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)
www.arcjournals.org

Revisiting Certain Procedures of the Galois Theory Using Symbolic Programming

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: *Although many and important papers, including valuable contributions in the domain of the Galois Theory have been published, there are still certain domains, the revisiting of which may be very interesting. Firstly, the definitions of various terms are very different for almost every author. For instance, there are two different definitions for the normal subgroup. Also, some subjects like the adjunction of roots, developed by many authors have avoided the difficulty which blocks in many cases its applicability, but does not affect the utility of the usual Galois condition of solvability. The condition fulfilled by the permutations was for a long time established; however no intuitive example was given for clarifying this problem. All these problems have been analyzed in this work looking for to bring intuitive presentations aiming practical application.*

Keywords: *group theory, adjunction of roots, reduction of the Galois group order.*

1. INTRODUCTION

Many studies have been devoted to the Galois Theory [1]-[14]. Some scientists have been very interested in this theory, returning several times to it, trying to find new ways for proving its theorems. The aim of the present paper is to make an explanation as concise and simple as possible, aiming practical applications, and avoiding possible confusions. Especially, we had in view the presentations of Galois and certain orientations due to Verriest. In order to avoid for the reader the necessity to read some details which intervenes in the presentation, we recalled shortly the useful explanations.

Among the encountered problems, we can mention those which concern: the order of a group and the order of permutations of the group; the conditions for the reduction of the group of an equation be applicable; the actual role of the use of permutations; the condition satisfied by the permutations in the case of equations solvable by radicals; some definitions.

2. CONSIDERATIONS ON CERTAIN DEFINITIONS

Let $f(x)=0$ be the general form of a polynomial equation, with its coefficients in number field F belonging to the field of rational numbers $\boldsymbol{Q}$. The group of this equation, also called Galois group, is expressed by the set of permutations of the roots, which do not modify any relation among these roots, over the number field F, [11, p. 117, 193].

We shall recall several definitions in the simplest form. Any number set (number field) say B is called a *subfield* of any set A (number field); if B is a subset of A. We recall that a number field F is a *field extension* of a field B, if and only if B is a subfield of a number field A.

The splitting field of a polynomial is the smallest number field which contains all the roots of the polynomial the coefficients of which are in a number field denoted say by K.

According to Verriest, one can consider a polynomial $f(x)$ in a number field denoted by F which may be included in a larger number field F'. One can call factorization field of $f(x)$, the numerical

field of smallest extension containing the number field F and the roots of $f(x)$, for example F'. We consider that this denomination may simplify some explanations.

2.1. The unit element. It belongs to any group or subgroup and may be denoted by the same symbol E, although certain authors are using different symbols for each type of any complex, i.e., element of any set, namely, group element, semi-group and group. The unity, i.e., the unit element which satisfies the relations $EX = XE$, $XX^{-1} = E$, regardless the type of X, the unity E taking the corresponding fore-name (group, subgroup, etc.).

A polynomial (or polynomial equation) the coefficients of which are all prime numbers among them (i.e. the greater common divisor of any two coefficients is 1) is called primitive polynomial (or equation). If they are not, it is called imprimitive polynomial, [11, p. 68].

Complex is called any expression of the form $C = aH$ where a and H may represent any element of a set.

For denoting that an element, namely an element a or a complex C belongs to any group or complex G, the following relation $a \in G$ or $C \in G$, respectively, is used.

If some of these complexes have common elements, each of these elements will be considered only once. For example, if $B + B = B$ and $B \subseteq G$ then $G + B = G$.

The multiplication of a complex $C = C_1 + C_2 + C_3 ...$ by any element a, yields $Ca = C_1 a + C_2 a + C_3 a ...$ written in this order or conversely with a before. Similarly, if a is in C or H, then $Ca = C$ and $Ha = H$. At any rate, despite the name of multiplication, this computation has nothing to do with the matrix product. Also, the product of element complexes belonging to any group is associative.

2.2. Discriminant and group class. The finite simple groups may be classified completely into several classes as detailed in [9]. Here, we shall consider only: 1. Symmetric groups S_n;2. Alternating groups A_n.

Let us denote the general equation of degree n in any number field F. The group of this equation (Galois group) is the symmetric group of its roots, hence a sequence of the roots. We recall that the discriminant, abbreviated Discr, of this equation is given by the product of all its root differences, namely the square of it. We have:

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

$$D = \prod_{i=1}^{n-1} \prod_{i=2}^{n} (x_i - x_j); \quad \text{Discr} = D^2. \tag{2}$$

The symmetric group of permutations leaves unchanged any relation in the number field F, what is valid for both odd and even permutations. The latter ones have the same effect for the discriminant, being similar to the equation group. The set of even permutations of a symmetric group of any degree n represents a subgroup, because the product of two such permutations yields also an even permutation. The odd permutations do not satisfy this condition, being called a complex adjoint. The order of the mentioned subgroup should be $\frac{n!}{2}$. Therefore, the sequence of composition factors includes the ratio of A_n and E. We can see that for $n > 4$, this ratio cannot be a prime number. It follows that any group of degree $n > 4$ is not metacyclic.

