

An Accessible Approach to the Galois Theory of Equations

Andrei Nicolaide

Professor, D.Sc.

Faculty of Electrical Engineering and Computer Science

Department of Electrical Engineering and Applied Physics

Transilvania University of Brasov

Brasov, Romania

andrei.nicolaide@gmail.com

Abstract: *The Galois Theory has been largely developed and analyzed. Despite its importance and very interesting deductions, keeps however certain part the revisiting of which has been necessary as shown in several relatively recent papers. Certain unclear situations emphasised in introduction, namely roles of adjoined quantities and permutations, make the object of the present paper aiming an accessible introduction to the mentioned theory.*

Keywords: *Role of permutations, Substitution, Arrangement of the equation group, Solvability, Composition factor.*

1. INTRODUCTION

The Galois Theory of equations [1-7], despite its importance and very interesting deductions, keeps however certain parts the revisiting of which has been necessary, as shown in several papers [2-3]. Several such unclear situations still exist. For instance, in the work, [1; p. 61], concerning the solving of the quartic, there is written that the solution of a quartic implies the solving of an equation of third degree, which requires the extraction of a square root. But adjoining to the quartic this square root, the group of the equation which contained fully 24 permutations decomposes into two, having only 12. Here, it is not clarified if the square root concerns the respective expression of the quartic formula in terms of the coefficients of the equation, or the square root of one of the roots of the quartic.

Another unclear situation is the fact that the Galois Theory is based on the usage of permutations of the roots. However, no mention was found, convincing for me, why the permutations are very important in the Galois Theory. We shall return further to this question.

2. STEPS FOR SOLVING AN ALGEBRAIC EQUATION

Let:

$$f(x) = \sum_{i=0}^n a_i x^{n-i} = 0, \quad (1)$$

be the given equation. We shall assume that the equation is of the fourth degree, hence a quartic, like in the first example of Galois. Let us express this equation in the form of a product of binomials:

$$f(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_4). \quad (2)$$

The resolvent of this equation will be obtained after performing certain substitutions as follow:

$$y_1 = \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4; \quad (3 a)$$

$$y_2 = \alpha_2 x_1 + \alpha_3 x_2 + \alpha_4 x_3 + \alpha_1 x_4; \quad (3 b)$$

$$y_3 = \alpha_3 x_1 + \alpha_4 x_2 + \alpha_1 x_3 + \alpha_2 x_4; \quad (3 c)$$

$$y_4 = \alpha_4 x_1 + \alpha_1 x_2 + \alpha_2 x_3 + \alpha_3 x_4; \quad (3 d)$$

The substitutions above can be considered as being of direct sense, and then we can obtain the substitutions of opposite sense. In order to consider all possible permutations, we should consider the order of the group of four factors of the equations, and we obtain the total number $4!$ hence 24 permutations. Here, the discussion existing in literature relatively to the two words used in the same meaning vanishes, because, implicitly, according to the mathematical usage, the word substitution refers to relations denoted above [3 a-d], while permutation means the replacement of one substitution by another one, the finality of one permutation is another substitution.

The 24 permutations can be obtained by two steps. In the first step, consider instead of the group of substitutions above, taking the coefficients α_i with index i numbered successively in both senses. There follow 8 substitutions, the group of substitutions having 8 lines (rows) and four columns, we could say that this group is composed of two subgroups, each having 4 lines (rows). In the second step, interchange columns 1 and 3 and then, 2 and 4, in the preceding group. After these two permutations, the preceding group delivers three groups, and we could call each of them subgroup, all together being the total group of substitutions usable for all possible permutations.

The equations (3 a-d) and the mentioned completion really satisfy the condition of permutations; because if a single equation is not fulfilled the solving is not possible.

Therefore, we can form the following equation:

$$F := \prod_{i=1}^{24} (y - y_i) = 0; \tag{4}$$

By solving equation (4), we obtain the left-hand side of the linear system (3 a-d), and the values of the input roots, i.e. the roots of the given equation. The solution of equation (4), also called *resolvent* of the given equation has an important role in the Galois Theory of equations, however to solve it, is in general difficult, because its degree is much higher than that of the given equation. Starting from the form of a quartic with the leading coefficient unity,

$$y := x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0, \tag{5}$$

we shall use a simplified form, also called canonical form:

$$y := x^4 + px^2 + qx + r = 0, \tag{6}$$

$$q \neq 0. \tag{6 a}$$

The group of the equation above is:

$$G_0 = \begin{matrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 \\ \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 \\ \alpha_4 & \alpha_1 & \alpha_2 & \alpha_3 \end{matrix} \tag{7}$$

Some maximum invariant subgroups are given below.

$$G_H = \begin{matrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_3 & \alpha_4 & \alpha_1 \end{matrix}. \tag{8}$$

3. THE SEQUENCE OF MAXIMUM INVARIANT SUBGROUPS AND THE COMPOSITION FACTORS

Having in view that we have not the values of the coefficients, we must take all possible maximum invariant subgroups and permutations, instead of G , vertically, and we have: $G = 24$ permutations,

