Considerations on the Galois Theory and Algebraic Solutions

Andrei Nicolaide, *Member, IAENG*

***Abstract*—In this paper, the fundamentals of the GALOIS Theory concerning algebraic equations are examined as well as certain deficiencies of the actual stage of knowledge in this field. The importance of an understandable presentation of the related field is pointed out. The useful connection with the facilities offered by the symbolic software has been developed by the author. A new manner for deducing a formula, developed by the author, has also been included. There is to be added that for making the work accessible, the most important theoretical algebraic definitions and procedures have been presented for avoiding to the reader the need of resorting to many other sources.**

***Index Terms*—Algebraic equations, a symbolic language used in the Galois theory, an alternative to the Hudde theorem, isomorphisms between certain physical phenomena and mathematical objects.**

I. INTRODUCTION

Many works have been devoted to the Galois Theory of algebraic equations. The major part of them concerns interesting analyses and valuable results. As known, despite this deep research, many practical subjects have not been completely solved and, as mentioned in literature, even solutions of various cases including radicals could be expected. Many interesting results can be found in literature [1]-[19]. In [2] and [15], there has been mentioned the difficulty for many interested reader in using many sophisticated works. Only more recently, certain works, among which [1], [2], [15], have been oriented, to a large extent, towards applications. The present paper aims to examine some practical subjects in order to extend the use of the analysis for applications. The scope includes the search of procedures which are simpler and more efficient for calculations, presented as much as possible, in an easily understandable manner. A new procedure, for deriving a formula, not found in literature, and other mentioned contributions have been developed. Also the link with certain symbolic software has been considered. For various calculations, the Maple 12 symbolic software has been used.

II. THE OBJECT OF THE ANALYSIS

Let us consider an algebraic equation of the form:

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + ... + a_{n-1} x + a_n = 0 , \qquad (1\text{ a})$$

or in a compact form:

$$a_i x^{n-i} = 0, \quad \forall i = [0, n]. \qquad (1\text{ b})$$

If no special mention is made, only rational number coefficients will be considered, hence $a_i = a(i) \in \boldsymbol{Q}$.

We consider that the coefficients of the equation are defined over a number field (domain) of rationality, K, also called field of rationality. The roots are considered as belonging to the *identical group*, namely $x(i), \forall i \in [1, n]$ and may be expressed by radicals of degree n in the domain K. At the same time, we shall consider an extension F of K which contains K and every root of any polynomial with coefficients over K. The order of the group is related to the degree of its extension because the last is related to the number of roots.

A *field automorphism* (concerning one mathematical object) or *isomorphism* (concerning two mathematical objects), fixes the smallest field containing number 1, which is $\boldsymbol{Q}$, the rational number field. Two objects cannot be distinguished if they are similar, considering their symmetry properties, and considered isomorph (having the same form). More precisely, considering a certain case, the automorphism is an invertible function denoted as $f := Q(\sqrt{2})$, for instance $f(a + b\sqrt{2}) = h(a - b\sqrt{2})$, because $a - b\sqrt{2} = \frac{a^2 - 2b^2}{a + b\sqrt{2}}$, and similarly if instead of $\sqrt{2}$ is the radical of an other number, even the imaginary unit $i := \sqrt{-1}$.

In a simple explanation, we can say that number of *permutations* (*substitutions*) should be equal to the number of roots (hence *automorphisms*) of the equation (polynomial, respectively).

For using the Galois Theory in the examination of the given equation, two purposes will be considered: a. To look for the solution, namely the roots of the equation or, what the same is, the values of the variable corresponding to the zero value of the corresponding polynomial. b. To establish if the equation has an algebraic solution, namely obtained by using the four operations: addition, subtraction, multiplication, division, to which there is to be added the root extraction. This procedure is known as algebraically obtaining the solution. For this purpose the Galois group theory has to be used.

For various calculations, we have used the symbolic language Maple 12. For the sake of uniformity, and because the writing of formulae in Maple contains small differences relatively to the conventional writing, we have written the computing formulae using the rules of Maple. Another reason has been that if someone would be interested, this manner could facilitate the access to applications.

Manuscript received 10th December, 2012. Andrei Nicolaide is with the "Transilvania" University of Brasov, Romania. Address: "Transilvania" University of Brasov, Bd. Eroilor Nr. 29, Brasov, Cod 500036, Romania (e-mail: andrei.nicolaide@gmail.com).