2.3. The adjoint complex. Let us consider a group G and any subgroup H of it. The result of the multiplication of H by any element a of G is called complex, being for instant neither element nor subgroup. All these results belong to group G. Moreover, if a belongs to H, the result is just the subgroup H, because, as shown $aH = H$.

2.4. Expanding a group in terms of one of its subgroups. Let as previously, G and H be a group and one of its subgroup, respectively. Let us denote by lower case letters the elements of the given group, which can appear several times. We can write:

$$G = H\,a + H\,b + H\,c + ... + H\,e, \tag{3}$$

because the sum of products above gives just the group, starting from the subgroup, and using the elements contained by the group but not contained by the subgroup. It is worth noting that the results obtained by writing the elements after the subgroup (rightly) or conversely, give different results.

2.5. The order of a group and of its subgroups. Let us suppose that in the decomposition above, we had an expression with a number of 5 elements, therefore in the right-hand side we have a sum with five terms, $r = 5$, and each of them, having the same construction, will have the same number of terms, say t. Therefore, the number of terms of the left-hand side will be: $g = r \cdot t$, so that in general, the number of terms of a subgroup should divide the number of terms of the group, and the *order of a subgroup* should divide the *order of the group* to which it belongs. It follows that a group with a prime order cannot accept a subgroup, except the unit subgroup, or itself. The ratio $i = t = \frac{g}{r}$ is called the *index* of the subgroup in the group G.

According to many authors, the order of a group is the number of objects it contains, and the degree of a permutation group is the number to which it refers [11, p. 8]. These statements could lead to confusions, we shall avoid. For this purpose, we shall mention if the word *order* concerns the number of permutations.

For being a group, a set must satisfy the four known postulates recalled as follows. Let U, V, W be elements (subgroups or letters) of any group G then, the next four fulfilled relations are the mentioned postulates: $U \cdot V = W$; $(U \cdot V) \cdot W = U \cdot (V \cdot W)$ the half-height point being optional; $E \cdot U = U \cdot E$, the last letter being called unit element; $U \cdot U^{-1} = E$.

At the same time, the number of permutations that may be performed by a permutation group generally differs from its order as defined above, although sometimes expressed by the same word, except the case that the order concerns the number of permutations. In the case of a group with n elements, the total number of permutations is $n!$, hence a factorial.

2.6. The normaliser of an element of a group. If two elements (letters or subgroups) of a group G, namely here subgroups, fulfil the relation $A\,X = X\,A$ they are called to be *permutable*. The set of elements X of a group which are permutable to any given element A represents a subgroup called the normaliser of A and denoted P_A.

3. TRANSFORMATIONS OF ELEMENTS

The permutation of an element (letter or subgroup) here a subgroup, by multiplying both sides of the preceding relation, with A^{-1} yields:

$$A\,X = XA; \quad A\,XA^{-1} = X; \quad X := A\,XA^{-1}, \tag{4}$$

where the last relation is called the *transform of any subgroup X by the subgroup A*. A subgroup of any group is called to be *invariant* if it is permutable with any other subgroup of the group. By performing all transformations of the element A above, by all elements of the group G with g elements, we shall obtain g transformed elements, but only a smaller number will differ from each other, this set is called a *class of conjugate elements* in G, namely *conjugate subgroups*. Also, one says that *X is the conjugate of A in G*.

A subgroup having the index $i = 2$ is invariant. Indeed, consider the group G having the subgroup H with index 2. We can expand $G = H + H M$ where M does not belong to H. By performing another expansion, there follows:

$$G = H + M H; \quad H M = M H;$$
(5)

and hence M and H are permutable, and this is valid for each element of G.

3.1. Divisor of a group. Each set of elements, A, forming a group inside any group G is called a *subgroup* of G, a *proper subgroup* of G or a *divisor* of G. Then, G can be called to be a G *improper divisor* of G. Let us denote by expression $N = \frac{G}{A}$ a divisor of group G. Any group G has two implicit divisors, namely E and G. If it has not another subgroup it is called to be *simple*, otherwise *composed*. It is worth noting that the denomination divisor, despite its name, differs as action from the known meaning in Arithmetic or Algebra, concerning rather a subtraction than a division.

3.2. Invariant or normal subgroup. A subgroup which is equal to each of its conjugate subgroups is called to be a normal or invariant subgroup. A normal subgroup denoted by letter N belonging to any group G should satisfy the relation:

$$N = A N A^{-1}; \quad N A = A N, \tag{6}$$

for any element (letter or subgroup) A of group G. It is worth noting that certain authors wrote the first formula above changing the position of A and A^{-1} with each other. Also, in the works of Galois, except the preceding procedure, he resorted to the structure of the group for distinguishing the normal subgroups.

