International Journal of Scientific and Innovative Mathematical Research (IJSIMR)
Volume 4, Issue 1, January 2016, PP 1-7
ISSN 2347-307X (Print) & ISSN 2347-3142 (Online)
www.arcjournals.org

Revisiting Certain Demonstrations of the Galois Theory of Equations

Andrei Nicolaide

Professor, D.Sc.
Faculty of Electrical Engineering and Computer Science
Department of Electrical Engineering and Applied Physics
Transilvania University of Brasov
Brasov, Romania
andrei.nicolaide@gmail.com

Abstract: *As we have previously shown in several papers, certain statements of the Galois Theory require to make clarifications and disambiguation. An important theorem in the Galois Theory is that whatever be the given equation, it is possible to find a rational function* y *of its roots so that each root be a rational function of* y. *Examining the results obtained by Galois, we could establish that these are not verified in the case of numerical verification. The subsequent contributions, we have found, did not change this consideration. Starting from our several previous contributions, we shall present a justified deduction, using for this aim a symbolic software for allowing us this analysis.*

Keywords: *Galois Theory, Transform equation, Galois group, Resolvent.*

1. Introduction

The Galois Theory has been largely developed by him and his followers, among which [1]-[12]. A very interesting result was the transform of the polynomial equation belonging to Galois and forming the equation called resolvent equation. For the sake of simplicity, as already mentioned, we shall call the roots of the given equation as *input* roots, and those of the transformed equation, i.e. the resolvent equation, as *output* roots. We shall use the notation of [8] and [9] even when referring to Galois results, for the sake of uniformity, except the formulae numbering, which will be with Latin numbers. 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 it is possible to form a function y 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:

$$y = A_1 x_1 + A_2 x_2 + A_3 x_3 + \ldots + A_n, \tag{II}$$

where $A_1, A_2, A_3, \ldots$ are integer numbers. The function y, chosen as above, will have the property that all roots of the given equation will be rationally expressed in terms of y. Therefore:

$$y = \Phi(x_1, x_2, x_3, x_4, \ldots); \qquad y - \Phi(x_1, x_2, x_3, x_4, \ldots) = 0. \tag{III}$$

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

$$\Phi(y, x_1) = 0. \tag{IV}$$

Hence, any root of the given equation can be expressed in terms of one root of the transformed equation, the resolvent. It is obvious that the value of y cannot depend only on x_1, but, what is not mentioned, also of the other quantities existing in the dependence, regardless if there are actually constant or not. In the text of Galois no mention is made concerning this circumstance.

2. The Equations Satisfied by the Input and Output Roots of a Polynomial 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 we shall obtain will be from two sources, the first three equations, those which achieve the transformation, according to Galois, also called the Galois resolvent, and the next three equations, the Viète relations between the roots and the coefficients of the given equation:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad (1)$$

eqn1:= $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 - y_1$; (2)

eqn2:= $\alpha_2 x_1 + \alpha_3 x_2 + \alpha_1 x_3 - y_2$; (3)

eqn3:= $\alpha_3 x_1 + \alpha_1 x_1 + \alpha_2 x_2 - y_3$; (4)

eqn4:= $x_1 + x_2 + x_3 + a_1$; Here and further on, a_1 is the sum of the roots with changed sign. (5)

eqn5:= $x_1 x_2 + x_1 x_3 + x_2 x_3 - a_2$; (6)

eqn6:= $x_1 x_2 x_3 + a_3$; (7)

For to fix the ideas, we shall consider the following values of the given equation:

$x_1 := 1; x_2 := 2; x_3 := 4;$ (8 a)

$a_1 := -7; a_2 := 14; a_3 := -8;$ (8 b)

$\alpha_1 := 4; \alpha_2 := 2; \alpha_3 := 9.$ (8 c)

There remains to choose the values of the coefficients involved in the transformation of the given equation. For this purpose, Galois proposed to use only whole numbers (integers). In the chosen case, according to Galois, we shall have 6 equations of first degree, with 6 roots of the resolvent equation, and one equations of third degree for the three roots corresponding to the given equation. Also, we should have a linear dependence between the output and input roots. In order to find such a situation, in our preceding analysis [8], we used for the three coefficients of transformation the three roots of unity, containing two complex numbers, which permitted to avoid a degree greater than unity. It is worth noting that, when using the Galois procedure, it is possible that the unknown coefficient appears at a higher power than unity. The places of functions φ_i are given in [1, p. 53], without a precise computational justification. In [12], Edwards wrote, that in his Table, in columns 2, 3, 4, Galois, did not use certain parentheses, and Edwards gave an explanation, how could be understood the respective table results.

Table 1.

