International Journal of Scientific and Innovative Mathematical Research (IJSIMR)
Volume 2, Issue 11, November 2014, PP 880-891
ISSN 2347-307X (Print) & ISSN 2347-3142 (Online)
www.arcjournals.org

Considerations on Certain Theorems of the Galois Theory

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. In the present paper, certain theorems that we considered not enough examined, have been revisited and completed with some supplementary results not found in the known publications. The respective objectives refer to the basic elements of the theory. Certain results could be reached due to the usage of symbolic programming language, namely Maple 12. Also, in the paper, there has been shown that various known procedures for building a permutation group, in some cases, can lead to different results.*

Keywords: *Galois Theory, Transform equation, Automorphism, Galois group, Solvable equations.*

1. INTRODUCTION

The Galois Theory has been largely developed [1]-[15] and important results have been obtained. In many works one considers as very interesting the transform of the polynomial equation belonging to Galois. According to [1, Lemma II and III], let be the polynomial equation:

$$P(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0, \tag{I}$$

the coefficients of which belong to the rational number field $\boldsymbol{Q}$ and has the distinct roots $x_i \ \forall i \in [1,\ n]$. Having the roots $a, b, c, \ldots$, it is possible to form a function V of the roots so that no value obtained by the permutations, in this function, of the roots, in all possible manners, be equal to each other. For instance there is taken:

$$V = A\,a + B\,b + C\,c + \ldots, \tag{II}$$

where $A, B, C, \ldots$ are integer numbers. The function V chosen as above will have the property that all roots of the given equation will be rationally expressed in terms of V. Therefore:

$$V = \phi(a,\ b, c, d, \ldots); \qquad V - \phi(a,\ b, c, d, \ldots) = 0. \tag{III}$$

Making the product of all binomials above, by permuting all letters, except the first, an equation in V will be obtained, and it is called the transform of the given equation. Further, there is written that:

$$F(V, a) = 0. \tag{IV}$$

Hence, any root of the given equation can be expressed in terms of one root of the transformed equation.

This deduction has been used in various forms in the works concerning this subject. Concerning this development, we have the objection that in last formulae no indication is made to see the structure of the function of V and if it contains some undetermined quantities. For this reason, we

gave a complete deduction to this problem, but for a small number of roots, in order to keep a form easy enough for to follow easily the deduction. Such analyses are not in the known literature.

2. THE EXAMINED PROBLEM

For ease expression, we shall call the roots of the given equation input roots and the roots of the transformed equations output roots. We established that between the output roots and the input ones certain relations exist. These relations contain the symbols of the input and output roots, the coefficients of the given equations and those of the transformed undetermined input roots. The results show that we can express all input roots in terms of a single output root as in the known works. Having available only the output roots and having in view that the relations mentioned above are not linear, we found that they are polynomials of a degree with a unit smaller than the degree of the given equation. Therefore, surely every output root allows for obtaining a solution for each input root, but the relation, may be of a certain degree, greater than unity, producing several solutions and it remains to keep only that is correct. For this reason, it is necessary to calculate for several output roots, and keep the value that is common to those roots. However, this situation can be avoided as further shown.

We show that if the coefficients transforming the given equation are suitably chosen, the input quantity x_i will be one solution for any output quantity y_j. Conversely, the relation does not hold. For this purpose, we selected the coefficients roots of unity. In the known papers concerning this subject these circumstances are not specified.

2.1 The Relations between the Roots of a given Algebraic Equation and the Roots of its Galois Transformed Equation

We shall present the procedure together with the principle of the program we prepared for this purpose in the symbolic language Maple 12. It is to be noted that semicolon is the end of a command in Maple, even if any text follows. We shall consider equation (1), for the case $n=3$, in order the results be simple enough for to be easily followed.

The equations which occur are from two sources, the first 3, those which achieve the transformation, according to Galois, and the next 3, the Viète relations between the roots and the coefficients of the given equation:

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n=0, \tag{1}$$

$$\text{eqn1}:=\alpha_1 x_1+\alpha_2 x_2+\alpha_3 x_3-y_1;$$

$$\text{eqn2}:=\alpha_1 x_2+\alpha_2 x_3+\alpha_3 x_1-y_2; \tag{2 a, b, c}$$

$$\text{eqn3}:=\alpha_1 x_3+\alpha_2 x_1+\alpha_3 x_2-y_3;$$

$$\text{eqn4}:=x_1+x_2+x_3+a_1;$$

$$\text{eqn5}:=x_1x_2+x_1x_3+x_2x_3-a_2; \tag{3 a, b, c}$$

$$\text{eqn6}:=x_1x_2x_3+a_3;$$

Now, let us find the relations between x_1 and y_1. A very simple solution is the elimination using the next Maple command:

$$w_{11}:=\text{eliminate}\left(\{eqn1,eqn4,eqn5\},\{x_2,x_3\}\right); \tag{4}$$

There follows the elimination, [10], result, below, represented by the second factor within braces:

$$\left\{\begin{array}{l} x_2 = \dfrac{\alpha_3 x_1 - \alpha_1 x_1 + y_1 + a_1 \alpha_3}{\alpha_2 - \alpha_3}; \\ x_3 = -\dfrac{-\alpha_1 x_1 + \alpha_2 x_1 + y_1 + a_1 \alpha_2}{\alpha_2 - \alpha_3}; \end{array}\right\} \left\{\begin{array}{l} -2\alpha_1 x_1 y_1 + a_1^2 \alpha_2 \alpha_3 + a_1 \alpha_2^2 x_1 + \alpha_3 x_1 y_1 \\ -2 a_2 \alpha_2 \alpha_3 - \alpha_2 \alpha_3 x_1^2 + a_1 \alpha_3 y_1 - \alpha_1 \alpha_3 x_1^2 \\ -\alpha_1 x_1^2 \alpha_2 + a_1 \alpha_2 y_1 + a_1 \alpha_3^2 x_1 + a_2 \alpha_2^2 \\ +\alpha_1^2 x_1^2 - a_1 a_2 \alpha_1 x_1 - a_1 \alpha_1 \alpha_3 x_1 + \alpha_2^2 x_1^2 \\ +\alpha_3^2 x_1^2 + \alpha_2 x_1 y_1 + a_2 \alpha_3^2 + y_1^2 \end{array}\right\} \tag{5}$$

We shall denote the elimination result after collecting the coefficients of like powers:

$$\begin{aligned} w_{11} = {} & (-2\alpha_1 + \alpha_2 + \alpha_3) x_1 y_1 + (-\alpha_1 \alpha_2 - \alpha_1 \alpha_3 - \alpha_2 \alpha_3 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2) x_1^2 \\ & + (a_1 \alpha_2^2 + a_1 \alpha_3^2 - a_1 \alpha_1 \alpha_2 - a_1 \alpha_1 \alpha_3) x_1 + y_1^2 + (a_1 \alpha_2 + a_1 \alpha_3) y_1 \\ & + (-2 a_2 \alpha_2 \alpha_3 + a_1^2 \alpha_2 \alpha_3 + a_2 \alpha_2^2 + a_2 \alpha_3^2) x_1^0; \qquad y_1 := 3/2 - \left(\sqrt{3}/2\right) \cdot I. \end{aligned} \tag{6}$$

In order to avoid any possible superposition, we shall replace, in the last equation, x_1 by u_1. The result represents the equation $w_{11} = 0$, having the variable u_1.

As it can be seen from the last equation, the relation between u_1 and y_1 is not linear, and for a given value of y_1, we do not obtain a single value of u_1, as assumed in the Galois Theory. For this reason, there is necessary to choose the other quantities which intervene so that this situation be avoided. As shown, there intervene only the coefficients of the given equation and the coefficients involved in the transformation of the equation. Only the latter ones could be modified. Their values cannot be guessed, but we can put the condition that the coefficients of the variable u_1 at a power greater than the unity be zero. For the case we verified, we found as suitable the complex roots of the unity: α, α^2, α^3, the last being equal to unity. However, we have kept the literal form, and replaced the numerical value at the end, in order to avoid any division by zero.

For our calculations, we took the input quantities: coefficients of the given equation:

$$a_1 := -6; \quad a_2 := 11; \quad a_3 := -6; \tag{7}$$

the values of the roots, given below to allow a verification, generally are not known,

$$x_1 := 1; \quad x_2 := 2; \quad x_3 := 3; \tag{8}$$

and the coefficients for transforming the equation, the imaginary unit being, as in Maple, letter I:

$$\alpha_1 := \exp\left(\frac{2\,\mathrm{Pi}}{3} I\right); \quad \alpha_2 := \exp\left(\frac{2\,\mathrm{Pi}}{3} 2I\right); \quad \alpha_3 := \exp\left(\frac{2\,\mathrm{Pi}}{3} 3I\right); \tag{9}$$

in order to verify easily the results. After replacing the input values, except the value of x supposed not known, we obtained the following equation:

$$\begin{aligned} w_{11} = {} & (2.8799103 \cdot 10^{-9} - 5.1961524\, I) u_1 + (-8 \cdot 10^{-10} + 0.I) u_1^2 - 4 \cdot 10^{-9} \\ & + 5.1961524\, I = 0. \end{aligned} \tag{10}$$

There follows $x_1 = u_1 = 1$, therefore the correct result is obtained.

Let us now, find the relations between x_2 and y_1. A very simple solution is the elimination using as above, the next Maple command:

$$w_{11} := \text{eliminate}\left(\{\, eqn1, eqn4, eqn5 \,\}, \{x_1, x_3\}\right); \tag{11}$$

It follows the elimination result, below, represented by the second factor within braces:

$$\left\{\begin{array}{l} x_1 = \dfrac{x_2\,\alpha_3 - \alpha_2\,x_2 + y_1 + a_1\,\alpha_3}{-\alpha_3 + \alpha_1}; \\ x_3 = -\dfrac{\alpha_1\,x_2 - \alpha_2\,x_2 + y_1 + a_1\,\alpha_1}{-\alpha_3 + \alpha_1}; \end{array}\right\} \quad \left\{\begin{array}{l} -2\,\alpha_2\,x_2\,y_1 + a_1^2\,\alpha_1\,\alpha_3 + a_1\,\alpha_3^2\,x_2 + \alpha_1\,x_2\,y_1 \\ -\alpha_2\,\alpha_1\,x_2^2 + a_1\,\alpha_1\,y_1 - \alpha_2\,\alpha_3\,x_2^2 + a_1\,\alpha_1^2\,x_2 \\ +\alpha_1\,x_2\,y_1 - 2\,a_2\,\alpha_3\,\alpha_1 + \alpha_3\,x_2\,y_1 - \alpha_3\,\alpha_1\,x_2^2 \\ +a_1\,\alpha_3\,y_1 + a_2\,\alpha_3^2 + a_2\,\alpha_1^2 - \alpha_1\,a_1\,\alpha_2\,x_2 \\ -a_1\,\alpha_2\,\alpha_3 x_2 + \alpha_3^2 x_2^2 + y_1^2 + \alpha_2^2\,x_2^2 \end{array}\right\} \tag{12}$$