$H_1 = 2$ subgroups(12 permutations/ subgroup), $H_2 = 3$ subgroups(4 permutations),

$H_3 = 2$ subgroups(2 permutations), $H_4 = 2$ subgroups(2 permutations), $H_{id} = 1$, called

composition or *constitutive* groups and subgroups. The sequence of the composition factors is:

$$f_1 = \frac{24}{12} = 2; f_2 = \frac{12}{4} = 3; f_3 = \frac{4}{2} = 2; f_4 = \frac{2}{2} = 1; f_{id} = 1. \tag{9}$$

We propose to consider as permutation group the system of substitutions (3 a-d) above. No matter if we interchange the quantities α_i and x_j , the solution of the system remaining unchanged. If the system is solvable, the solution of the equation exists. It follows that we can use as group of the equations the table of roots:

$$G_0 = \begin{matrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_1 \\ x_3 & x_4 & x_1 & x_2 \\ x_4 & x_1 & x_2 & x_3 \end{matrix} .$$

Therefore it means, according to Galois, that all 4 subgroups should be solvable, and the composition factors f_i of the composition subgroups (G_i or H_i) are prime numbers.

Theorem: Therefore, the considered polynomial (equation) satisfying the condition of having the composition factors prime numbers is considered metacyclic, hence solvable.

This is, in fact, the essential result obtained by Galois.

Lemma: at the same time, it follows that the coefficients of the system of substitutions must be arranged as above, regardless the polynomial (equation) form (what is not usually found in known literature).

Obviously a prime group of degree greater than 4 being not metacyclic, according to the Lemma of odd permutations [3], is not solvable. Indeed, the sequence of composition factors does not include the ratio of A_n and E , if the mentioned number is $n = 4$. For $n > 4$, the ratio of A_n and E cannot be a prime number. It follows that any group of degree $n > 4$ is not metacyclic.

4. THE ANALYTIC SOLUTION OF THE QUARTIC BY DESCARTES

Because Galois founded his first proof of solvability by radicals of polynomial equations on the Descartes solution of the 4-th degree, we shall remake it, after Tignol [5, pp. 64-66], but simplified using Maple 12:

$$(x^2 + ax + b)(x^2 + cx + d) = 0, \tag{10}$$

The total number of permutations for (5) or (6), for each of them is 24. Because of the form of (6), we can keep only the half of the number of permutations hence 12.

The role of permutations in the Galois Theory is very important because on it is based the developed procedure. In the known literature, we found many references to this subject, but the explanations cannot be considered as convincing. At any rate, there must have been certain justified reason for Galois, but I could not find it in the known literature.

5. THE ROLE OF THE PERMUTATIONS

On the Internet, in **Mathematics Questions** we found the subject: *Why are permutations of the roots interesting?*

As an answer there is recalled that if we have a polynomial with the leading coefficient unity, then the coefficients are symmetric functions of the roots and will be:

$$(x - r_1)(x - r_2) \dots (x - r_n) = x^n - (r_1 + \dots + r_n)x^{n-1} + \dots + (-1)^n (r_1 \dots r_n)$$

The scope has been *Intuition looking at permutations of the roots in Galois Theory-mathematics stack exchange*. After our opinion, these arguments do not hold because no permutation is related in any manner for distinguishing the effect of that permutation.

By expressing the relations between the coefficients of the factors of (6), and (5), we obtain the following equations:

$$eq1 := a + c; \tag{11 a}$$

$$eq2 := b + d + ac - p; \tag{11 b}$$

$$eq3 := bc + ad - q; \tag{11 c}$$

$$eq4 := bd - r; \tag{11 d}$$

all equated to zero. The system contains three given quantities and four unknown ones. We shall express three of the unknowns in terms of the known quantities p, q, r and of the calculated a , by using the following Maple 12 command:

$$\text{eliminate}(\{eq1, eq2, eq3, eq4\}, \{b, c, d\}); \tag{12}$$

Result:

$$\left[\left\{ b = \frac{1}{2} \cdot \frac{-q + a^3 + p \cdot a}{a}, c = -a, d = \frac{1}{2} \cdot \frac{q + a^3 + p \cdot a}{a} \right\}, \left\{ a^6 + 2a^4 p + p^2 a^2 - 4ra^2 - q^2 \right\} \right]; \tag{13}$$

Now, the number of permutations is reduced from 12 to 4, composed of three subgroups with 4 rows each of them.

