let

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

or

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

Let us multiply together all the similar equations which one obtains by permuting in these all the letters, leaving just the first one fixed; this will give the following expression:

$$(V - \phi(a, b, c, d, \ldots))(V - \phi(a, c, b, d, \ldots))(V - \phi(a, b, d, f, c, \ldots))\ldots,$$

which is symmetric in b, c, d, etc., . . . , and which can consequently be written as a function of a. We will therefore have an equation of the form

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

But I say that one can extract from this the value of a. For this it suffices to look for the common solution of this equation and the given one: for one cannot have, for example,

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

unless (this equation having a common factor with the similar equation) one of the functions $\phi(a, \ldots)$ is equal to one of the functions $\phi(b, \ldots)$; which is contrary to the hypothesis.

It therefore follows that a can be expressed as a rational function of V, and it is the same for the other roots.

This proposition† is stated without demonstration by Abel in his posthumous memoir on elliptic functions.‡

* We have transcribed word-for-word the demonstration that we gave of this lemma in a memoir presented in 1830. We attach as an historical document the following note which M. Poisson felt he needed to make upon it.

"The demonstration of this lemma is insufficient; however, it is true according to n° 100 of the memoir of Lagrange, Berlin, 1771."

On jugera. (Author's note.)

† It is remarkable that one can conclude from this proposition that every equation depends on an auxiliary equation with the property that all the roots of this new equation are rational functions of one another. For the auxiliary equation for V is of this type.

Moreover, this remark is a mere curiosity; in fact, an equation which has this property is not in general any easier to solve than any other. (Author's note.)

‡ This appears to be a reference to §1 of Chapter 2 of Abel's "Précis d'une théorie des fonctions elliptiques" [A2, p. 547]. Elsewhere [G1, p. 35] Galois says "It would be easy for me to prove that I was unaware even of the name of Abel when I presented my first researches on the theory of equations to the Institute, and that Abel's solution could not have appeared before mine." (Translator's note.)

LEMMA IV. Suppose one has formed the equation for V, and that one has taken one of its irreducible factors, so that V is the root of an irreducible equation. Let V, V', V'', ... be the roots of this irreducible equation. If $a = f(V)$ is one of the roots of the given equation, $f(V')$ will also be a root of the given equation.

In fact, in multiplying together all the factors of the form $V - \phi(a, b, c, \ldots, d)$ in which one applies to the letters all possible permutations, one obtains a rational equation which is necessarily divisible by the equation in question; therefore V' can be obtained by an exchange of letters in the function V. Let $F(V, a) = 0$ be the equation that one obtains in permuting in V all the letters except the first; then one will have $F(V', b) = 0$, where b may be equal to a, but is certainly one of the roots of the given equation. Consequently, just as the given equation and $F(V, a) = 0$ combine to give $a = f(V)$, the given equation and $F(V', b) = 0$ combine to give $b = f(V')$.

With these principles set forth, we shall proceed to the exposition of our theory.

PROPOSITION I

Theorem. Let an equation be given whose m roots are $a, b, c, \ldots$. There will always be a group of permutations of the letters $a, b, c, \ldots$ which will have the following property:

1. that each function invariant* under the substitutions of this group will be known rationally;
2. conversely, that every function of the roots which can be determined rationally will be invariant under these substitutions.

(In the case of algebraic equations, this group is none other than the set of all $1 \cdot 2 \cdot 3 \ldots m$ permutations of the m letters, because in this case the symmetric functions are the only ones that can be determined rationally.)

(In the case of the equation $(x^n - 1)/(x - 1) = 0$, if one supposes that

* Here we call a function invariant not only if its form is unchanged by the substitutions of the roots, but also if its numerical value does not vary when these substitutions are applied. For example, if $Fx = 0$ is an equation, Fx is a function of the roots which is not changed by any substitution.

When we say that a function is rationally known, we mean that its numerical value can be expressed as a rational function of the coefficients of the equation and the quantities that have been adjoined. (Author's note.)

$a = r, b = r^g, c = r^{g^2}, \ldots$, g being a primitive root, the group of permutations will be simply this one:

$$abcd \ldots k,$$
$$bcd \ldots ka,$$
$$cd \ldots kab,$$
$$\ldots\ldots\ldots$$
$$kabc \ldots i \quad \text{[sic; } i \text{ precedes } k\text{]}.$$

In this particular case, the number of permutations is equal to the degree of the equation, and the same will be true for equations all of whose roots are rational functions of one another.)

DEMONSTRATION. No matter what the given equation is, one can find a rational function V of the roots such that all the roots are rational functions of V. With such a V, let us consider the irreducible equation of which V is a root (Lemmas III and IV). Let $V, V', V'', \ldots, V^{(n-1)}$ be the roots of this equation.