3.3. Maximum Invariant or normal subgroup. The set N is a maximum invariant subgroup of group G if $\frac{G}{N}$ is a simple group. Indeed, in this case $\frac{G}{N}$ has no an invariant subgroup and N fulfils the condition to be maximum.

3.4. The expression of permutations in form of cycles. Consider a permutation with five elements, letters or numbers:

$$P := \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,4\,5\,1\,2 \end{pmatrix}; \quad P := \begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,4\,5\,1\,3 \end{pmatrix}; \quad P := \begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,4\,1\,2\,3 \end{pmatrix}. \tag{7 a, b, c}$$

The cycles are established starting from the upper row from any element position (letter or number, here we shall use numbers), for instance 1, and go to the element, on the same column, below, on the lower row. Then, we go up to the upper row, on any column, to the same number or letter which we leaved on the lower row. Then, we go back, down on the lower row to the number of the same column. After having encountered the starting element, we consider the *cycle* closed. If we have encountered all elements, the procedure is finished. If not, we repeat the procedure starting from an element not still encountered, and so on, till we have browsed all elements. If there remains, on the same column the same elements we can write them once constituting by themselves a single cycle, however it is not strictly required and can be omitted.

In the first case, one starts from any position like 1, of first upper row: 1, 3, 3, 5, 5, 2, 4, 1, or then 1, 3, 5, 2, 4 and stops after reaching the starting number. The last set is called the orbit of 1. This denomination can be always used.

In the second case, one starts from any position like 3, of first upper row: 3, 5, 5, 3, or then 3, 5, called the orbit of 3. One stopped after reaching the starting number, but number 2 has not been encountered. Therefore, continuing 2, 4, 4, 1, 2 or then 2, 4, 1, and stops having reached the starting number. In the third case, one will start from position 1 of the upper row: 1, 5, 3, 3, 1, or then 1, 5, 3, and stops after having reached the starting number, but numbers 2 and 4 not encountered. Therefore, continuing 2, 4, 4, 2.

For the first case, there exists a single cycle: (1, 3, 5, 2, 4).

For the second case, there exists two cycles: (3, 5)(2, 4, 1).

For the third case, there exists two cycles: (1, 5, 3)(2, 4).

The stabilizer is represented by those permutations which keep elements (letters or numbers) at fixed points, for example on the same column.
As seen, these cycles have not common elements and they are called *fundamental cycles*.

3.5. Order of a cycle. Having not common elements, the elements of each cycle will be found only within this cycle or a power of it. Therefore, the order of a cycle will be equal to the number of elements it contains. If a cycle is raised to a power, e.g. 2, each element will be replaced by the element found at a place displaced with a unity in the positive sense (to the right). Each power means to repeat the same permutation. If one of the cycles above is raised to power 5, each given cycle having five elements, each element will be replaced with the element found farther with 5 units, in the positive sense, and we obtain just the unit group E. In a two-rows representation, having in each row one of the mentioned powers, there is given a permutation row.

3.6. The notation in the form of a cycle. For example, consider the double-rows permutations:

$$S=\begin{pmatrix}1\,2\,3\,4\\2\,1\,4\,3\end{pmatrix};\quad T:=\begin{pmatrix}1\,2\,3\,4\\4\,2\,1\,3\end{pmatrix};\quad TS=\begin{pmatrix}1\,2\,3\,4\\4\,2\,1\,3\end{pmatrix}\cdot\begin{pmatrix}1\,2\,3\,4\\2\,1\,4\,3\end{pmatrix}=\begin{pmatrix}1\,2\,3\,4\\2\,4\,3\,1\end{pmatrix} \tag{8 a, b, c}$$

and

$$TST^{-1}=\begin{pmatrix}1\,2\,3\,4\\2\,4\,3\,1\end{pmatrix}\cdot\begin{pmatrix}4\,2\,1\,3\\1\,2\,3\,4\end{pmatrix}=\begin{pmatrix}4\,2\,1\,3\\2\,4\,3\,1\end{pmatrix}. \tag{9 a, b}$$

In cycle form, we obtain:

$$\begin{aligned}&S=(1,2)(3,4);\quad T=(1,4,3),\quad T^{-1}=(1,3,4),\\&TST^{-1}=(1,2)(3,4)(1,4,3)(1,3,4)=(1,3)(4,2).\end{aligned} \tag{10 a-e}$$

4. CYCLIC GROUPS

A group having all elements powers of the same element is called cyclic group, and the mentioned element is called the *group generator*. As already mentioned each subgroup order divides the order of the group. Example of a cyclic group written in two manners, as sum and sequence:

$$G:=E+\sum_{i=1}^{m-1}A^i;\quad E:=A^0;\quad A^m:=E. \tag{11 a, b, c}$$

$$G:=E,A^i,\forall i\in[1,m-1];\quad E:=A^0;\quad A^m:=E. \tag{11 d, e, f}$$

If all elements of a group (letters, numbers and subgroups) are powers of an element, the group is by definition a cyclic group. If this element is not contained in the group, a supplementary explanation is necessary. Let A^c be the smallest power contained in the group for $k=1$, with $E:=A^0$, and in general, $A^{k(c-1)}$ which for $k=1$ and $c=1$, and for $k=1$ and $c=6$ yields A^0 and $A^5=1$, at the period end being A^4. If all elements of a cyclic group act simultaneously, the group is like a permutation row. In the case of circular permutations, the last term will be followed by the first one.