By solving the equation obtained by equating to zero the expression in last brace of (13), we obtain:

$$a^6 + 2 \cdot a^4 \cdot p + p^2 \cdot a^2 - 4 \cdot r \cdot a^2 - q^2 = 0. \tag{14}$$

In the last equation we shall denote:

$$z = a^2, \tag{15}$$

and obtain

$$z^3 + 2 \cdot z^2 \cdot p + (p^2 - 4 \cdot r) \cdot z - q^2 = 0 \tag{16}$$

which will be examined further on. For simplification, we shall perform on (16) the canonical transformation, by putting:

$$z := w - \frac{2p}{3}. \tag{17}$$

There follows:

Summing up the like terms, the terms of power two vanishes, and we find the canonical form:

$$Y := w^3 - \frac{1}{3}wp^2 - \frac{2}{27}p^3 - 4rw + \frac{8}{3}rp - q^2 = 0. \tag{18}$$

By solving equation (18) of third degree, hence with a unity smaller than the given equation, what does not happen if the given equation was of any degree greater than 4, we shall obtain three values for w . By using (17), we shall find three values for z . Having in view (15), there follows 6 values for the parameter a . For each of them, we may obtain the two decomposition factors of (10), all may be different from each other. However, the roots of (6) will be always the same, the parameters satisfying always the same conditions. Surely, one can select the values of the simplest form. Therefore, it is now possible to solve both equations from the product (6) above, obtaining the four roots of the given equation from (6).

From the preceding, as well as from the known literature, it does not result that the permutations can have a fundamental role in determining the relations existing among the roots of the equations, because all permutations keep the same solution. For this purpose, a natural proof is necessary. By such a proof, many mathematicians understand that the proof should be simple and also convincing, what we tried above, in Sub-section 3.

Concerning the Descartes demonstration referred by Galois, the single but clear advantage is the transformations which lead to the solving of an equation of degree six, convertible into a cubic equation.

If instead of the Descartes method, we used the Lagrange method [9, pp. 591-592] for solving the quartic equation, we had to decompose the unknown into three components, raise the expression to square and comparing two forms of the expressions, by requiring certain identification conditions, and arrive anew at a cubic equation to be solved, like previously.

If we are interested in practical numerical applications, the literal considerations above can be easily avoided by using other procedures, like [8].

According to Galois, for an equation polynomial of prime order would be solvable by radicals, it is necessary and sufficient that two of its roots being known, the others result rationally. Even this theorem could be discussed, because the fundamental question has been if an algebraic equation is solvable by radicals. But when one states that for a given equation we know two roots, it follows that the fundamental question was already answered.

6. CONCLUSION

The transformed of the given algebraic equation, leads to a system of equations which contains a system of equations the form of which is like that of permutations but at the difference that if a single of those equations is not fulfilled, the solution cannot be obtained. Also, by comparing the explanation of the heuristic solution of Galois, with the Descartes solution of quartic, and with the set of equations (3 a-d), respectively, the latter seems to be nearest the explanation of the role of permutations and does not require precise adjunctions.

REFERENCES

- [1] *** Écrits et Mémoires Mathématiques d'Évariste Galois. Édition critique intégrale de ses manuscrits et publications par Robert Bourgne et J.-P. Azra, Gauthier-Villars, Paris, 1962.
- [2] H.M. Edwards, Galois for 21st -Century Readers, Notice of the AMS, Volume 59, Number 7, 2012, pp. 912-923.
- [3] A. Nicolaide, Revisiting Certain Procedures of the Galois Theory Using Symbolic Programming, International Journal of Scientific and Innovative Mathematical Research (IJSIMR), Volume 3, Issue 6, June 2015, pp 1-13, ISSN 2347-307X (Print) & ISSN 2347-3142 (Online).
- [4] ***Maple - 12 Handbook, 2011.
- [5] P. Tignol, Galois Theory of Algebraic Equations, World Scientific Publishing. Ltd., 2011.
- [6] Évariste Galois, Analyse d'un Mémoire sur la résolution algébrique des équations (*Pour qu'une équation de degré premier soit résoluble par radicaux, il faut et il suffit que deux quelconques de ces racines étant connues, les autres s'en déduisent rationnellement*), Bulletin de M. Férussac, XIII (avril 1830), pp. 271-272.
- [7] Évariste Galois, Note sur la résolution des équations numériques, Bulletin de M. Férussac, XIII (avril 1830), pp. 413-414.
- [8] A. Nicolaide, A Direct Approach to the Galois Procedure Concerning the Solvability of Polynomial Equations, International Journal of Scientific and Innovative Mathematical Research (IJSIMR) Volume 3, Issue 8, August 2015, PP 16-22. ISSN 2347-307X (Print) & ISSN 2347-3142 (Online).
- [9] Ch. De Comberousse, Cours d'Algèbre Supérieure, Deuxième édition, refondue et augmenté. Seconde partie. Gauthier-Villars et Fils, Imprimeurs-Libraires, Paris, 1890.

AUTHOR'S BIOGRAPHY



Andrei Costin Nicolaide, was born on the 1st of September 1933 in Bucharest. He received the degree of Electrical Engineer with honours, from Technical Institute of Craiova, Faculty of Electrotechnics (1956); Doctor of Engineering and Doctor of Sciences (Polytechnic Institute of Bucharest, in 1962 and 1974, respectively). Full professor at the Transilvania University of Brasov (1969-2003), consulting professor since 2004. His scientific activity includes field computation by conformal transformation and numerical methods, and Special and General Theory of Relativity. He is a regular member of the Academy of Technical Sciences of Romania.