Memoir on the Conditions of Solvability of Equations by Radicals

Évariste Galois

January 16, 1831

The attached memoir is extracted from a work that I had the honor of presenting to the Academy a year ago. That work not having been understood, the propositions it contained having been called into question, I have had to content myself with giving, in a synthesized way, the general principles and a *single* application of my theory. I beg my judges to read at least these few pages carefully.

One will find herein a general *condition* which *each equation solvable by radicals satisfies*, and which reciprocally assures their solvability. We apply this only to equations for which the degree is a prime number. Here is the theorem given by our analysis:

So that an equation of prime degree, which does not have commensurable divisors, should be solvable by radicals, it is necessary and sufficient that all the roots be rational functions of any two among them.

The other applications of the theory are special theories in their own right. They require, however, the use of number theory and a special algorithm: we reserve them for another occasion. They are in part related to modular equations from the theory of elliptic functions, which we show not able to be solved by radicals.

E. Galois
January 16, 1831

Principles

We begin by establishing a few definitions and a series of lemmas, all of which are well-known.

Definitions

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

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

When *all* the coefficients of an equation are numerical and rational, this simply means that the equation can be decomposed into factors whose coefficients are numerical and rational.

However, when the coefficients of an equation are not all numerical and rational, a *rational divisor* must be understood as a divisor whose coefficients can be expressed as rational functions of the proposed equation's coefficients.

Furthermore, we may agree to consider as rational any rational function of certain quantities that are determined and assumed to be known *a priori*. For example, one may choose a certain root of an integer and consider any rational function of this radical as rational.

When we agree to regard certain quantities as known in this way, we will say that we *adjoin* them to the equation that must be solved. We will say that these quantities are *adjoined* to the equation.

With this in mind, we will call *rational* any quantity that can be expressed as a rational function of the coefficients of the equation and of a certain number of quantities adjoined to the equation and chosen arbitrarily.

When we use auxiliary equations, they will be called rational if their coefficients are rational in ours.

Furthermore, we see that the properties and difficulties of an equation can be quite different depending on the quantities adjoined to it. For example, adjoining a certain quantity can render reducible an otherwise irreducible equation.

Thus, when one adjoins to the equation

$$\frac{x^n - 1}{x - 1} = 0,$$

where n is prime, a root of one of Mr. Gauss's auxiliary equations, that equation factors and therefore becomes reducible.

Substitutions are the passage from one permutation to another.

The permutation from which we start to indicate the substitutions is entirely arbitrary, when dealing with functions; for there is no reason that, in a function of several letters, one letter should occupy one position rather than another.

However, since one can hardly form the idea of a substitution without that of a permutation, we will often use permutations in language, and we will consider substitutions only as the passage from one permutation to another.

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

Since these are always questions where the original arrangement of the letters does not affect the groups we consider, we should have the same substitutions, regardless of the starting permutation.

Page 37

Lemma II. — Given any equation that has no repeated roots, whose roots are $a, b, c, \ldots$, one can always form a function V of the roots such that none of the values obtained by permuting the roots in every possible way coincide.

For example, one may take

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

where A, B, C are suitably chosen integers.

Lemma III. — The function V, chosen as indicated in the previous article, has the property that all the roots of the given equation can be expressed rationally in terms of V.

Indeed, let

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

or

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

By multiplying this equation by all the similar ones obtained by permuting its letters in every way (the first letter remaining fixed, and so on), one arrives at an expression symmetrical in $a, b, c, \ldots$, which can therefore be written in the form of an equation in a alone. In this manner, one obtains an equation of the form

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

Thus, if in such a group one has substitutions S and T, one is assured of having the substitution ST. These are the definitions we felt it necessary to recall.

Lemma I. — An irreducible equation cannot share a common root with a rational equation without dividing the latter. For the greatest common divisor between the irreducible equation and the other equation would still be rational; hence, and so forth.

Lemma II. (restated) — Being given any equation (with no repeated roots), whose roots are $a, b, c, \ldots$, one can form a function V of those roots so that none of the values obtained by permuting all the roots in every way is equal to another.

(*Repeat of the same construction:* $V = Aa + Bb + Cc + \ldots$.)