Each group of *prime order* is a cyclic group. Because the orders of subgroups must divide the order of the group, then when it is a prime number p, the latter can be divided only by 1 and by p, the only possible maximum subgroup is the whole group, the every element of which should be of order p,

except $A^0 = E$ (order 1). There follows that the group is composed of powers of A, and the elements are of order p. The various properties may be verified by performing the division $\frac{x^m - 1}{x - 1}$ for any x.

5. CYCLIC EQUATION

Abelian group is a group where the multiplication of any two elements, letters or numbers, as well as subgroups, is commutative, therefore $A\,B = B\,A$.

An equation, irreducible in a number field, having its group cyclic, is called a cyclic equation in the mentioned number field say F^i. For such an equation of degree n, a permutation will have a single cycle. In the case in which the power n is prime, it is possible to construct, starting from the known equation, a sequence over number fields F^{i+1} by adjoining to it a necessary quantity. For this purpose, if the equation is written in the general usual form, we can use the roots of binomial equations. It should be added that due to the form of its terms, it is an Abelian equation. If the first term of the cyclic group is the unity, then the order of the group is equal to its degree.

The roots can also be obtained directly, by simple procedures.

6. COMPOSITION SEQUENCE

Consider a group G and let be N_1 its maximum invariant divisor. Then let N_2 be the maximum invariant divisor of N_1, and so on. We obtain the following series and sequence:

$$G = E + \sum_{i=1}^{r-1} N^i; \quad N^r := E, \tag{12 a, b}$$

$$G, N_3, E; \quad G, N_2, E. \tag{12 c}$$

where every composition element as subgroup N_{i+1} is the maximum invariant subgroup of N_i but it does not mean that it could be maximum invariant subgroup of the preceding elements. The ratio $\frac{N_i}{N_{i+1}}$ is called *composition factor*.

A group can have several maximum invariant divisors. We can see the following cyclic group of order 6:

$$G = E + A + A^2 + \mathrm{A}^3 + \mathrm{A}^4 + \mathrm{A}^5, \tag{13}$$

and the subgroups have to be searched among the divisor of the order of the group, and they may be of orders 3 and 2. Therefore, according to Sub-section 3.3, there are two maximum divisors:

$$N_3 = E, A^2, \mathrm{A}^4; \quad N_2 = E, \mathrm{A}^3. \tag{14}$$

7. METACYCLIC GROUP

The group the composition factors of which are prime numbers is called metacyclic group. Every group of prime order p should be a metacyclic group. According to the Galois procedure, after having supposed we have adjoined a root (adjoint root), we shall take the first maximum invariant subgroup H_1 of G. In this case, the number of permutations not still browsed diminishes, becoming equal to n_1. Then, after adjoining another root, the numbers of permutations, not still browsed, becomes smaller, equal to n_2, and so on. Therefore, finally we shall obtain several composition subgroups represented by the successive maximum invariant subgroups and the corresponding

composition factors. There remains to establish how to choose the permutations subgroups. As already mentioned, the number of permutations of a subgroup must divide the number of permutations of the group to which it belongs. For each of the steps above, it means that we have to verify a smaller numbers of equalities, corresponding to a smaller number of roots that have to be adjoined. Therefore, referring to the example of Galois for a quartic polynomial, the total number of permutations may be: $4!=24$. The successive subgroups will be: $\boldsymbol{G}_{\text{sym}}=24;\ \boldsymbol{H}_1=12;\ \boldsymbol{H}_2=4;\ \boldsymbol{H}_3=2;\ \boldsymbol{H}_4=1;\ \boldsymbol{H}_{\text{id}}=1;$ and the composition factors will be: $f:\frac{24}{12}=2;\ \ \frac{12}{4}=3;\ \ \frac{4}{2}=2;\ \ \frac{2}{1}=2;\ \ 1$. We can see that every composition factor is a prime number. From the above description, there results the Galois conclusion that for the considered equation could be solvable by radicals, the composition factors, explained above should be prime numbers. Here, the digit 1 is included as prime, although in many works it is not accepted its denomination of prime, but keeping all known properties, that in the present case are included.

Each group of prime order is a cyclic group. For this reason, a metacyclic group contains a cyclic group.