We shall denote the elimination result after collecting the coefficients of like powers:

$$\begin{aligned} w_{21} &= (-2\,\alpha_2 + \alpha_1 + \alpha_3)\,x_2\,y_1 + (-\alpha_1\,\alpha_2 - \alpha_1\,\alpha_3 - \alpha_2\,\alpha_3 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)\,x_2^2 \\ &+ (a_1\,\alpha_3^2 + a_1\,\alpha_1^2 - a_1\,\alpha_1\,\alpha_2 - a_1\,\alpha_2\,\alpha_3)\,x_2 + y_1^2 + (a_1\,\alpha_1 + a_1\,\alpha_3)\,y_1 \\ &+ (-2\,a_2\,\alpha_1\,\alpha_3 + a_1^2\,\alpha_1\,\alpha_3 + a_2\,\alpha_1^2 + a_2\,\alpha_3^2)\,x_2^0; \quad y_1 := 3/2 - \left(\sqrt{3}/2\right)\cdot I. \end{aligned} \tag{13}$$

After replacing the input values, except the value of x supposed not known, and replacing, like previously, x_2 by u_2 we obtained the following equation:

$$\begin{aligned} w_{21} &= (4.50000005 + 2.598076212\,I)\,u_2 + (-8.10^{-10} + 0.I)\,u_2^2 - 9.0000004 \\ &- 5.19615243\,I = 0, \end{aligned} \tag{14}$$

and there follows $x_2 = u_2 = 2$, therefore the correct result is obtained.

Let us now, find the relations between x_3 and y_1. A very simple solution is the elimination using as above, the next Maple command:

$$w_{31} := \text{eliminate}\left(\{\, eqn1, eqn4, eqn5 \,\}, \{x_1, x_2\}\right); \tag{15}$$

There follows the elimination result, below, represented by the second factor within braces:

$$\left\{\begin{array}{l} x_1 = \dfrac{-\alpha_3 x_3 + \alpha_2\,x_3 + y_1 + a_1\,\alpha_2}{\alpha_1 - \alpha_2}; \\ x_2 = -\dfrac{-\alpha_3\,x_3 + \alpha_1\,x_3 + y_1 + a_1\,\alpha_1}{\alpha_1 - \alpha_2}; \end{array}\right\} \quad \left\{\begin{array}{l} -2\,\alpha_3\,x_3\,y_1 + a_1^2\,\alpha_1\,\alpha_2 + a_1\,\alpha_2^2\,x_3 + \alpha_1\,x_3\,y_1 \\ -\alpha_1\,\alpha_2\,x_3^2 + a_1\,\alpha_2\,y_1 - \alpha_2\,\alpha_3\,x_3^2 + \alpha_1^2\,a_1\,x_3 \\ +\alpha_2\,x_3\,y_1 - 2\,a_2\,\alpha_1\,\alpha_2 + \alpha_3\,x_3\,y_1 - \alpha_2\,\alpha_3\,x_3^2 \\ +a_1\,y_1\,\alpha_1 + a_2\,\alpha_2^2 + a_2\,\alpha_1^2 - a_1\,\alpha_1\,\alpha_3\,x_3 \\ -a_1\,\alpha_2\,\alpha_3\,x_3 + \alpha_1^2\,x_3^2 + \alpha_2^2\,x_3^2 + y_1^2 + \alpha_3^2\,x_3^2 \end{array}\right\} \tag{16}$$

As previously, we shall denote the elimination result after collecting the coefficients of like powers:

$$\begin{aligned} w_{31} &= (-2\,\alpha_3 + \alpha_1 + \alpha_2)\,x_3\,y_1 + (-\alpha_1\,\alpha_2 - \alpha_1\,\alpha_3 - \alpha_2\,\alpha_3 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)\,x_3^2 \\ &+ (a_1\,\alpha_2^2 - a_1\,\alpha_2\,\alpha_3 - a_1\,\alpha_1\,\alpha_3 + a_1\,\alpha_1^2)\,x_3 + y_1^2 + (a_1\,\alpha_1 + a_1\,\alpha_2)\,y_1 \\ &+ (-2\,a_2\,\alpha_1\,\alpha_2 + a_1^2\,\alpha_1\,\alpha_2 + a_2\,\alpha_1^2 + a_2\,\alpha_2^2)\,x_3^0; \quad y_1 := 3/2 - \left(\sqrt{3}/2\right)\cdot I. \end{aligned} \tag{17}$$

After replacing the input values, except the value of x supposed not known, and replacing, like above, x_3 by u_3, we obtained the following equation:

$$w_{31} = (-4.499999996 + 2.598076210\,I)\,u_3 + (-8\cdot 10^{-10} + 0.I)\,u_3^2 + 13.5000001 - 7.794228636\,I = 0, \tag{18}$$

and there follows $x_3 = u_3 = 3$, therefore the correct result is obtained.