Let $\phi V, \phi_1 V, \phi_2 V, \ldots, \phi_{m-1} V$ be the roots of the given equation.

Let us write the following n permutations of the roots:

$$\begin{array}{llllll}
(V), & \phi V, & \phi_1 V, & \phi_2 V, & \ldots, & \phi_{m-1} V, \\
(V'), & \phi V', & \phi_1 V', & \phi_2 V', & \ldots, & \ldots, \\
(V''), & \phi V'', & \phi_1 V'', & \phi_2 V'', & \ldots, & \ldots, \\
\ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\
(V^{(n-1)}), & \phi V^{(n-1)}, & \phi_1 V^{(n-1)}, & \phi_2 V^{(n-1)}, & \ldots, & \phi_{m-1} V^{(n-1)}.
\end{array}$$

I say that this group of permutations has the stated property.

In fact:

1. Every function F of the roots invariant under the substitutions of this group can be written as $F = \psi V$, and one will have
$$\psi V = \psi V' = \psi V'' = \cdots = \psi V^{(n-1)}.$$
The value of F can therefore be determined rationally.
2. Conversely, if a function F is determinable rationally, and if one sets $F = \psi V$, one will have
$$\psi V = \psi V' = \psi V'' = \cdots = \psi V^{(n-1)},$$
because the equation for V has no commensurable divisor and V satisfies the rational equation $F = \psi V$, F being a rational quantity. Therefore the function F will necessarily be invariant under the substitutions of the group written above.

Thus, this group has the double property given in the theorem. The theorem is therefore demonstrated.

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

SCHOLIUM. Clearly in the group of permutations under discussion the disposition of the letters is of no importance, but only the *substitutions* of the letters by which one passes from one permutation to the other.

Thus one can give a first permutation arbitrarily, provided the other permutations are always deduced from it using the same substitutions of the letters. The new group formed in this way will obviously have the same properties as the first, because in the preceding theorem all that matters is the substitutions which one can make in the functions.

SCHOLIUM. The substitutions are independent even of the number of roots.

PROPOSITION II

Theorem. If one adjoins to a given equation the root r of an auxiliary irreducible 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 to the given equation respectively when one adjoins each of the roots of the auxiliary equation;
(2) these groups will have the remarkable property that one will pass from one to the other in applying the same substitution of letters to all the permutations of the first.

(1)† If, after the adjunction of r, the equation for V mentioned above remains irreducible, it is clear that the group of the equation will not be changed. If, on the other hand, it can be reduced, then the equation for V decomposes into p factors, all of the same degree and of the form

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

$r, r', r'', \ldots$ being the other values of r. Thus the group of the given equation also decomposes into groups, each containing the same number of permutations, because each value of V corresponds to a permutation. These groups are, respectively, those of the given equation when one adjoins successively $r, r', r'', \ldots$.

* The original version included the words "of prime degree p" which Galois later struck out, perhaps the night before the duel. Thus the letter p, which occurs in the statement of property (1), is intended to be the degree of the auxiliary equation. For the correct statement of the proposition, it should be modified to say that "the group will be partitioned into j 'groups' where j divides p." If p is prime then the partition is into 1 "group" or p. (Translator's note.)

† There is something that needs completing in this demonstration. I haven't the time. (Author's note.)

(2) We saw above that the values of V were all rational functions of one another. In view of this, let V be a root of $f(V, r) = 0$, and $F(V)$ another. It is then clear that if V' is a root of $f(V, r') = 0$, $F(V')$ will be another.*

With this stated, I say that one obtains the group relative to r' by applying the same substitution of letters throughout to the group relative to r.

In fact, if one has, for example,

$$\phi_p F(V) = \phi_n V,$$

one will also have (Lemma I),

$$\phi_p F(V') = \phi_n V'.$$

Therefore, in order to pass from the permutation $(F(V))$ to the permutation $(F(V'))$ one must make the same substitution as one must in order to pass from the permutation (V) to the permutation (V').

The theorem is therefore demonstrated.

(1832. PROPOSITION III

Theorem. If one adjoins to an equation *all* the roots of an auxiliary equation, the groups in Theorem II will have the further property that each group contains the same substitutions.

One will find the proof.†)

PROPOSITION IV

Theorem. If one adjoins to an equation the *numerical* value of a certain function of its roots, the group of the equation will be reduced in such a way as to contain no permutations other than those which leave this function invariant.

In fact, by Proposition I, every known function must be invariant under the permutations of the group of the equation.

* Because one will have $f(F(V), r)$ = a function divisible by $f(V, r)$. Therefore (Lemma I) $f(F(V), r')$ = a function divisible by $f(V, r')$. (Author's note.)