We recall that a group is an algebraic structure consisting of a set together with an operation which combines any two of its elements to form a third element of this set. For instance, if one adds two relative entire numbers (i.e., with the sign plus or minus), one performs an operation with a group structure of the respective set, but if one adds two natural entire numbers, one does not perform an operation with a group structure, because the opposite of a natural entire number is not a natural entire one.

A group is written in the form of a row (sequence) of letters. It is useful to mention that Galois used the group denomination in the context of a group of permutations or a group of substitutions. The starting of a group of permutations, usually denoted with G, is a finite set of say p elements (letters, e.g., x), written all on the same line, and which can be submitted to composition of permutations. Such a group have orders which divide n *factorial*. In the case of the next permutation, the p elements will be written on the next line placed below the preceding. In the case of the end permutation, the p elements will be written on the next line placed below the preceding. The grade of a permutation group is equal to the number of elements (letters, e.g., x) used in these permutations (substitutions). The order of the same group is equal to the performed number of substitutions (permutations). Consider a function φ of five variables $x_i,\ i \in [1,\ 5]$, and four permutations (substitutions) $S_i,\ i \in [1,\ 4]$, including also the unit (also called *identical* or *symmetrical*) substitution. With the adopted notation, there follow four lines and five columns. For certain applications, it could be supposed that the function φ keeps the same value regardless of the ordinal number of each of the five variables.

We shall denote the set of roots of an equation as:

$$x_1,\quad x_2,\quad x_3,\ldots,\ x_n\ , \tag{2 a}$$

or in a compact form:

$$x_i, \forall i \in [1, n]. \tag{2 b}$$

It is well to recall from the beginning that the Galois Theory of equations is based on the permutations also called substitutions, in *all possible manners*, of the roots, generally having not known their values, but considering only those permutations which keep the value of the roots, regardless of the ordinal number of each of them. In the case of (2 b) the *all possible manners* lead to the number n *factorial*. We could add that despite the discussion in literature, no a special importance has to be attributed to the difference between permutation and substitution, being very close to each other. However, permutation means writing the starting permutation and below, the final permutation that will replace it. Substitution means to replace the elements of a fix permutation by those of another one. It can be considered an analogy with the denomination of the substitution-permutation network used in block cipher algorithms.

There has also to be added, what is not always stated, that only the set of roots with the position numbers got after each permutation, which will fulfil the same relations as those of the identical group (*unit group*) with their ordinal number, will be considered. The set of these permutations is called, as previously mentioned, the group of permutations (substitutions).

The permutations are carried out either by transpositions or by circular permutations. A transposition means the permutation between the elements, not in any manner, but only of two elements (e.g., letters) of a sequence of n elements, the others $n-2$ remaining invariable.

A substitution means the resultant of a succession of transpositions. In fact, a permutation of three elements is equivalent with two transpositions.

From the obtained group, it is possible to predict if the obtaining of the algebraic solution (using radicals) is possible or not.

III. Recall of the Operations with Permutations Occurring in the Analysis

A. The Decomposition of a Permutation (Substitution) in which all Elements or a Part of them Have Been Permuted

Having in view that several operations with permutations (substitutions) occur and there are explained in various manners in various texts, what could make difficult the understanding, we have presented these subjects in accordance with our aim, as simply as possible.

An example of a decomposition of a permutation into *cycles* may be made in general relatively to the following relation, using the Cauchy notation:

$$\sigma = S_1 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_4 & x_1 & x_2 & x_5 \end{pmatrix}, \tag{3}$$

because various authors use various notations, we have to mention that according to the choice above, the starting state is represented by the upper row, while the new state is represented by the lower row. All groups of permutations may be decomposed into a product of cycles. For this aim, let us rewrite (3) in the form:

$$\sigma = S_1 = \begin{pmatrix} 1, & 2, & 3, & 4, & 5 \\ 3, & 5, & 4, & 1, & 2 \end{pmatrix}, \tag{4}$$

where commas have been used for making the relation easier legible and the symbol sigma has been written without index, being a general usage. The procedure can begin, like in relation (5) below, with x_1, denoted simply x_1 or 1 in relation of the row above, then, it follows 3 that corresponds to 1, in the lower row of the relation (3); to 3 of the upper row, there corresponds 4, in the lower row. When we encounter an answer number equal to that of starting, in the present case of value 1 in the lower row, corresponding to 4 in the upper row, the first cycle is finished. We continue with the next number, not yet used of the upper row, in the present case 5, to which there corresponds 2, in the lower row, and to 2, in the upper row, there corresponds 5, in the lower row. Now, all number being browsed, we reached the end. The result will be:

$$\begin{gathered} \sigma(x) \neq x; \\ x\ \ \sigma(x)\ \ \sigma(\sigma(x))\ \ \sigma(\sigma(\sigma(x)))\ \ \sigma(\sigma(\sigma(x)))\ \ \sigma(\sigma(\sigma(\sigma(x)))) = 1; \\ (3,\ \ 4,\ \ 1,\ \ 5,\ \ 2) = (1,\ \ 3,\ \ 4)(2,\ \ 5). \end{gathered} \tag{5}$$

ISBN: 978-988-19251-0-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

B. *The Decomposition into Transpositions when all Elements or a Part of them Have Been Transposed*

The decomposition into transpositions may be achieved in various manners. A simple solution can be obtained from the preceding result, as follows:

$$\begin{aligned}&(1,\ 2,\ 3,\ 4,\ 5)=\\ &(1,\ 3,\ 4)(5,\ 2)=(1,\ 4)(1,\ 3)(5,\ 2).\end{aligned} \tag{6}$$

C. *The Product (the Composite) of two Permutations (two Substitutions)*

Let us consider two permutations, say S_1 and S_2, the starting permutation included, and their product in the form:

$$S_1=\begin{pmatrix}1,2,3,4,5\\3,5,4,1,2\end{pmatrix},\qquad S_2=\begin{pmatrix}3,5,4,1,2\\4,5,1,3,2\end{pmatrix},$$
$$S_2S_1=\begin{pmatrix}1,2,3,4,5\\4,5,1,3,2\end{pmatrix}. \tag{7 a, b, c}$$

Therefore, the operations performed in the order S_1 and S_2 and denoted S_2S_1 represent finally the lower row of S_2 when starting from upper row of S_2. The same result will be obtained when starting from upper line (row) of S_1, arriving at the lower row of S_1, and then, starting from upper row of S_2 and arriving at the lower line (row) of S_2.

IV. Analysis of a Polynomial Equation

In order to be able to easily control the results, we have chosen an equation the roots of which could be obtained without difficulty. There yields, after factorization using Maple 12 software:

$$\begin{aligned}&f:=x^5-2x^3+4x^2+x-4;\\ &\text{Scope}:=factor(f);\\ &\#x^5-2x^3+4x^2+x-4=(x-1)(x+1)\left(x^3-x+4\right),\end{aligned} \tag{8}$$

and

$$\begin{aligned}&x_1=1;\\ &x_2=-1;\\ &u=\left(54+3\sqrt{321}\right)^{1/3};\\ &x_3=-\frac{1}{3}u-\frac{1}{u};\\ &x_4=\frac{1}{6}u+\frac{1}{2}\cdot\frac{1}{u}+\sqrt{3}\left(-\frac{1}{3}u+\frac{1}{u}\right)I;\\ &x_5=\frac{1}{6}u+\frac{1}{2}\cdot\frac{1}{u}-\sqrt{3}\left(-\frac{1}{3}u+\frac{1}{u}\right)I;\end{aligned} \tag{9 a, b,..., f}$$

where, we have denoted with the symbols of Maple 12 software, which we have used, the imaginary unit by italic capital letter I. According to (8), the given equation is reducible, while the remaining factor is an irreducible polynomial (or equation); therefore it suffices to consider only the irreducible factor.

Then, in order to obtain the group of permutations (substitutions), we shall write one group of permutations, including also the unit or symmetric permutation group, of the given equation, using the Cauchy notation:

$$S_1=\begin{pmatrix}x_1\ x_2\ x_3\ x_4\ x_5\\ x_a\ x_b\ x_c\ x_d\ x_e\end{pmatrix}. \tag{10}$$