Output roots	Input roots including three permutations		
y_1	$x_1 = \varphi_1 y_1$	$x_2 = \varphi_2 y_1$	$x_3 = \varphi_3 y_1$
y_2	$x_2 = \varphi_1 y_2$	$x_3 = \varphi_2 y_2$	$x_1 = \varphi_3 y_2$
y_3	$x_3 = \varphi_1 y_3$	$x_1 = \varphi_2 y_3$	$x_2 = \varphi_3 y_3$

Further on, we shall examine several cases, in order to obtain the existing dependence between the input and the output roots.

2.1. First case

The task is in fact very clear, to establish, the relation existing between an input root and an output root. Now, let us find the relations between x_1 and y_1 by a computational procedure.

$\# x_1 := 1;$
$\# x_2 := 2;$
$\# x_3 := 4;$

$\# a_1 := -7;$
$\# a_2 := 14;$
$\# a_3 := -8;$

$\# \alpha_1 := 4;$
$\# \alpha_2 := 2;$
$\# \alpha_3 := 9;$

$\# y_1 := \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3;$
$\# y_2 := \alpha_2 x_1 + \alpha_3 x_2 + \alpha_1 x_3;$
$\# y_3 := \alpha_3 x_1 + \alpha_1 x_2 + \alpha_2 x_3;$

We have blocked the identifiers above, in order to firstly obtain the general form of needed expressions, regardless the numerical values;

A very simple solution is the elimination using the next Maple command:

$$\# w_{11} := \text{eliminate}\left(\{eqn1, eqn4, eqn5\}, \{x_2, x_3\}\right); \tag{9}$$

$eqn1 := \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 - y_1;$
$eqn4 := x_1 + x_2 + x_3 + a_1;$
$eqn5 := x_1 x_2 + x_2 x_3 + x_3 x_1 - a_3;$

eliminate$(\{eqn1, eqn4, eqn5\}, \{x_2, x_3\});$

The program command above will deliver the expressions of x_2, x_3, and an expression which equated to zero, contains x_1 and y_1.

The result is:

$$\left\{x_2 = \frac{\alpha_3 x_1 - \alpha_1 x_1 + a_1\alpha_3 + y_1}{\alpha_2 - \alpha_3}, \quad x_3 = -\frac{-\alpha_1 x_1 + \alpha_2 x_1 + a_1\alpha_2 + y_1}{\alpha_2 - \alpha_3}\right\},$$

$$\left\{\begin{array}{l} -a_1\alpha_1\alpha_2 x_1 - a_1\alpha_1\alpha_3 x_1 \\ +\alpha_1^2 x_1^2 + \alpha_2^2 x_1^2 + \alpha_3^2 x_1^2 - \alpha_1\alpha_2 x_1^2 - \alpha_2\alpha_3 x_1^2 - \alpha_1\alpha_3 x_1^2 + y_1^2 + a_1\alpha_2^2 x_1 + \alpha_2 x_1 y_1 + \alpha_3 x_1 y_1 \\ +a_1\alpha_3^2 x_1 - 2\alpha_1 x_1 y_1 + a_1\alpha_2 y_1 + a_1^2\alpha_2\alpha_3 + a_1\alpha_3 y_1 - 2a_2\alpha_2\alpha_3 + a_2\alpha_2^2 + a_2\alpha_3^2 \end{array}\right\}$$

The function delivering the equation containing the required input root x_1 as a function of the output root $y_1 = 44$:

$\# W := -a_1\alpha_1\alpha_2 x_1 - a_1\alpha_1\alpha_3 x_1$
$+\alpha_1^2 x_1^2 + \alpha_2^2 x_1^2 + \alpha_3^2 x_1^2 - \alpha_1\alpha_2 x_1^2 - \alpha_2\alpha_3 x_1^2 - \alpha_1\alpha_3 x_1^2 + y_1^2 + a_1\alpha_2^2 x_1 + \alpha_2 x_1 y_1 + \alpha_3 x_1 y_1$
$+a_1\alpha_3^2 x_1 - 2\alpha_1 x_1 y_1 + a_1\alpha_2 y_1 + a_1^2\alpha_2\alpha_3 + a_1\alpha_3 y_1 - 2a_2\alpha_2\alpha_3 + a_2\alpha_2^2 + a_2\alpha_3^2;$

Given data:
$a_1 := -7;$
$a_2 := 14;$
$a_3 := -8;$

$\alpha_1 := 4;$
$\alpha_2 := 2;$
$\alpha_3 := 9;$

$y_1 = 44;$
Command
$W := -a_1\alpha_1\alpha_2 x_1 - a_1\alpha_1\alpha_3 x_1$
$+ \alpha_1^2 x_1^2 + \alpha_2^2 x_1^2 + \alpha_3^2 x_1^2 - \alpha_1\alpha_2 x_1^2 - \alpha_2\alpha_3 x_1^2 - \alpha_1\alpha_3 x_1^2 + y_1^2 + a_1\alpha_2^2 x_1 + \alpha_2 x_1 y_1 + \alpha_3 x_1 y_1$
$+ a_1\alpha_3^2 x_1 - 2\alpha_1 x_1 y_1 + a_1\alpha_2 y_1 + a_1^2\alpha_2\alpha_3 + a_1\alpha_3 y_1 - 2a_2\alpha_2\alpha_3 + a_2\alpha_2^2 + a_2\alpha_3^2;$