† This is a revision made in 1832. The original version was:

PROPOSITION III

THEOREM. If the equation for r has the form $r^p = A$, and if the pth roots of unity have already been adjoined, the p groups of Theorem II will have the further property that the substitutions of letters by which one passes from one permutation to another in each group are the same for all the groups.

In fact, in this case it does not matter which value of r one adjoins to the equation. Consequently, its properties must be the same after the adjunction of any value of r whatever. Thus its group must be the same as far as the substitutions are concerned (Proposition 1, Scholium). Therefore, etc. (Translator's note.)

PROPOSITION V

PROBLEM. In which case is an equation solvable by simple radicals?

I shall observe first that in order to solve an equation it is necessary to reduce its group successively until it contains only one permutation. For, when an equation is solved, any function whatever of its roots is known, even when it is not invariant under any permutation.

With this set forth, let us try to find the condition which the group of an equation should satisfy in order that it can be thus reduced by the adjunction of radical quantities.

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

Adjoin to the equation the first radical to be extracted in the solution. One of two things can happen: either by the adjunction of this radical the group of permutations of the equation will be diminished, or, this extraction of a root being only a preparation, the group will remain the same.

In any case, after a certain *finite* number of extractions of roots the group must find itself diminished because otherwise the equation would not be solvable.

If at this point it occurs that there are several ways to diminish the group of the given equation by the simple extraction of a root, it is necessary, in what we are going to say, to consider only a radical of the least possible degree among all the simple radicals which are such that the knowledge of each of them diminishes the group of the equation.

Therefore let p be the prime number which represents this minimum degree such that the extraction of a root of degree p diminishes the group of the equation.

We can always suppose, at least in relation to the group of the equation, that a pth root of unity α is included among the quantities that have already been adjoined to the equation. For, since this expression can be obtained by extractions of roots of degree less than p, its knowledge does not alter in any way the group of the equation.

Consequently, according to Theorems II and III, the group of the equation should decompose into p groups having in relation to one another this double property:

(1) that one passes from one to the other by one single substitution;
(2) that they all contain the same substitutions.

I say that, conversely, if the group of the equation can be partitioned into p groups which have this double property, one can, by a simple extraction of a pth root, and by the adjunction of this pth root, reduce the group of the equation to one of these partial groups.

Let us take, in fact, a function of the roots which is invariant under all substitutions of one of the partial groups, and does not vary [sic] for any other substitution.*

Let θ be this function of the roots.

Let us apply to the function θ one of the substitutions of the total group which it does not have in common with the partial groups. Let θ_1 be the result. Apply the same substitution to θ_1 and let θ_2 be the result, and so forth.

Since p is a prime number, this sequence can end only with the term θ_{p-1}, after which one will have $\theta_p = \theta$, $\theta_{p+1} = \theta_1$, and so forth.

In view of this, it is clear that the function

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

will be invariant under all the permutations of the total group, and consequently will now be known.

If one extracts the pth root of this function and adjoins it to the equation, then by Proposition IV the group will no longer contain any substitution other than those of the partial groups.

Thus, in order for it to be possible to reduce the group of an equation by simple extraction of a root, the condition stated above is necessary and sufficient.

Let us adjoin to the equation the radical in question; we can now reason with respect to the new group as with respect to the preceding one, and it must be possible to decompose it too in the manner indicated, and so forth, until a group is reached which contains only one permutation.

SCHOLIUM. It is easy to observe this process in the known solution of general equations of the fourth degree. In fact, these equations are resolved by means of an equation of the third degree, which itself requires the extraction of a square root. In the natural sequence of ideas, it is therefore with this square root that one must begin. But in adjoining this square root to the equation of fourth degree, the group of the equation, which contains twenty-four substitutions in all, is decomposed into two which contain only twelve. When the roots are designated by a b c d here is one of these groups:

abcd	*acdb*	*adbc*
badc	*cabd*	*dacb*
cdab	*dbac*	*bcad*
dcba	*bdca*	*cbda*

* For this it suffices to choose a symmetric function of the various values assumed by a function invariant under no substitutions when it is subjected to the permutations of one of the partial groups. (Author's note.)

Now this group itself splits into three groups, as is indicated in Theorems II and III. Thus, after the extraction of a single radical of third degree just the group

$$abcd$$

$$badc$$

$$cdab$$

$$dcba$$

remains, and this group again splits into two groups

$$abcd \qquad cdab$$

$$badc \qquad dcba.$$

Thus, after a simple extraction of a square root,

$$abcd$$

$$badc$$

remains, which will be resolved, finally, by a simple extraction of a square root.