Lemma III. (restated) — Once V is chosen as indicated above, it follows that all the roots of the proposed equation can be expressed rationally in terms of V. Indeed, let

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

or

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

Let us multiply together all the similar equations obtained by permuting all of the letters (with only the first letter remaining fixed). We then arrive at the following expression:

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

which is symmetric in $b, c, d, \ldots$, and can therefore be expressed as a function of a. Hence, we obtain an equation of the form

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

Page 38

I assert that from here one can deduce the value of a. Indeed, it is enough to look for the common solution of this equation and of the original (proposed) one. Such a solution is unique, for one cannot have, for example, $F(V, b) = 0$. That would require the equation $F(V, b) = 0$ to share a common factor with the analogous equation, unless one of the functions $\phi(a, \ldots)$ were equal to one of the functions $\phi(b, \ldots)$, which contradicts our hypothesis.

It follows that a is thus expressed as a rational function of V, and the same holds for the other roots. This proposition (marked *) is cited without proof by Abel in his posthumous memoir on elliptic functions.

Lemma IV. — Suppose that one has formed the equation in V, and that one has selected an irreducible factor so that V is a root of an irreducible equation. Let $V, V', V'', \ldots$ be the roots of that irreducible equation. If $a = f(V)$ is one of the roots of the proposed equation, then $f(V')$ will also be a root of the proposed equation.

Indeed, by multiplying all factors of the form

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

while permuting all the letters, every possible permutation is necessarily accounted for by that polynomial, so that we end up dividing the given equation. Thus we arrive at the function V. Under

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

or in the equation obtained by permuting V in all letters except the first, we find

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

for some root b of the proposed equation. Hence, as soon as $a = f(V)$ (i.e. the original root) is combined with $F(V', b) = 0$, it follows that $b = f(V')$.

It is thus remarkable that from this proposition one can deduce that the entire group results from an auxiliary equation, namely one in which all of that new equation's roots are rational functions of V in the given equation. One also notices how peculiar this observation is. Indeed, a single equation with this property is in general not sufficient without a special contrivance.

Page 39
Proposition I.

Theorem. Let there be a given equation, whose roots are $a, b, c, \ldots$. There will always be a group of permutations of the letters $a, b, c, \ldots$ that enjoys the following property:

1. That any function of the roots, which is invariant under the substitutions of this group, is rationally known;
2. Conversely, that any function of the roots that is rationally determinable is invariant under those substitutions.

(In the case of algebraic equations, this group is nothing other than the set of all $1, 2, 3, \ldots, n$ permutations possible on the n letters, since in that situation, only the symmetric functions are rationally determinable.)

(If in the equation

$$\frac{x^n - 1}{x - 1} = 0$$

one assumes $a = r$, $b = r^g$, $c = r^{g^2}, \ldots$, with g being a primitive root, the group of permutations is simply

$$\begin{array}{c} abcd.....k, \\ bcd.....ka, \\ cd.....kab, \\ ..... \\ kabc.....i; \end{array}$$

In this particular example, the number of permutations is equal to the degree of the equation, just as in cases where all the roots are expressed rationally one in terms of another.)

Demonstration. — No matter what the given equation may be, one can find a rational function V of its roots (so that, for instance, the roots remain distinct under its permutations). Then the entire set of roots can be shown to be rationally dependent on V.

(We call the group of the equation the group in question.)

Remark. We do not merely want a function to remain invariant in form under those permutations, but to keep its numerical value constant under them as well. For instance, if $F = 2$ or if F is some equation, that is a function of the roots that remains the same under any permutation. We want every value that is supposed to be rationally known to be expressible as a rational function of the coefficients of the equation and the adjoined quantities.

Page 40

Therefore, consider the irreducible equation for which V is a root (Lemmas III and IV). Let $V, V', V'', \ldots, V^{(n-1)}$ be the roots of that equation. Let

$$\phi V, \phi_1 V, \ldots, \phi_{m-1} V$$

be the roots of the proposed equation. Write out the following n permutations of these roots:

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

I assert that this group of permutations possesses the stated property.

Indeed:

1° Any function F of the roots, invariant under the substitutions of this group, can be written in the form $F = \psi(V)$. Then one will have

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

and thus the value of F can be determined rationally.

2° Conversely, if a function F is rationally determinable, and if we define $F = \phi(V)$, then we must have

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

because the equation in V cannot share a common (commensurable) factor with that in V satisfying $F = \psi V$ unless it is a purely rational quantity. Therefore F is necessarily invariant under the substitutions of the group in question.

Hence, this group enjoys the twofold property stated in the theorem. The theorem is therefore proven. We shall call this group the *group of the equation* in question.