By comparing for a fixed y_i, the values of the corresponding values of x_j there follows that for passing from any x_j to the next x_{j+1} it is necessary and sufficient to make a step of a circular permutation of the index of the coefficients α_j of the transform equation.

Let us now, find the relations between x_3 and y_2. A very simple solution is, like previously, the elimination using as above, the next Maple command:

$$w_{32} := \text{eliminate}\left(\{\, eqn2, eqn4, eqn5 \,\}, \{x_1, x_2\}\right); \tag{19}$$

There follows the elimination result, below, represented by the second factor within braces:

$$\left\{\begin{array}{l} x_1 = \dfrac{-\alpha_2 x_3 + \alpha_1 x_3 + y_2 + a_1\,\alpha_1}{\alpha_1 - \alpha_3}; \\ x_2 = -\dfrac{-\alpha_2 x_3 + \alpha_3 x_3 + y_2 + a_1\,\alpha_3}{\alpha_1 - \alpha_3}; \end{array}\right\} \quad \left\{\begin{array}{l} -\alpha_1 x_3^2\,\alpha_3 + a_1\,\alpha_2^2\,x_3 + a_1\,\alpha_1\,y_2 + \alpha_1\,x_3\,y_2 \\ -\alpha_1\,\alpha_2\,x_3^2 - \alpha_2\,\alpha_3\,x_3^2 + \alpha_3\,x_3\,y_2 - 2\,\alpha_2\,x_3\,y_2 \\ -2\,a_2\,\alpha_1\,\alpha_3 + a_1\,\alpha_3^2\,x_3 + a_1\,\alpha_3\,y_2 + a_1^2\,\alpha_1\,\alpha_3 \\ -a_1\,\alpha_2\,\alpha_3\,x_3 + a_2\,\alpha_1^2 + a_2\,\alpha_3^2 - a_1\,\alpha_1\,\alpha_2\,x_3 \\ +\alpha_2^2\,x_3^2 + \alpha_3^2\,x_3^2 + \alpha_1^2\,x_3^2 + y_2^2 \end{array}\right\} \tag{20}$$

We shall denote the elimination result after collecting the coefficients of like powers:

$$\begin{aligned} w_{32} = {} & (-2\,\alpha_2 + \alpha_1 + \alpha_3)\,x_3\,y_2 + (-\alpha_1\,\alpha_3 - \alpha_1\,\alpha_2 - \alpha_2\,\alpha_3 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2)\,x_3^2 \\ & + (a_1\,\alpha_3^2 - a_1\,\alpha_1\,\alpha_2 - a_1\,\alpha_2\,\alpha_3 + a_1\,\alpha_1^2)\,x_3 + y_2^2 + (a_1\,\alpha_1 + a_1\,\alpha_3)\,y_2 \\ & - 2\,a_2\,\alpha_1\,\alpha_3 + a_1^2\,\alpha_1\,\alpha_3 + a_2\,\alpha_1^2 + a_2\,\alpha_3^2; \end{aligned} \tag{21}$$

and it is not necessary to carry out the calculations as before, because by replacing the quantities, $x_3 = 3$ and $y_2 = -3/2 - (\sqrt{3}/2)\cdot I$ or similarly $x_3 = 3$ for $y_3 = \sqrt{3}\cdot I$, we can see that the last equation is fulfilled. However, we gave the literal results because, in the known literature, we find no reference to the structure of the involved quantities.

3. SOLVABILITY OF POLYNOMIAL EQUATIONS

In order to examine the conditions of solvability, we need to recall the following basic concepts:

a. Adjoining a quantity, term introduced by Galois. When one selects as known some quantities, in fact not then available, one says that they have been *adjoined to the equation* which should be solved.

b. Rational quantity means any quantity expressed in a rational form in terms of the coefficients of the equation and some adjoined quantities (even if the latter ones are not rational).

c. Invariant subgroup of a group (detailed in Subsection 3.2).

Any group ***H***, considered as a subgroup of a group ***G***, is an invariant subgroup of the latter, if any *permutation* of ***G***, on the transform of ***H*** yields also ***H***. We recall that the transform of any group ***H*** (here a subgroup) is $\text{transf}(\boldsymbol{H}) = \sigma\,\boldsymbol{H}\,\sigma^{-1}$ where σ is the preceding mentioned permutation.

The inversion of two roots (letters, numbers) is called a transposition. The group which includes at least one invariant subgroup, except itself (permutation 1), and also surely the identical group, is called to be a composed group, otherwise a simple group.
The order of a subgroup (number of permutations) divides the order (number of permutations) of the group to which it belongs. This proposition is proved in several works in the known literature in similar ways. We consider not necessary to remind what is well established, but a suggestive explanation may be useful because of its many applications. An equation of degree 4 can have at most 24 permutations, corresponding to 24 equations of the first degree. This permutation set may be decomposed, in principle, into several subgroups corresponding to the following number of permutations: 24; 12; 4; 2; 1, and: 24; 12; 3; 2; 1 equations. It is obvious that each of them divides the total number of permutations. The product of two of them can give the order of one preceding them, as it results by composing the equations. For instance, for the quintic, we can select say the subgroups of orders 5; 3; 2; 1, but they do not divide each other, hence not valid.