Because except the two linear factors, only the irreducible factor has to be examined, the identical reference permutation group of the equation will be:

$$S_3=\begin{pmatrix}x_3\ x_4\ x_5\\ x_3\ x_4\ x_5\end{pmatrix}. \tag{10 a}$$

Examining the solution of (9 d, e, f), there follows that all simple symmetric functions expressing the relation between the coefficients and roots keep unchanged their values, but not all possible relations. Therefore, the permutations below:

$$S_2=\begin{pmatrix}x_3\ x_4\ x_5\\ x_3\ x_5\ x_4\end{pmatrix},\qquad S_3=\begin{pmatrix}x_3\ x_4\ x_5\\ x_5\ x_4\ x_3\end{pmatrix}, \tag{10 b, c}$$

show, considering the sum x_4+x_5, of the group S_2, of (10 b), keeps the value of the relations of the identical group. The sum x_4+x_3 occupying the equivalent positions in (10 c) does not keep this value. There follows that from all 6 possible permutations (the identical permutation included) only two are, in this case, necessary and sufficient. The resulting group of permutations, as shown below in Sub-sections VI and VIII, is solvable, therefore the Galois resolving condition is fulfilled.

The fundamental theorem of Galois is expressed as follows: Each rational function of the roots, invariable at the permutations of the elements of the group, generally denoted by G (above by S_i), belongs to the field of rationality, and conversely, each rational function of the roots belonging to the field of rationality is invariable at the group of permutations.

It is useful to add certain completions usually omitted. Let us consider a rational function:

$$\varphi:=\varphi(x_1,\ x_2,\ x_3,...,\ x_n), \tag{11}$$

and a permutation (substitution *S*):

$$S_1=\begin{pmatrix}x_1\ x_2\ x_3\ \dots\ x_n\\ x_\alpha\ x_\beta\ x_\gamma\ \dots\ x_\nu\end{pmatrix}. \tag{12}$$

Let us assume that the function φ keeps the same numerical value if the variables x_i are submitted to a permutation. Denote φ_b and φ_a the value of the function before and after the substitution, respectively. Therefore, as assumed $\varphi_a=\varphi_b$. This equality did not exist if the variables x_i were independent variables. At the same time, it is useful a remark of a few authors that one can disregard the case in which the rational functions built up by roots and the permutations yield multiple expressions, because all considered expressions are invariable [7, p. 479].

Consider a group of substitutions G, set of n variables as in relation (2 b) and a set of rational functions $\varphi_i\ \forall i\in[1,n]$, depending on these variables. We shall consider only those functions which keep unchanged their values for all substitutions of G. Let H be the subgroup formed by all permutations (substitutions) keeping the

ISBN: 978-988-19251-0-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

preceding functions invariable. If the subgroup H belonging to G is transformed by any permutation of G, into the identical value H, it is called *invariant subgroup*.

Any group of permutations is called to be a *group solvable by radicals* if its splitting field is included in a radical extension of K. A radical extension is a field that includes roots of the given equation (polynomial respectively). The splitting field of a polynomial is the smallest number field which contains all the roots of a polynomial the coefficients of which are in the number field K.

We shall make some considerations concerning the simple and composed groups [7, p. 483].

A group G having p letters (namely roots) is considered containing another group G_q if the former includes all permutations of the latter, called subgroup. The number of lines (rows), with the notation we have adopted, represents the order of the group. We shall assume that the order of groups G and G_q are m and μ, respectively, and $m > \mu$.

We shall denote the substitutions of G_q using notation as explained in Sub-section II, for the upper row, by:

$$S_1, \quad S_2, \quad S_3,..., \quad S_\mu . \tag{12 a}$$

Therefore, we have obtained the substitutions (12 a) by the permutations from G to G_q, and S belongs to G. Let us now perform another permutation T on (12 a) and obtain:

$$TS_1, \quad TS_2, \quad TS_3,..., \quad TS_\mu . \tag{12 b}$$

This substitution must belong to G but not to G_q of (12 a). Indeed, consider the substitution T where, for simplicity, the index has been omitted,

$$TS_i = S_j ; \quad T = S_j S_i^{-1}, \tag{12 c, d}$$

where S^{-1} denotes the inverse permutation. Therefore, S and T should be the same but it is not possible because T, as assumed, is simple, then it belongs to G. Hence hitherto, we distinguished in G, apart G_q another subgroup T, and there follows:

$$m \geq 2\mu . \tag{12 e}$$

If we stop at the step n_s, we have:

$$m \geq n_s \mu . \tag{13}$$

It is necessary that in the previous relations, (12), (13) to adopt instead of the symbol greater than or equal to, the symbol equal, because the order of a group, being a number of substitutions (permutations) should be a natural number, and m, being the total number of substitutions (permutations) of a group with n elements, will be n *factorial*, there follows that n_s should also be a natural number (hence without decimals).