Scholium I. — It is evident that in the group of permutations of the letters under consideration, the specific arrangement of letters is not at issue; rather, one only considers the substitutions of the letters by which one passes from one permutation to another.

Page 41

Thus, one may arbitrarily choose an initial permutation, provided that the other permutations are always deduced from it by the same letter substitutions. The new group formed in this way will obviously enjoy the same properties as the first, since, in the preceding theorem, we only deal with the substitutions that may be performed in the functions.

Scolie II.

The substitutions are independent even of the number of roots.

Proposition II

Theorem (1). — If one adjoins to a given equation the root r of an irreducible auxiliary equation, then one of two things will happen: either the group of the equation remains unchanged, or else it splits into p groups, each belonging respectively to the proposed equation when one adjoins to it each of the roots of the auxiliary equation. Moreover, (2) these groups enjoy the remarkable property that one can pass from one group to another by performing, in all the permutations of the first group, the same letter substitution.

1. If, after adjoining r, the equation in V (mentioned above) remains irreducible, it is clear that the group of the equation will not be changed. If, on the contrary, it factors, then the equation in V will decompose into p factors, all of the same degree, of the form

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

where r', r'', r''', ... are other values of r. Thus, the group of the proposed equation will likewise decompose into p groups, each having the same number of letters.

Page 42

Permutations exist because each value of V corresponds to a permutation. These groups will respectively be those of the proposed equation when one adjoins successively r', r'', r''', ...

2°. We saw above that all values of V were rational functions of one another. From this, suppose that V is a root of $f(V,r) = 0$, that $F(V)$ is also a root; in the same way, if V' is a root of $f(V,r') = 0$, $F(V')$ will also be one; for one will have

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

Hence (by Lemma I)

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

This being established, I then see that one obtains the relative group i' by operating throughout in the group relative to i with the same letter substitution.

[1] In the manuscript, the statement of the theorem that has just been read appears in the margin and reads: *"In the absence of the theorem, after these words: the root of an irreducible auxiliary equation, Galois had first written this: of prime degree, which he later erased. Likewise, in the demonstration, instead of r', r'', r''', one reads other values of r. Finally, one finds in the margin of the manuscript the following note by the author: 'There is something to be completed in this demonstration: I do not have the time.' Probably, because of the same great haste in writing, it is also written further on, on page 1: 'I do not have the time,' which leads one to think that Galois reviewed his Memoir to correct it before heading out to the field of honor." (A. Ch.)*

Indeed, if one has, for example,

$$\varphi_i F(V) = \varphi_i V,$$

one still has (by Lemma I),

$$\varphi_{i'} F(V') = \varphi_{i'} V'.$$

Hence, to pass from the permutation $\big(F(V)\big)$ to the permutation $\big[F(V')\big]$, one must make the same substitution that transforms the permutation (V) into the permutation (V').

The theorem is thus proved.

Proposition III

Theorem. — If one adjoins to an equation all the roots of an auxiliary equation, the groups in question in Theorem II join together; moreover, they share the property that the substitutions are the same in each group.

We shall find the proof in (1).

Page 43

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 lowered in such a way as to have no other permutations than those for which this function is invariant.

Indeed, according to Proposition I, any known function must remain invariant under the permutations of the group of the equation.

Proposition V.

Problem. — In which cases is an equation solvable by simple radicals?

I should first observe that, to solve an equation, one must successively lower its group until it contains only a single permutation. For when an equation is solved, a certain function of its roots is known, even if it is not invariant under any permutation.

That being posited, let us search for what condition the group of the equation must satisfy so that it can be lowered in this way by adjoining radical quantities. Indeed, for it to be lowered in this way, it is enough for one to be able to successively adjoin these radical quantities.

In place of another that Galois had set forth with a demonstration on the same subject, here is the primitive text:

[1] In the manuscript, the statement of the theorem we have just read is placed in the margin and includes: "*In the statement of the theorem, it says that one adjoins to an equation all the roots of an auxiliary equation of prime degree, and it is a question in Theorem II as to how many quantities must be adjoined. Also, the property that the substitutions are the same in all the groups is mentioned. We will discover the demonstration in (1).*" The editor's note refers to textual variants.

Theorem: — If the equation in r is of the form $r^p = A$, and if the p-th roots of the unity are found among the previously adjoined quantities, then the p groups in question in Theorem II will join, and moreover, this property remains that the substitutions of letters to pass from one group to another use the same substitutions in the same groups.