7.1. Conjugate quantities. They are defined as follows. Let α_k be a set of quantities which all depend on one of them, like of $x_1=r_1^{1/p}$ in any number field F becoming a number field $F'=F\left(r^{1/p}\right)$. The quantities $\varphi(\alpha_k)$, and consequently x_k are called as conjugate quantities with respect to F, [11, p. 140].

7.2. An equation which is solvable by radicals contains a metacyclic group. This result follows from the procedure called by Galois reduction of the permutation group of an equation. Consider that an equation of degree n is solvable by radicals. We shall have in view the various radicals which occur. We can examine only the case of prime number radicals, because the other cases may be reduced to the mentioned one, by expressing the respective numbers using products of prime numbers. If we express the various occurring radicals as $x=r^{1/p}$, we can rewrite it as:

$$x_k=\sqrt[p]{r}\cdot\exp\left(\frac{2\cdot\pi}{p}\cdot i\cdot k\right);\quad k\in[2,p], \tag{15}$$

where, p is the smallest number, so that the adjunction of x_k will reduce the group of the given equation, while r belongs to the starting number field F. We shall obtain $p-1$ complex numbers (if $p\geq 3$) and one equal to the arithmetic radical of modulus r (if it is a positive real number). The adjunction of these radicals will not change the group of the equation, because as mentioned, they concern only indices less than p. Assuming that the value so obtained for the roots, and r has an adequate value, one can express the given equation in the form of a binomial product of factors $(x-x_k)$, and the numbers of permutations will be reduced with the number of corresponding binomials, being a maximum invariant subgroup. The ratio between the permutations group orders (namely numbers of permutations), i.e., the value of corresponding composition factor will be $\frac{\text{ord}\,H_k}{\text{ord}\,H_{k+1}}=f_k$, a prime number. For instance, if we started from a group with n elements, we find the number $n!$ permutations. After reducing the square roots of unity, we reduce the number of permutations to $\frac{n!}{2}$. We have to continue the procedure. After reducing the radical of the third order, $p=3$, starting from the number $n!$ permutations, we reduce the number to $\frac{n!}{p}$ permutations. If the composition factor will be in this case a prime number, the result of the preceding ratio should also be

a prime one, otherwise, the group will not be metacyclic, and the equation not solvable by radicals. Therefore, the respective equation should be metacyclic. We continue the procedure till we arrive at the identical permutation (unit permutation).

We shall give a simple explanation, for the case of a quartic equation, referring only to explanations above, without resorting to the usual ones. According to the definition, the total number of permutations, in this case, is $n=4!$. After adjoining the roots corresponding to $p=2$, the next number of permutations will be $\frac{24}{2}=12$. Then, after adjoining the roots corresponding to $p=3$, the next number of permutations will be $\frac{12}{3}=4$. Finally, after adjoining the roots corresponding to $p=4$, which being not prime number, will be replaced, as explained, by the product of prime numbers, hence we shall use, successively, twice $p=2$. The next numbers of permutations will be $\frac{4}{2}=2$, and $\frac{2}{2}=1$. Therefore, we arrive at the identical permutation. With this explanation, we found the same result as in the Galois explanation, but avoiding the presentation of permutation groups. Thus, the considered equation group contains a metacyclic group.

It is to be noted that it is possible that any radical does not introduce an imaginary component. Such an example can be found in the case of the equation we studied in [12], but for other aims. It still remains to prove that if an equation contains a metacyclic group, it is solvable by radicals. For proving it, Galois and his successors used a proposition by which all roots of an algebraic equation can be obtained from a single root of the Galois transformed equation. In fact, if a group is cyclic, it suffices to take a single element of the set of roots, and implicitly all become known.

7.3. Adjoining the root from a binomial equation. Let us assume that the root x_1 of a normal equation $f(x)=0$, that means irreducible in a number field F, has been known and adjoined to number field F. Similarly, also the other roots have successively been introduced.

Consequently, the considered equation being metacyclic, we obtain a number field F' containing all roots, including all conjugate roots, and thus the solution of the equation, like previously. Finally, it is worth noting that the reason for using the permutation group is for verifying, in principle, that the adjoined quantities fulfil the given equation.

Although the procedure is interesting and logically justified, its practical utilization cannot lead to useful results. For clarifying this problem, we performed the following numerical experiment. We considered the equation (polynomial) of [9]:

$$y=x^3-\frac{3}{2}\cdot x^2+1 \tag{16}$$

and tried to reduce its group by adjoining a root x_k of the binomial equation:

$$r^p=q, \tag{17}$$

where the right-hand side q of the equation, belongs to the initial number field, like F, and p is any prime number [9], as previously explained. But, not knowing a value of the roots, we can use anyone, assuming the possibility of reducing the equation group.
At the same time, we made a graphical representation of the function f as ordinate in terms of the abscissae x. The results can be seen in Fig. 1, which is plotted over the abscissae included in the domain of the roots. The used Maple commands are given below.