4. GROUP OF AN ALGEBRAIC EQUATION

4.1. General Denominations

In order to examine the conditions of solvability, we shall use the concepts described above: Adjoining a quantity, to the equation which should be solved; rational quantity; invariant subgroup of a group. Here, the maximum invariant subgroup will be considered.

4.2. Permutations and the Group of an Algebraic Equation

Consider a polynomial equation of degree n and a rational function of its roots, the value of which differs for any different permutation of the roots. We recall, for there are various denominations concerning the permutations. We have to use generally n objects. For representing the replacement of certain of them by others, a permutation is used. For this purpose, one can use two lines (rows). The given objects (numbers, letters) are written on the upper line and the replacement objects (numbers, letters) on the lower line. This replacement gives the result called permutation. There are also several other notation manners among which the cycle notation, [19]. The first line (row) presents the roots (by numbers or letters) of any polynomial. If the second line (row) represents the same values, the both represent together the identical group. We shall assume that the coefficients of the equation belong to the rational number field, $\boldsymbol{Q}$. The algebraic group of an equation, according to Galois, who introduced this denomination, contains only those roots and permutations which preserve the relation between the roots, namely the roots which play the same role with respect to the rational numbers. For instance, two complex conjugate roots may be replaced with each other, but a rational number and a complex (or a radical) one may not be.

A basic remark, due to Galois, is the following: A group of permutations of an equation of a prime degree p may not be reduced to a group of p permutations except the case in which each permutation can be deduced from another one by a circular permutation [1, Proposition VII]. If this condition is not fulfilled, the permutations preserve the roots and the coefficients of the equations, but spoils its structure, so that in the penultimate permutation, a complex conjugate root does no longer appear as produced by an equation of the second degree, but from two whatever binomial products, one containing a rational quantity and the other a complex one.

According to Galois, the greatest group of an equation with m roots is the set of the $N = m!$ permutations which can be achieved with the m roots, group usually denoted by the letter $\boldsymbol{G}$, [1, Proposition I]. In practical cases, due to limitations mentioned above, the number can be much smaller. Therefore, one should not confuse the permutation group of a polynomial equation with the general group of permutations in Algebra.

It is useful to note that in the all known recent books, for the calculation of a permutation group, one starts from an irreducible polynomial, but in his works, Galois used as well also reducible

polynomials [6, p. 238-239]. We consider that the latter procedure can be useful for the proof of certain reducing procedures.

A subsequent definition is based on the concept of automorphism [10]. Let the number field $\boldsymbol{E}$ that contains all roots of the polynomial equation, be an extension of the field $\boldsymbol{F} \subset \boldsymbol{Q}$ which contains the coefficients of the equation, then the expression $\boldsymbol{E}/\boldsymbol{F}$ represents the group of automorphisms. The *automorphism* is a *mathematical object* the elements of which have bijective applications over a number field belonging, in the case of the Galois Theory, to $\boldsymbol{Q}$. These elements can be interchanged in permutations without spoiling the results, for instance two complex conjugate roots or the two results of a square root, because they result from a polynomial of second degree. According to certain works, [17, p. 95], we may include also the integer and rational roots, each being an application at the same point. Any automorphism of $\boldsymbol{E}/\boldsymbol{F}$ fixes pointwise $\boldsymbol{F}$, set of all automorphisms.
This group is sometimes denoted by $\mathrm{Aut}(\boldsymbol{E}/\boldsymbol{F})$. It is useful to note that roots of higher degree behave to some extent in a different way. For example, the case of the equations of third degree: 3 roots, one real and other 2 complex conjugate, also called automorphisms, although not emphasized in usual books (detailed for any degree in Section 5). The basic role of permutations, in this theory, is to keep the structure of the group, and the existence of invariant subgroups.
Several authors developed the last definition, renouncing the previous ones. Our impression is that both types are useful, the former in order to analyze the solvability, the latter for easily establishing the expression of the Galois group. This Galois group of (the extension) $\boldsymbol{E}$ over $\boldsymbol{F}$ is usually denoted by $\mathrm{Gal}(\boldsymbol{E}/\boldsymbol{F})$.
The discriminant of an equation (polynomial) is a rational and symmetric function of the roots, and implicitly of the coefficients of the equation. For these reasons, it may be used as the permutation group of the equation. If it is positive, all roots are real and may also contain complex conjugate roots, and if it is a perfect square it belongs to the alternating group $\boldsymbol{A}_n$ [14].

5. Form of the Group of Permutations of a Polynomial (Equation), also Called Galois Group

There are several manners for presenting the permutation group of a polynomial equation. We shall remark that not all manners give just the same result; we saw a certain difference in various cases. We shall consider the results applying the procedures of Galois and those by using the concept of automorphism in the form given by Maple 12. We shall examine the following polynomial equations and give the obtained results in tables 1 and 2.
The calculation of the roots and permutation group has been carried out by using the Maple commands:

$r := solve(evalf(f));$	f - the name of the polynomial function
$galois(f);$	

We introduced the first formula in order to avoid the form containing radicals, although the involved numbers are irrational, which lead to very long formulae, whereas we have been interested in the nature of the results, namely if there are real or complex. The roots been known, we could express the permutation group according to recommendations of Galois [1], [6, pp. 238-239].