One obtains in this way either the solution of Descartes or that of Euler. For even though the latter extracts three square roots after the solution of the auxiliary equation of third degree, it is well known that two suffice, because the third can then be derived rationally.

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

APPLICATION TO IRREDUCIBLE EQUATIONS OF PRIME DEGREE

PROPOSITION VI

LEMMA. An irreducible equation of prime degree cannot become reducible by the adjunction of a radical. [Sic. Galois evidently means that it cannot become reducible without being solved completely.]

For, if $r, r', r'', \ldots$ are the various values of the radical and if $Fx = 0$ is the given equation, Fx would have to split into factors

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

all of the same degree, which is impossible, at least unless $f(x, r)$ is of the first degree in r. [x]

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

PROPOSITION VII

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

By the preceding proposition, the smallest group possible before the one which contains only a single permutation will contain p permutations. But a group of permutations of a prime number n of letters cannot contain just n permutations unless each of these permutations can be derived from any other by a cyclic substitution of order n (see the memoir of Mr. Cauchy, *Journal de l'Ecole*, **17**).

Thus the next-to-the-last group will be of the form

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

$x_0, x_1, x_2, \dots, x_{n-1}$ being the roots.

Now the group which immediately precedes this one in the sequence of the decompositions must be made up of a certain number of groups having all the same substitutions as this one. But I observe that these substitutions can be expressed as follows: (Let us set $x_n = x_0$, $x_{n+1} = x_1, \dots$. It is clear that each of the substitutions of the group (G) can be obtained by putting x_{k+c} in place of x_k throughout, c being a constant.)

Let us consider any one of the groups similar to the group (G). According to Theorem II, it can be obtained by applying one and the same substitution throughout the group, say by putting $x_{f(k)}$ in place of x_k throughout the group (G), f being a certain function.

Since the substitutions of this new group must be the same as those of the group G, one must have

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

C being independent of k.

Therefore.

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

If $c = 1$ and $k = 0$, one finds

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

which is to say

$$fk = ak + b,$$

a and b being constants.

Therefore the group which precedes immediately the group G cannot contain any substitutions other than those of the form

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

and consequently can contain no cyclic substitutions other than those of the group G.

One can apply the same argument to this group that was applied to the preceding one, and it follows that the first group in the order of the decompositions, that is, the *actual* group of the equation cannot contain any substitutions other than those of the form

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

Therefore "if an irreducible equation of prime degree is solvable by radicals then the group of this equation can contain no substitutions other than those of the form

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

a and b being constants."

Conversely, I say that when this condition holds the equation will be solvable by radicals. In fact, consider the functions

$$(x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1})^n = X_1,$$

$$(x_0 + \alpha x_a + \alpha^2 x_{2a} + \cdots + \alpha^{n-1} x_{(n-1)a})^n = X_a,$$

$$(x_0 + \alpha x_{a^2} + \alpha^2 x_{2a^2} + \cdots + \alpha^{n-1} x_{(n-1)a^2})^n = X_{a^2},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

α being an nth root of unity and a a primitive root of n.

It is clear that in this case any function that is unchanged by cyclic substitutions of the quantities $X_1, X_a, X_{a^2}, \ldots$ will be immediately known. Therefore one can find $X_1, X_a, X_{a^2}, \ldots$ by the method of Mr. Gauss for binomial equations. Therefore, etc.

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

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

be rationally known.

Thus the function

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

must be known, no matter what X is.

It is therefore *necessary* and *sufficient* that the equation which gives this function of the roots admit, no matter what X is, a rational value.

If the given equation has rational coefficients, the auxiliary equation will also have rational coefficients as well, and it will suffice to determine whether this auxiliary equation of degree $1 \cdot 2 \cdot 3 \ldots (n-2)$ does or does not have a rational root. And one knows how to do this.

This is the method that one must use in practice. But we are going to present the theorem in a different form.

PROPOSITION VIII

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

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

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

never leaving two letters in the same place, it is clear that when two roots of the equation are adjoined, by Proposition IV, the group is reduced to a single substitution.

In the second place, it is sufficient: because in this case, no substitution of the group can leave two letters in the same place. Consequently the group will contain at the very most $n(n-1)$ permutations. Therefore it will contain only a single cyclic substitution (otherwise it would have at least p^2 [sic; should be n^2] permutations). Therefore each substitution of the group x_k, x_{fk}, must satisfy the condition

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

Therefore, etc.

The theorem is therefore demonstrated.

Example of Theorem VII

Let $n = 5$. The group will be the following one:

abcde
bcdea
cdeab
deabc
eabcd

acebd
cebda
ebdac
bdace
daceb

aedcb
edcba
dcbae
cbaed
baedc

adbec
dbeca
becad
ecadb
cadbe