Another interesting mathematical (geometrical) object is the *invariant maximum subgroup* of any group G, namely a subgroup G_q such that no invariant subgroup exists containing G_q as a subgroup. Example of a composed group, the sequence of groups such that each term is an invariant subgroup [7, p. 487] of the preceding one, the last being the identical substitution. The decreasing order of the respective group and subgroups permutation number will be:

$$m, \quad m_1, \quad m_2,..., \quad m_\mu . \tag{14}$$

The numbers above yield the ratios:

$$\frac{m}{m_1}, \quad \frac{m_1}{m_2}, \quad \frac{m_2}{m_3},..., \quad \frac{m_p}{1}, \tag{15}$$

where 1 represents the *unit* (or *identical*) permutation.

The numbers of (15) are called *factors of composition*. They have been studied by Camille Jordan [7, p. 487] and Otto Hölder [7, p. 492].

The function which for any permutation can take only two values equal but of opposite sign is called *alternating function*, whereas the group of substitutions (permutations) which keep invariable the mentioned function is called *alternating permutation group*. A group containing n elements (letters) has $n!$ substitutions [7, pp. 462-464]. Therefore, according to the preceding definition, the order of the corresponding permutation group will be the half:

$$N_{\text{perm}} = \frac{n!}{2}. \tag{16}$$

If n is greater than 4, the single invariant group is the alternating group as shown in [7, p. 494]. The alternating group is an *invariant maximum subgroup* of the symmetric group [7, p. 493], because the order of a subgroup of the symmetric group, is a divider of n factorial.

Let us assume now that the roots are distinct. We can distinguish the following field and subfields.

$$\boldsymbol{Q} \subseteq \boldsymbol{Q}(x_3) \subseteq \boldsymbol{Q}(x_3, x_4, x_5) . \tag{17}$$

Because x_4 and x_5 are complex conjugate numbers in the field extension $\boldsymbol{Q}(x_4, x_5)$, we can consider that they satisfy a quadratic equation, or in the present case, we obtain them in the form of radical expressions of third order, hence by solving a cubic equation. There also follows that the presence of the two first roots, although unnecessary, does not trouble the results by using the described procedure.

After numerical experiments, we realized that the reduction of the entire functions and implicitly of the group of permutation, by factorization in order to keep only the irreducible factor, using for instance a Maple software, and the procedure known in literature, the former one seems to be advantageous, and concerning the results, no practical differences have occurred, except the former could be more complete.

V. Procedure for Solving a Polynomial Equation by Radicals

According to Galois procedure, one starts from the equation (1) above. Its coefficients belong to any number field $C \subset \boldsymbol{Q}$. One also considers a rational function of its roots, in the form:

ISBN: 978-988-19251-0-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$V_i = \sum_{k=1}^{n} \alpha_k x_k , \qquad (18\ a)$$

here the coefficients α_k also belong to the number field C like the coefficients a_i. The roots denoted by the n letters x_k may be written with these letters one after the other in all possible manners, obtaining n factorial sequences. Using the terms of these rows in (18 b) below, one will obtain $n!$ values of V_i. Using these results, one can write the following expression called the *Galois transform*, from x to V of the given equation:

$$\prod_{i=1}^{N} (V - V_i) = 0, \quad N = n!. \qquad (18\ b)$$

For obtaining from (18 a) a number of $n!$ distinct expressions, it is possible to use for each expression other ordinal numbers of the roots, by using the permutations of type (4).

In Sub-section II, we assumed the case in which the function $\varphi(x_i), \quad i \in [1, n]$ keeps the same value, regardless the order in which the roots x_i are taken (their ordinal number). Now, we shall assume the case in which for every order in which the roots x_i are taken, the function will have another value. Then, it means that for any value of V_i of the root of the equations (18 b), there should correspond a certain sequence of the root set x_i. The condition to be true, is the relation (18 a) be bijective.

According to a theorem of Galois, the roots of the given equation are rational functions of any root of the Galois transform equation. This proposition has been proved by several authors in the known literature by a thorough logical analysis.

This result may be directly obtained from the explanations given above, after (18 a). It is to be noted that the importance of this transform is that it is factored, although not suitable for computing, because of the large number of equations.

It is worth noting that we have prepared a program we called Évariste-Galois-Nic.mw, which by a simple system of equations deduced from the transform relations and Viète formulae, then, certain automatic elimination procedures, yield several results including the theorem above, in a simple and suggestive manner, for enough large conditions.