By inspecting the tables 1 and 2, we can see that from polynomials **a**-**d**, only the first polynomial has complex conjugate roots, whereas the other three have only real roots. For the cases **a**, **c**, **d**, from Maple 12 there follows the same permutation group, whereas from the deduction we made according to the Galois procedure, only case **a**, with complex roots has a group different from the other cases with real roots. This result is in good accordance with Galois explanations in his texts.

Table 1. *Examples **a** and **b** of permutation group of a polynomial (equation, function).*

Function	$f := x^3 - \frac{3}{2}x^2 + 1$ **(a)**	$f := x^3 - 3x^2 + 1$ **(b)**
Group after Maple 12	"3T2", {"S(3)"}, "-", 6, {"(1 3)", "(2 3)"}	"3T1", {"A(3)"}, "+", 3, {"(1 2 3)"}
Group according to Galois	$\sigma_{id} = \begin{pmatrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{pmatrix}$ $\sigma_1 = \begin{pmatrix} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{pmatrix}$	$\sigma_{id} = \begin{pmatrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{pmatrix}$ $\sigma_1 = \begin{pmatrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{pmatrix}$
Roots	$1.08882534 + 0.5386519\,I$ $1.08882534 - 0.5386519\,I$ -0.6776506	$0.6527036 \quad 2.8793852 \quad -0.5320888$

Table 2. *Examples **c** and **d** of permutation group of a polynomial (equation, function).*

Function	$f := x^3 - 4x^2 + 1$ **(c)**	$f := x^3 - 7x^2 + 1$ **(d)**
Group after Maple 12	"3T2", {"S(3)"}, "-", 6, {"(1 3)", "(2 3)"}	"3T2", {"S(3)"}, "-", 6, {"(1 3)", "(2 3)"}
Group according to Galois	$\sigma_{id} = \begin{pmatrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{pmatrix}$ $\sigma_1 = \begin{pmatrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{pmatrix}$	$\sigma_{id} = \begin{pmatrix} 1 \to 1 \\ 2 \to 2 \\ 3 \to 3 \end{pmatrix}$ $\sigma_1 = \begin{pmatrix} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{pmatrix}$
Roots	$0.5374015 \quad 3.9354323 - 0.4728339$	$0.388923 \quad 6.979471 - 0.3683948$

6. REDUCTION OF THE GROUP OF AN EQUATION

This action means the reduction of the number of needed permutations. We shall consider the case of an irreducible equation. It implies its group be transitive. Assuming that the group is not transitive, there must exist a set of roots less than n, and the permutations of the group ***G*** of the equation, leave them invariable or only permute them, but not with other elements (roots). Hence, the mentioned set of roots keeps the form of a product and is a divisor of the equation. Therefore, the equation is reducible. If the mentioned set did not exist, the group should be transitive and irreducible.

The roots are not known, but we know that the roots of the given equation are all function of one of them, for example of x_1. Then, we can adjoin (according to the above mentioned meaning) a value of this root to the field of rationality ***Q***. Thus, the group will be reduced to the permutations which leave x_1 invariable. A simple extraction of a root can reduce the group of an equation by extracting the root of the smallest degree, choosing anyone of the simplest radicals the adjoining of which diminishes the group of the equation.

The sign of the Galois group delivered by the Maple software is given by the sign of the disjoint generators, i.e., permutations. If a permutation performs an odd number of inversions of the roots, it is called to be an odd permutation, and if it performs an even number, it is called an even one. A permutation with three letters (or numbers) yields an even result. The same result is obtained by two transpositions.

For solving (as procedure, not by solving formulae) an algebraic equation, according to Galois, it is necessary to reduce the group of the equation, namely $\boldsymbol{G}$, till the identical (unit permutation) will be reached. For this purpose, a successive adjunction of the roots of binomial equations of prime degree may be performed. Let the examined equation and the first binomial equation and a prime number be:

$$f\left(x\right)=0;\quad r^{p}=q,\quad p\le n; \tag{22 a, b}$$

where p is the smallest prime number needed for reducing the group by adjunction. If it is not a prime number, then it can be written as the ratio of two prime numbers. In fact, this means, firstly to build an invariant permutation group of $\boldsymbol{G}$. The coefficients of the given equation are considered to belong to number field $\boldsymbol{F}\subset\boldsymbol{Q}$. The above integer number q also belongs to the same number field. Let r_1 be the first complex root of index p of unity above. Then we can form the number field, $\boldsymbol{E}=\boldsymbol{F}\left(r_1\right)$ also called adjoined field. Assume that the equations have the maximal invariant group over the field $\boldsymbol{E}$. The permutation group of the given equation is $\boldsymbol{G}$ or an invariant group $\boldsymbol{H}$ of it, containing also the binomial equation above included in $\boldsymbol{E}$. Indeed, the permutation group of equation (22 a) already contains all roots of unity of index $v\in\left[2,n\right]$, hence including p, because $p\le n$. We take any rational function of all roots, hence it can be expressed only in function of a single one, say r_1. Therefore it will be not modified by the permutations of $\boldsymbol{G}$. Finally, $\boldsymbol{H}$ is an invariant subgroup of $\boldsymbol{G}$. We shall repeat the procedure, forming the fields taking the other values of exponent p. The procedure will be repeated with another binomial equation and so on. Concerning the order of subgroups, there follows:

$$\boldsymbol{G}>\boldsymbol{G}_1>\boldsymbol{G}_2\cdots\boldsymbol{G}_{\mathrm{id}};\qquad f>f_1>f_2\cdots f_{\mathrm{id}}=1;\quad f_i=\boldsymbol{G}_i/\boldsymbol{G}_{i+1}; \tag{23}$$

where the sequence of $\boldsymbol{G}_i$ is called the constitutive group, and f_i are called composition factors. Therefore, one obtains a sequence of subgroups, each of them being an invariant group of the preceding one. The ratio of the orders of each subgroup and the next one will be a prime number. The last term represents the final identical permutation. The Galois Theorem concerning the solving is usually expressed as follows: A general polynomial equation of degree n is solvable by radicals in the number field $\boldsymbol{Q}$ if its group is solvable, what means that its composition factors are prime numbers. Consider the group of a trinomial, it may be written in the form: $\boldsymbol{G}_{\mathrm{sym}},\boldsymbol{G}_{\mathrm{alt}},1$, the second is the invariant subgroup of the permutation group, the last being the identical permutation. But for $n=3$, we have: $ord\ \boldsymbol{G}_{\mathrm{sym}}=n!=6$; $ord\ \boldsymbol{G}_{\mathrm{alt}}=\boldsymbol{G}_{\mathrm{odd}}=\boldsymbol{G}_{\mathrm{even}}=\dfrac{n!}{2}=3$. Hence, composition factors are 2 and 1, hence all prime numbers. The solving conditions are fulfilled. Consider now the permutation group of a quartic (equation of degree 4), the maximum invariant subgroups may be written in the form: $\boldsymbol{G}_{\mathrm{sym}}=24;\ \boldsymbol{H}_1=12;\ \boldsymbol{H}_2=4;\ \boldsymbol{H}_3=2;\ \boldsymbol{H}_4=1;\ \boldsymbol{H}_{\mathrm{id}}=1;$ and the composition factors will be as follows: $f:\dfrac{24}{12}=2;\ \dfrac{12}{4}=3;\ \dfrac{4}{2}=2;\ \dfrac{2}{1}=2;\ 1$. There follows that all composition factors are prime numbers, and the polynomial of fourth degree is solvable by radicals. The permutation group of polynomial of degree 5 or greater have as invariant subgroup only the alternating group [2, p. 494], therefore, repeating calculations as above, it follows that the solving condition by radicals is not fulfilled. Concerning the reduction of the equation group, by using binomials as above, may be found in literature in several various forms. However, according to our experiments, the process does not modify the Galois procedure, but allows by a thought experiment (e.g., adjunction of a root), when possible, to work with equations of a lower degree.

From the sequence of successive invariant maximum subgroups above, there follows, that due to the adjunction of the binomial of degree p we begin with the invariant group from a lower number p instead of n, the reduction being $\frac{n}{p}$. It is worth noting that there is mentioned in literature, the case of equations of a degree higher than 4 that are solvable solutions by radicals, due to their form. We should add that some examples of this type satisfy indirectly the Galois conditions. For instance, the equation $x^6 + a x^4 + b x^2 + c = 0$, after the change of variable $x^2 = y$ will be reduced to the third degree, and implicitly it fulfils the Galois conditions.

7. THE GALOIS GROUPS

The finite simple groups may be classified completely into several classes among which: 1. Symmetric groups S_n; 2. Alternating groups A_n; 3. Dihedral groups D_n (non-abelian groups D_4); The groups S_n and A_n permute the set $\{1, \ldots, n\}$. The groups D_n correspond to the permutation of the vertices of any $n-$vertices polygon. It is important to be mentioned [2, p. 496], [5, p. 330] that a symmetric group also contains an alternating subgroup. Also, it is worth noting that for $n > 4$, the symmetric group contains only the alternating group as invariant subgroup.

An interesting remark found in [6, p. 303], states that Galois always worked with the roots of the equations, but not with its coefficients what, according to our opinion, implies that he did not establish the permutation group of an equation the roots of which were not known [17], [18].

However, we should add that his proof of [1, pp. 57-63] is of an outstanding concision and clarity. In fact, he considered the solutions of Descartes [16, p. 262, p. 590], [6, p. 64] and others of the quartic equation, which with certain notation, yields an equation of degree 6 in, say z, that has to be solved (step 0). All its terms, with unknowns containing only powers of z^2, can be reduced to another equation of the third degree (step 1) that fulfils now the solving condition. Therefore, the latter delivers three intermediary solutions, (step 2), the square root of which gives the searched roots (step 3). Supposing that all occurring quantities are known, by adjoining them in order to assume as extracted a square root of the equation solving formula, the total number of permutations splits from 24 to 12 (step 1). It is the step 1 above. Similarly, by adjoining the occurring quantities, in order to assume as extracted a third degree radical of the equation solving formula, there remains only 4 permutations, (step 2), where the solutions are in expressions of second degree. From these expressions one obtains three roots, and the number of permutations will be 2 (step 3). By extracting the square roots, the final solutions will be obtained. It suffices to obtain only two final roots, the third results directly, using the previous two.

