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.