VI. The Existence of an Algebraic Solution Including Radicals

For this purpose, we go back to the permutation group of the given equation. We assume that a number field C has been used. Let us consider a supplementary number [8, p. 228] say α outside of C. The number field of C and α and the five arithmetic operations form a new field of numbers denoted $C(\alpha)$, also called adjoin field [8, p. 320].

It is worth noting that at the base of the analysis of the algebraically solving a polynomial equation with cyclical solution lies the remarks of Gauss and Abel that the polynomial equation deduced from the binomial one, can be solved by radicals. The *condition necessary and sufficient* for an algebraic equation could be solved by radicals, in the number field $C(\alpha)$, is that its permutation group in $C(\alpha)$, have the composition factors prime numbers. The radicals of the root expressions should be assumed prime numbers, since otherwise they have to be replaced by superposed prime numbers.

Let us assume that the symbols of the roots have only prime numbers indices as power exponent. Assume that the greatest indices q of these radicals are $q \in Q, \quad q < n$.

The following sequence of the binomial equations, solvable by radicals will be considered:

$$x^i = 1, \quad i \in [2,\ q]. \qquad (19)$$

The first radical to be encountered may be $\sqrt{2}$. The next adjoin field, radical included, will be $C_1 = C(\sqrt{2})$ and the square roots will be in the same number field. If instead of $\sqrt{2}$, the encountered radical had been $\sqrt{-2}$, the adjoin field were $C_1 = C(\sqrt{-2})$. Let the next encountered radical be $\sqrt{3}$, and the adjoin number field will be $C_2 = C(\sqrt{3})$. The procedure has to be continued until the last number field say C_f.

The obtained expressions of permutation group and subgroups correspond to the numbers given above, in (15), which represent the sequence of the factors of composition of the groups [8, pp. 335-336]. This stage is necessary, since otherwise, without knowing the number field it is not possible to establish if the considered equation is reducible or not in a certain field, and the simplest case of the binomial equation could not be solved. Also, it is sufficient because at the end, the identical substitution is obtained, hence the roots are not modified [7], [8, p. 336].

In the case of a symmetric group with two elements (roots, letters), the group sequence of G is:

$$G, \quad 1, \qquad (19\ a)$$

and according to (13) the composition factors is 2, and the equation is solvable by radicals.

In the case, of a symmetric group with two elements (roots, letters), and an alternating subgroup with three elements, the group sequence of G is:

$$G,\ G_1,\ 1, \qquad (19\ b)$$

and according to (13) the composition factors are 2 and 3, hence prime numbers, therefore the case is solvable by radicals. In the case of a symmetric group with a number of elements greater than 4, as already mentioned above, the permutation group includes the alternating subgroup A, the sequence of G is;

$$G,\ A,\ 1, \qquad (20)$$

and, according to (13) and (15), the composition factors are 2, $\frac{n!}{2}$, hence the second is no more a prime number, and the case is not solvable by radicals.

ISBN: 978-988-19251-0-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

VII. A New Proof of the Formula of Cubic Equations

We established it using the isomorphism of a set of electric currents and certain mathematical objects. With this circumstance we established formulae permitting to express the Viète relations between the roots and coefficients of an algebraical equation easily applicable by Maple language even for higher degrees. In the case of $n = 3$, we found:

$$f_1 := \sum_{i=1}^{n} x_i = -a_1; \quad a_0 = 1;$$

$$f_2 := \sum_{i=1}^{n} x_i \sum_{j=i+1}^{n} x_j = a_2; \qquad (21\text{ a, b, c})$$

$$f_3 := \sum_{i=1} x_i \sum_{j=i+1} x_j \sum_{k=j+1} x_k = -a_3.$$

These relations may be an alternative to Hudde method [6, p. 53].

VIII. Computer Analysis of the Permutation Group of an Equation

There are several computer programs for the calculation of the permutation group of a polynomial equation. We shall refer to the Maple 12 program. The calling program is presented below using the example we have chosen above. First it is to be noted that the program accept only irreducible functions, otherwise it returns only the called polynomial function and stops.