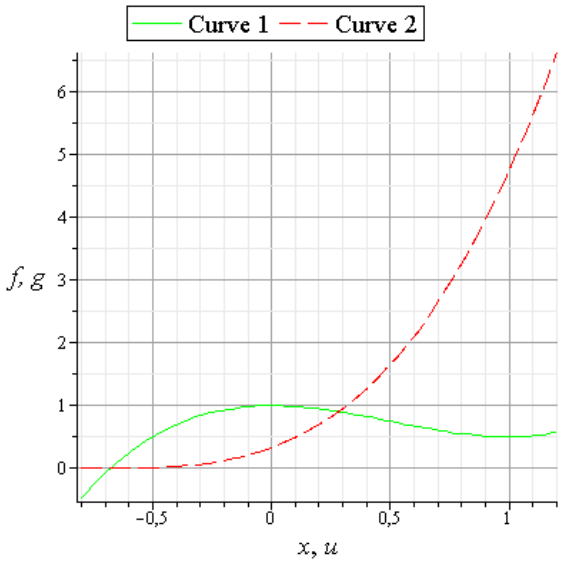

Fig. 1. The curves of the polynomial function in terms of the abscissae which include the roots. Curve 1, obtained by Maple plot; Curve 2, obtained after a root adjunction. Case of a real root and a pair of complex conjugate roots.

The Maple commands (in Maple, the imaginary unit is denoted by I):
Line Solid; Line Dash; Plot Axes normal; Show Legenda; Export.
$solve(evalf(f))$;
Roots of f :

$x[1] = 1.088825349 + I \cdot 0.5386519064$; $x[2] = 1.088825349 - I \cdot 0.5386519064$;
$x[3] = -0.6776506988$;
Roots for start adjunctions of g (in fact the Galois Theory does not imply numerical results):
$u[1] := x[1]$; $u[2] := x[2]$; $u[3] := x[3]$;
$u[1] := u[1]$; $u[2] := u[2]+1$; $u[3] := u[3]+1$;
$f = \text{expand}((x - x[1]) \cdot (x - x[2]) \cdot (x - x[3]))$;
$g = \text{expand}((u - u[1]) \cdot (u - u[2]) \cdot (u - u[3]))$;
$plots[multiple](plot, [f, x = -0.8..1.2, colour = green], [g, u = -0.8..1.2])$;

There follows that the curve 1 (solid line) intersects the axis of abscissae at a single point. Hence, the equation has a single real and two complex conjugate roots. In the same figure, we have also represented by curve 2 (dashed line), the resulting curve after adjoining roots. The single power to be reduced is that corresponding to $p = 2$. If we select a negative value of q, the equation (17) will deliver a pair of complex conjugate roots what, as seen, is acceptable, but we could, as well, select a positive value of q. For both selections, the automorphisms and the Galois groups will be of the same form.

In general, a polynomial equation of odd degree should have an odd number of real roots; while a polynomial equation of even degree must have an even number of real roots. In the case of Fig. 1, the order of the equation is odd, then using the constant term of the equation, we obtain a real root. However, for the taken value of x_2 differing by 1.1, or by 0.99 from the correct value, the obtained curve does not intersect the axis of abscissae, at any point within the roots limits, whereas when it differs by 1, it intersects this axis at a point. There follows that the procedure, is not adequate for solving an equation, but the mentioned difficulty does not influence the Galois condition of solvability [9]. It is useful to be noted that if we calculate the value of the discriminant, of the considered equation by Maple, we obtain:

$$\text{Discr} := discrim(y, x) = -\frac{27}{2}, \tag{18}$$

what means that the equation has a real root and two roots complex conjugate, hence correct result. We shall now give an example different from the previous one. Consider the following equation:

$$y = x^3 - 3 \cdot x^2 + 1, \tag{19}$$

we have studied in [12]. Like before, we shall perform the representation of the curve y for two cases, the first according to the given equation, when we know the roots of the equation, and then, considering the role of binomials from the case of reducing the group of the equation. The formulae and the results we need are the following:

$solve(evalf(f))$;

Roots of f :

$x[1] = -0.1774041483; \quad x[2] = 0.188598641; \quad x[3] = 2.988805500$.