Finally, in any case, it amounts to adjoining to the equation every such value of r. Consequently, these p-th roots must be found among the previously adjoined quantities. Thus one sees how far we are dealing here with substitutions (Proposition I, scolie). Hence, one must...

This new finding dates from 1832 and shows, for that reason, that the author was extremely pressed for time while writing it, which confirms what I asserted in the note cited. (A. Ch.)

Page 44

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

Let us adjoin to the equation the first radical extracted in the solution. Two cases can arise: either, by adjoining this radical, the permutation group of the equation is reduced; or else, this extraction of a root is only preparatory, and the group remains the same.

Will there always come a time, after a certain finite number of root extractions, when the group is found to be diminished without the equation being unsolvable? Yes, for if at this point there were multiple ways of reducing the group of the proposed equation through a simple root extraction, one would have to consider only that root of smallest possible degree among these simple radicals, which alone, by becoming known, would reduce the group of the equation.

So let p be the smallest prime number that is represented by this minimal degree, so that a root extraction of degree p diminishes the group of the equation.

We can always suppose, at least for what is relevant to the group of the equation, that among the quantities previously adjoined to the equation there is a p-th root of unity. For indeed, as this expression is obtained by extracting roots of a degree less than or equal to p, its acquisition will not change anything in the group of the equation.

Consequently, by Theorems II and III, the group of the equation will be separated into p groups which, as far as their relationship to the other previously adjoined groups, enjoy this property: (1) that one passes from one to another by a single letter substitution; and (2) that all of them contain the same substitutions.

Adjoining further this p-th root, if the group of the equation splits into p groups that enjoy this double property, one can, by a simple extraction of the p-th root, reduce the group of the equation to the union of these partial groups.

Let us take, finally, the function of these roots which must be known in order to unite these partial groups, and let us, for that purpose, add any sym-

metric function of them whatsoever. (It suffices, for this, to choose a symmetric function...)

Page 45

[Beginning of the visible text]
"... les diverses valeurs taken by a function, through all the permutations of one of the partial groups, which thereby remains invariant under no substitution."

Let φ be this function of the roots.
Apply to φ one of the substitutions of the total group that is not common to the two partial groups. Let φ_1 be the result. Apply the same substitution again to φ_1, and let φ_2 be the outcome, and so on.
Since p is a prime number, this sequence can only stop at the term φ_{p-1}; then we shall have $\theta_p = \theta_1$, $\theta_{p+1} = \theta_1$, and so on.
That established, it is clear that

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

will be invariant under all permutations of the total group and, consequently, is thus known at present.
If one takes the pth root of this function and adjoins it to the equation, then, by Proposition IV, the group of the equation no longer contains any substitutions other than those of the partial groups.
Thus, for the group of an equation to be lowered (in its order) by a single adjunction of a root, the condition stated above is necessary and sufficient.
We now adjoin to the equation the radical in question; we can reason by analogy about this new group as we did for the preceding one, and so it must itself decompose in the indicated manner, and so on, until we reduce ourselves to considering no more than a single partial substitution.

Scholium.—It is easy to observe that this approach is the one followed in the resolution of the general equations of the same degree. Indeed, these equations are solved by means of a cubic equation, which itself, in order to be solved, requires a square root. In the natural progression of ideas, it is therefore by this square root that one must begin. Now, by adjoining an arbitrary square root to the equation, the group of the equation—which contains twenty-four substitutions—decomposes into two subgroups that differ only by a sign. Denoting the roots by a, b, c, d, e, here is one of these groups:

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

Page 46

Now, this group itself is split into three groups, as indicated by Theorems II and III. Thus, by extracting a single cube root, there remains only the group

$$abcd,$$
$$badc,$$
$$cdab,$$
$$dcba :$$

Then this group splits again into two groups:

$$abcd, \quad cdab,$$
$$badc, \quad dcba :$$

Hence, after a simple square-root extraction, there will remain

$$abcd,$$
$$badc;$$

which will finally be resolved by yet another square-root extraction.

We thus obtain either Descartes's solution or Euler's solution; for although, in solving the auxiliary cubic equation, the latter extracts three square roots, one knows that two of them suffice, since the third is then deduced by rational means.

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

Application to irreducible equations of prime degree.

Proposition VI. Lemma.—An irreducible equation of prime degree cannot become reducible by adjoining a radical whose index would be anything other than the very degree of the equation.

Page 47

For if $r,\ r',\ r'', \ldots$ are the various values of the radical, and if $Fx = 0$ is the proposed equation, then it would be necessary for Fx to factor into

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

all of the same degree, which is impossible unless $f(x,r)$ is linear in x.