For the last mention, we shall refer to the irreducible function resulted above, after factorization:

```
N := x^3 - x + 4;
infolevel[galois] := 2;                    (22 a)
Scope := galois(N);
```

where the command of the second row aims the obtaining of certain details:

```
Returned = 3T2 {"S[3]", "-", 6, {"(1 3)", "(2 3)"};   (22 b)
```

where the meaning of symbols is as follows: a) a string (i.e., a sequence) giving the name of the Galois group, here the third group in the list of degree 3 transitive groups; b) a set of strings giving the description of the group; c) a string giving the parity of the group, minus for odd groups and plus for even groups; d) the order of the group; e) the set of generators, in disjoint cycle notation (disjoint sets are those sets which have no element in common), like the roots, as given in Maple books. The group constituted by a set, e.g., the identical one, is called *transitive* if any element x_i can replace any element x_j, both of the same set, and conversely, by two substitutions.

Generating set of a group also called generator of a group or group generator is a set denoted by S such that every element of G can be expressed as being the product of the elements of group S, in finite number and their inverses.
If S contains a single element, it is usually denoted $< x >$ also called cyclic subgroup of the powers of x and it represents the entire G.

IX. Remark Concerning the Abel Equations

An interesting remark concerns the Abel equations because they have cyclic solutions. For this reason, they have been thoroughly treated in literature [8, p. 258].

For the same reason, we tried to examine the inverse problem, namely taking any value for the considered to be the first root, r_1, of a polynomial equation, to establish the other roots of the equation, which by the composition of functions, the former being the chosen root r_1, and the latter any convenient function, g, after a number of compositions namely $r_1 \circ g$, for the second root, etc., equal to the number of chosen roots, we obtain just the starting value. We have taken for g a linear binomial and a quadratic binomial plus two constants to be determined. After all numerical experiments, we found as a solution only the classical case of the binomial equation with the left-hand side the unknown raised at an entire power. In fact, also the known general solution of this type of equations is expressed in terms of some functions that we have not directly available.

References

[1] Tuen Wai Ng, Solving Polynomial Equations. Seminar on Advanced Topics in Mathematics. Hong Kong University, 5 December, 2006.
[2] L. Lerner, Galois Theory without Abstract Algebra, School of Physical Sciences, Flinders University, Adelaide, Australia, 5001, 11 August, 2011.
[3] 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 pages.
[4] C. Erhardt, Le mémoire d'Évariste Galois sur les conditions de résolubilité par radicaux (1831).
[5] Si Ying LEE, ZHANG De-Ki, Solving Polynomial Equations by Radicals, pp. 1-9. Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543.
[6] J.-P. Tignol, Galois Theory of Algebraic Equations, World Scientific Publishing Co. Pte. Ltd., 2011.
[7] E. Picard, Traité d'Analyse, Tome III, Troisième édition, Gauthier-Villars et C-ie, Paris, 1928.
[8] Th. Anghelutza, Curs de Algebră superioară (Cours of higher Algebra), Vol. II, Editura Universitatii din Cluj, 1945.
[9] D. Barbilian, Algebră, E.D.P., Bucuresti, 1985.
[10] A. Betten, Table of solvable groups of order up to 242, 1996, EuroPVM '96 Proceedings of the Third European PVM Pages 16-133. Springer-Verlag London, UK ©1996.
[11] Conrad Keith, Galois groups of Cubic and Quartics (not in characteristic 2), http://www.math.uconn 2012.
[12] J.S. Milne, Fields and Galois Theory, Course Notes, Taiaroa Publishing, Erehwon, New Zealand, 2005-2012.
[13] Ch. De Comberousse, Cours d'Algèbre Supérieure, Gauthier-Villars et fils, Imprimeurs-Libraires, Paris, 1890.
[14] D. Kalman, J.E. White, Polynomial equations Circulant Matrices, Mathematical Association of America, Monthly 108, November 2001, pp. 821-840.
[15] D. Grieser, Grundideen der Galoistheorie, Oldenburg, 2007.
[16] H.U. Besche, B. Eick, E. O'Brien, The *groups* of order at most 2000, Electron. Res. Announc. Amer. Math. Soc., 7 (2001), 1–4 (electronic).
[17] D.A. Cox, Évariste Galois, Solvable permutation groups, Amherst College, Bilbao, May, 2012, p. 41.
[18] D. Godman, An introduction to Galois Theory. NRICH enriching Mathematics. Ask NRICH web board.
[19] D. Joao, Galois-theoretic derivation of the cubic formula (version 5). *PlanetMath.org*. Freely available at: http://planethMath.

ISBN: 978-988-19251-0-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)