Roots for start adjunctions of g :

$u[1] := x[1]; \quad u[2] := x[2]; \quad u[3] := x[3];$

$u[1] := u[1]; \quad u[2] := u[2]; \quad u[3] := u[3] + 0.2;$

$f = \text{expand}((x - x[1]) \cdot (x - x[2]) \cdot (x - x[3]))$;

$g = \text{expand}((u - u[1]) \cdot (u - u[2]) \cdot (u - u[3]))$;

$g = plots[multiple](plot, [f, x = -0.2..3, colour = green], [g, u = -0.2..3, colour = red])$;

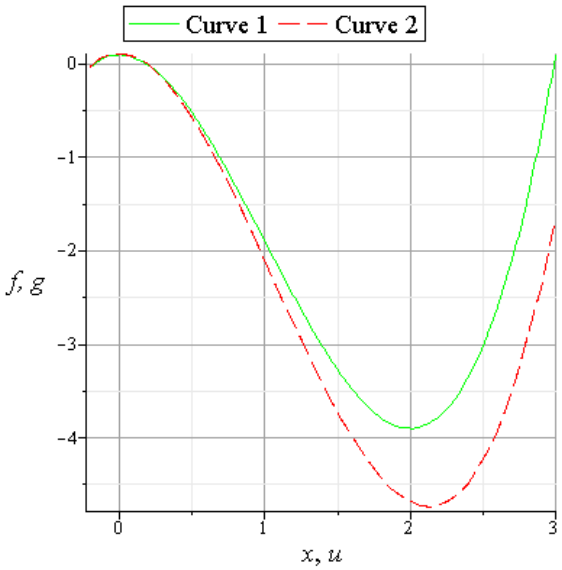

Fig. 2. The curves of the polynomial function in terms of the abscissae which include the roots. Curve 1, obtained by Maple plot; Curve 2, obtained after roots adjunction. Case of all real roots.

We tried to reduce its group by adjoining a root. In the previous example, we obtained a pair of complex conjugate roots. In the case of Fig. 2, the situation of the previous figure is not possible, because the curve intersects at three points the axis of abscissae, hence there must be three real roots. We shall take $p = 2$ and select a real positive value of letter q, what yields two real roots. As previously, the degree of the equation being odd, resorting to the constant term in the equation, we obtain another real root. We calculate the discriminant as previously and obtain $Discr = 81$, what means that the equation has all three roots real numbers. Such specific situations have not been found in the known literature, [2, p. 510].

If the group of a polynomial equation is not metacyclic, the equation cannot be solved algebraically (i.e., including radicals).

8. CONSIDERATIONS ON THE GALOIS GROUP

We shall give an example, but use notation close to that of Galois, which seems to be best oriented for a logical analysis:

$$\left(x^2-3\right)^2+7=0;\quad x^4-6x^2+16=0;\quad x_1=\sqrt{3+\sqrt{-7}};\quad x_2=\sqrt{3-\sqrt{-7}};$$
$$x_3=-\sqrt{3+\sqrt{-7}};\quad x_4=-\sqrt{3-\sqrt{-7}}. \tag{20}$$

The Galois group, will be described in the rational number field $\boldsymbol{Q}$, and could, in principle, have 24 permutations. There are several possible definitions for the group of an equation. Let $f(x)=0$ be the general form of a polynomial equation in number field F. The group of this equation, also called Galois group, is expressed by the set of permutations of the roots, which do not modify any relation among these roots, over the number field F, [11, p. 193]. Hence, the Galois group keeps or permutes the roots, according to their type, without modifying the results.

According to Verriest [11. p. 170], the Galois group is considered being the set of permutations by which we can pass from the first to the last root. There is interesting to remark that in the latter definition, the condition of the former one is not mentioned, but it is implicitly satisfied.

We obtained:

$$\mathrm{I}=\begin{pmatrix} x_1\to x_1\\ x_2\to x_2\\ x_3\to x_3\\ x_4\to x_4\end{pmatrix},\quad \mathrm{II}=\begin{pmatrix} x_1\to x_2\\ x_2\to x_1\\ x_3\to x_4\\ x_4\to x_3\end{pmatrix},\quad \mathrm{III}=\begin{pmatrix} x_1\to x_3\\ x_2\to x_4\\ x_3\to x_1\\ x_4\to x_2\end{pmatrix},\quad \mathrm{IV}=\begin{pmatrix} x_1\to x_4\\ x_2\to x_3\\ x_3\to x_2\\ x_4\to x_1\end{pmatrix}. \tag{21 a}$$

It is possible to express the Galois group in cycle form.

The permutations above, written in the two-rows form, are:

$$\mathrm{I}=\begin{pmatrix} x_1\,x_2\,x_3\,x_4\\ x_1\,x_2\,x_3\,x_4\end{pmatrix},\ \mathrm{II}=\begin{pmatrix} x_1\,x_2\,x_3\,x_4\\ x_2\,x_1\,x_4\,x_3\end{pmatrix},\ \mathrm{III}=\begin{pmatrix} x_1\,x_2\,x_3\,x_4\\ x_3\,x_4\,x_1\,x_2\end{pmatrix},\ \mathrm{IV}=\begin{pmatrix} x_1\,x_2\,x_3\,x_4\\ x_4\,x_3\,x_2\,x_1\end{pmatrix}. \tag{21 b}$$