With the current names, in the presented formal solution (thought experiment), in step 0, one had in view the starting permutation group of the given equation of order 24, denoting it by $\boldsymbol{G}$. In step 1, one had in view, in fact, the maximal invariant subgroup $\boldsymbol{G}_1 = \boldsymbol{H}_1$ of $\boldsymbol{G}$, having the order 12. In step 2, one considered the maximal invariant subgroup $\boldsymbol{G}_2 = \boldsymbol{H}_2$ of $\boldsymbol{G}_1$, having the order 4. In step 3, one considered the maximal invariant subgroup $\boldsymbol{G}_3 = \boldsymbol{H}_3$ of $\boldsymbol{G}_2$, having the order 2. The extraction of the square root yields a final root. It follows that the solution has been obtained. Galois added also some general considerations.

Galois considered that this is the general condition necessary and sufficient that a polynomial equation must fulfill for to be solvable by radicals, but with the mention the orders of composition factors being prime numbers as shown above.

8. CONCLUSION

The Galois Theory has been largely developed and analyzed, but after analyzing its content we saw that certain deductions remained limited at a general level, and practical aspects were not examined. One of them is the construction and the choice of transforming the given equation or polynomial for keeping a linear dependence between the roots of the given equation and the

transformed equations. The calculations, facilitated by the use of the symbolic language have been also presented. Supplementary results not found in the known publications have been obtained. Certain remarks of Galois, not specified in many known works, have been emphasised as simply as possible for their utility in practice. Another result we consider as useful, we established by examples that the establishing of the permutation of an equation, carried out by the two possibilities, by Galois procedure and by automorphism procedure, does not lead always to the same result. However, each procedure keeps certain advantages we mentioned.

REFERENCES

[1] *** Écrits et Mémoires Mathématiques d'Évariste Galois. Édition critique intégrale de ses manuscrits et publications par Robert Bourgne et J.-P. Azra, Gauthiers-Villars, Paris, 1962.

[2] É. Picard, Traité d'Analyse, Tome III, Troisième Édition, Gauthier-Villars et C-ie, Paris, 1928.

[3] A. Cox, Galois, Theory, Second Edition, John Wiley & Sons, 2012.

[4] ***Maple - 12 Handbook, 2011.

[5] Th. Anghelutza, Curs de Algebră superioară (A Course of higher Algebra), Vol. II, Editura Universităţii din Cluj, 1945.

[6] J.-P. Tignol, Galois Theory of Algebraic Equations, World Scientific Publishing Co. Pte. Ltd., 2011.

[7] É. Galois, Mémoire sur les conditions de résolubilité des équations par radicaux, Auteur: Évariste Galois (1811-1832). Publication: Mémoire manuscrit de 1830, publication dans le Journal de mathématiques pures et appliquées, pp. 417-433. Année de publication:1830. Nombre de pages:18.

[8] H.U. Besche, B. Eick, E. O'Brien, The groups of order at most 2000, Electron. Res. Announc. Amer. Math. Soc., 7 (2001).

[9] A. Nicolaide, An Approach to Common Roots and Elimination of Variables by Using a Symbolic Programming Language. Proceedings of the World Congress on, Engineering, 2014, Vol. II, WCE 2014, July 2 – 4, 2014, London, U.K., pp. 870-875.

[10] A. Nicolaide, Considerations on the Galois Theory and the Algebraic Solutions. Proceedings of the World Congress on Engineering, 2013, Vol. II, WCE 2013, 3 June-5 July, 2013, London, U.K., pp. 85-90.

[11] C. Bright, Computing the Galois group of a polynomial. April 15, 2013 pp. 1-11. https_cs.uwaterloo.ca_, pp. 1-11.

[12] Keith Conrad, Recognizing Galois groups S_n and A_n, pp. 1-7.math.uconn. 7.math. uconn.edu/~konrad/blurbs/galoistheory/galoisSnAn.pdf

[13] H.K. Sørensen, Niels Henrik Abel and the Theory of Equations. History of Science Department University of Aarhus, Denmark, E-mail: hkragh@imf.au.dk, 1999.

[14] Keith Conrad, Some examples of the Galois Correspondence, math.uconn. edu/~konrad, 2014.

[15] Keith Conrad, Galois Groups of Cubics and Quartics (Not in Characteristic 2), math.uconn. edu/~konrad, 2014.

[16] Ch. de Comberousse, Cours d'Algèbre Supérieure, Seconde Partie, Gauthier-Villars et Fils Imprimeurs-Libraires, Paris, 1890.

[17] G. Verriest, Leçons sur la Théorie des Équations selon Galois, précédées d'une Introduction à la Théorie des Groupes. Gauthier-Villars, Imprimeur-Éditeur, Paris, 1939.

[18] A. Nicolaide, Establishing the Galois Group of a Polynomial Equation the Roots of which are not Known, International Journal of Scientific and Innovative Mathematical Research (IJSIMR), Volume II, Issue 3, 2014, pp. 249-255.

[19] F. Rodrigues-Villegas, Handout 3, Department of Mathematics, University of Texas at Austin, TX 78712.

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.