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

Proposition VII.

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

From the preceding proposition, the smallest possible group, before the group that has only a single permutation, will contain n permutations. Now, a group of permutations on a prime number p of letters cannot reduce to p permutations unless one of those permutations can be deduced from another by a cyclic substitution of order n. (See the paper by M. Cauchy, *Journal de l'École Polytechnique*, 17th issue.)

Hence, the next-to-last group will be

$$(G)\qquad \left\{\begin{array}{llllllll} x_0, & x_1, & x_2, & x_3, & \ldots, & x_{n-3}, & x_{n-2}, & x_{n-1} \\ x_1, & x_2, & x_3, & x_4, & \ldots, & x_{n-1}, & x_n, & x_0, \\ x_2, & x_3, & \ldots, & \ldots, & \ldots, & x_{n-1}, & x_0, & x_1, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\ x_{n-1}, & x_0, & x_1, & \ldots, & \ldots, & x_{n-4}, & x_{n-3}, & x_{n-2} \end{array}\right.$$

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

Now, the group that immediately precedes this one in the sequence of decompositions will be composed of a certain number of groups all having the same substitutions as it does. Indeed, I observe that these substitutions can be expressed in just that way (let us suppose, in general, $x_n = x_0$, $x_{n+1} = x_1$, $\ldots$; it is clear that each of the substitutions of the group (G) are obtained by systematically replacing x_k with x_{k+c}, where c is a constant).

Page 48

Let us consider any one of the groups similar to group (G). According to Theorem II, it must arise by applying the same substitution throughout this group; for instance, by everywhere replacing x_k by $f(x_k)$, provided there is some defined function. The substitutions in these new groups must be the same as those of group (G), so we must have

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

where C does not depend on k. Hence,

$$f(k + 2c) = f(k) + 2C,$$

.....

$$f(k + mc) = f(k) + mC.$$

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

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

or

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

where a and b are constants.

Hence, the group that immediately precedes group (G) must contain substitutions of the form

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

and will therefore not contain, as a result, any other circular substitution than that of group (G).

We reason about this group just as with the preceding one, and it follows that the first group in the order of decompositions, that is, the actual group of the equation, may well contain substitutions of the form

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

and will not, in consequence, contain any other circular substitution like that of group (G).

Page 49

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

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

where a and b are constants.

Conversely, if this condition is met, I assert that the equation is solvable by radicals. Indeed, consider the functions

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

where α is an n-th root of unity, a a primitive root of n.

It is clear that any function invariant under the cyclic substitutions of the quantities $X_1,\ X_a,\ X_{a^2}, \dots$ will then be immediately known. Thus, one can find $X_1,\ X_a,\ X_{a^2}, \dots$ by Gauss's method for binomial equations, etc.

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

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

be rationally known. Therefore, the function

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

must be known, regardless of what X might be, as soon as X is rational.

Finally, we need only ensure that the equation whose roots are these functions admits, whatever X may be, a rational value. If the proposed equation has its coefficients in rational terms, then the auxiliary equation that gives all of these roots does as well, and thus it is proven that this irreducible equation of degree $1, 2, 3, \dots, (n-2)$ has a primitive n-th root of unity, which we know how to handle.

Page 50

This is the method that ought to be used in practice. But we will now present the theorem in another form.

Proposition VIII

THEOREM.—For an irreducible equation of prime degree to be solvable by radicals, it is necessary and sufficient that, once any two of its roots are known, the others can be deduced rationally.

First, it is necessary, for the substitution

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

never leaves two letters in the same place. Hence it is clear that, upon adjoining two roots to the equation, by Proposition IV, its group must reduce to a single permutation.
Secondly, this also suffices. Indeed, in that case, no substitution in the group will leave two letters in the same places. Consequently, the group will contain at most $n(n-1)$ permutations. Hence, it will contain only one circular substitution (otherwise, there would be at least n^2 permutations). Therefore, every substitution of the group, $x_k, x_{f\,k}$, must satisfy the condition

$$f(k+c) \;=\; f(k) \;+\; C.$$

Thus, and so forth, the theorem is proven.

Example of Theorem VII. Let $n = 5$. The group is as follows:

abcde	acebd	aedcb	adbec
bcdea	cebda	edcba	dbeca
cdeab	ebdac	dcbae	becad
deabc	bdace	cbaed	ecadb
eabcd	daceb	baedc	cadbe