The expressions of these permutations, in cycle form, are:

$$\mathrm{I}=E,\quad \mathrm{II}=(x_1\,x_2)(x_3\,x_4),\quad \mathrm{III}=(x_1\,x_3)(x_2\,x_4),\quad \mathrm{IV}=(x_1\,x_4)(x_2\,x_3). \tag{22}$$

Summing up the subgroups of permutations, with the usual symbols of the group theory, we obtain:

$$G\coloneqq E,(x_1\,x_2)(x_3\,x_4),(x_1\,x_3)(x_2\,x_4),(x_1\,x_4)(x_2\,x_3), \tag{23}$$

or according to the notation of [11, p. 170]:

$$G\coloneqq E+(x_1\,x_2)(x_3\,x_4)+(x_1\,x_3)(x_2\,x_4)+(x_1\,x_4)(x_2\,x_3). \tag{23 a}$$

The cyclic form can be directly explained, because it does not keep the same value for any order of the roots, different from that of the unit permutation.

According to Maple, the equation group is:

$$\text{"1T1"},\{\text{"Id"}\},\text{"+"},1,\{\text{""}\}; \tag{24}$$

where the notation is the same as in [4] and [9].

9. RELATION BETWEEN THE INDICES OF THE ROOTS OF A SOLVABLE EQUATION

Another question to be examined is the following. The majority of the authors consider the reduction of the equation group. They try to replace the various radical represented by the solution of an equation, adjoining binomial expressions, starting with the smallest radical which can lead to the

reduction of the permutation group and the solution by radicals. Galois stated that, in the case of solvability, a certain relation among the indices of roots in the permutation group exists, but did not give a detailed proof. His followers, Serret [13] and Picard [2] presented some proofs. According to our opinion, the clear and simplest deduction results from the book of Verriest, although not given or expressed there as such. As follows, no calculations are required.

An equation solvable by radicals is a metacyclic equation [11, p. 277]. Consequently its group is a metacyclic one. All its composition factors are prime numbers [11, p. 81], and its group is a cyclic group [11, p. 81]. All prime groups are cyclic groups [11, p. 25]. But in the case of a cyclic group, the number of permutations is equal to that of the equation degree. There follows that every solvable equations must have a similar group, and the equations may be considered as similar. Therefore, the index of the roots will fulfil the same number order. It is worth noting that if we use the permutation group valid for a metacyclic group, it is not valid for any equation type. If, for example, the expression of a root contained two radicals of second degree of different expressions, a single adjunction of a root could not satisfy two different conditions.
The example gives for some entry numbers, the output numbers, denoted by z, which repeat the order of the former.
In this case, the permutation group can be written so that the number of permutations (i.e., permutation rows) should be equal to that of the equation degree, as below, [1, Proposition 7] in expression (25). It follows that in the group of one equation of degree p, solvable by radicals, the permutation succession should be of the form in (26) and (27).
Concerning the calculation of the indices, respecting the result for cyclic and metacyclic equations, it can be presented, very simply, using Maple 12 program for changing permutation indices.

Maple 12 Program

$i := 2;$
$q := 3; \quad r := 4;$
$n := 5;$
$z := i \cdot q + r;$
$u := z \bmod n;$
if $u = 0$ then print(n) end if ;
5

Symbols
$i - initial\ index;$
$q, r - whole\ numbers;$
$n := - numbers\ per\ row;$
$z := i \cdot q + r;$
$u := z \bmod n;$
$u - number\ along\ period;$

The numbers are like examples.

$$S := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}, \quad (25)$$

In the simplest form

$$x_k \to x_{k+1} \qquad (26)$$

In the more general form

$$x_k \to x_{ak+b} \qquad (27)$$

a and b integer constants

We did not find an intuitive remark of this content, in the known literature.

10. CONCLUSION

We should mention that the main steps have been the Galois transform of the given equation and the concept of root group, because they emphasized the existence of the circular permutation character of transformed roots arriving at metacyclic equations. Certain interesting subjects of the Galois Theory, concerning the solvability of equations and other questions, were developed by many authors, but in

most cases, they have avoided the difficulty which blocks, in many cases, their applicability. Several such cases have been analysed and intuitive examples for avoiding certain difficult situations have been explained in the present paper. We must add the mentioned circumstances do not affect the utility and importance of the usual Galois condition of solvability.

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

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

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

[5]. Th. Anghelutza, Curs de de Algebră superioară (A Course of higher Algebra), Vol. II, Editura Universității 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, Considerations on certain Theorems of the Galois Theory, International Journal of Scientific and Innovative Mathematical Research (IJSIMR), Volume II, Issue 11, 2014, pp. 880-891.

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

[11]. 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.

[12]. 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.

[13]. E. Artin, Galois Theory, Edited and supplemented by and A.N. Milgram with a Section on Applications, University of Notre Dame Press, London, 1971.

[14]. J.A. Serret, Cours d'algèbre supérieure, (2 vol.) Gauthier-Villars, Paris, 1866.

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.