The function delivering the equation containing the required root x_1:

W:=$39x^2 - 155x + 116;$

$$x_1 = x = \frac{155 + \sqrt{155^2 - 4\cdot 39\cdot 116}}{2\cdot 39} = \frac{116}{39}; \quad x_1' = x' = \frac{155 - \sqrt{155^2 - 4\cdot 39\cdot 116}}{2\cdot 39} = 1.$$

2.2. Second case

Now, let us find the relations between x_1 and y_2 by a computational procedure. A very simple solution is the elimination using the next Maple command.

The first part of the Maple program will be till before the command *eliminate,* like the previous. The rest as below.

eliminate($\{eqn2, eqn4, eqn5\}, \{x_2, x_3\}$);
# The result:

$$\left\{x_2 = -\frac{\alpha_1 x_1 - \alpha_2 x_1 + a_1\alpha_1 + y_2}{\alpha_1 - \alpha_3},\quad x_3 = \frac{-\alpha_2 x_1 + \alpha_3 x_1 + a_1\alpha_3 + y_2}{\alpha_1 - \alpha_3}\right\},$$

$$\left\{\begin{array}{l} -2\alpha_2 x_1 y_2 + \alpha_1 x_1 y_2 \\ + \alpha_3 x_1 y_2 - \alpha_1\alpha_3 x_1^2 + a_1\alpha_3^2 x_1 + a_1\alpha_3 y_2 - 2a_2\alpha_1\alpha_3 + a_1\alpha_1 y_2 + a_1^2\alpha_1\alpha_3 - \alpha_1\alpha_2 x_1^2 \\ + a_1\alpha_1^2 x_1 - \alpha_2\alpha_3 x_1^2 - a_1\alpha_1\alpha_3 x_1 - a_1\alpha_2\alpha_3 x_1 + \alpha_1^2 x_1^2 + \alpha_2^2 x_1^2 + \alpha_3^2 x_1^2 + y_2^2 + a_2\alpha_1^2 + a_2\alpha_3^2 \end{array}\right\}$$

The function delivering the equation containing the required input root x_1 as a function of the output root $y_2 = 36$.

W:=$-2\alpha_2 x_1 y_2 + \alpha_1 x_1 y_2$
$-\alpha_2\alpha_3 x_1^2 - a_1\alpha_2\alpha_3 x_1 + a_1\alpha_3^2 x_1 + a_1\alpha_3 y_2 - 2a_2\alpha_1\alpha_3 + a_1\alpha_1 y_2 + a_1^2\alpha_1\alpha_3 - \alpha_1\alpha_2 x_1^2$
$+ a_1\alpha_1^2 x_1 - \alpha_2\alpha_3 x_1^2 - a_1\alpha_1\alpha_2 x_1 - a_1\alpha_2\alpha_3 x_1 + \alpha_1^2 x_1^2 + \alpha_2^2 x_1^2 + \alpha_3^2 x_1^2 + y_2^2 + a_2\alpha_1^2 + a_2\alpha_3^2;$

Given data;
$a_1 := -7;$
$a_2 := 14;$
$a_3 := -8;$
$\alpha_1 := 4;$
$\alpha_2 := 2;$
$\alpha_3 := 9;$
$y_2 := 36;$

Command:

$$W:=-2\alpha_2 x_1 y_2+\alpha_1 x_1 y_2$$
$$-\alpha_2\alpha_3 x_1^2-a_1\alpha_2\alpha_3 x_1+a_1\alpha_3^2 x_1+a_1\alpha_3 y_2-2a_2\alpha_1\alpha_3+a_1\alpha_1 y_2+a_1^2\alpha_1\alpha_3-\alpha_1\alpha_2 x_1^2+a_1\alpha_1^2 x_1$$
$$-\alpha_2\alpha_3 x_1^2-a_1\alpha_1\alpha_2 x_1-a_1\alpha_2\alpha_3 x_1+\alpha_1^2 x_1^2+\alpha_2^2 x_1^2+\alpha_3^2 x_1^2+y_2^2+a_2\alpha_1^2+a_2\alpha_3^2;$$

The function delivering the equation containing the required root x_1:
$W:=-173x_1+39x_1^2+134;$

$$x_1=x=\frac{173+\sqrt{173^2-4\cdot 39\cdot 134}}{2\cdot 39}=\frac{134}{39};\quad x_1'=x'=\frac{173-\sqrt{173^2-4\cdot 39\cdot 134}}{2\cdot 39}=1.$$

2.3. Third case

Now, let us find the relations between x_3 and y_2 by a computational procedure. A very simple solution is the elimination using the next Maple command:

The first part of the Maple program will be till before the command *eliminate,* like the previous. The rest as below.

eliminate($\{eqn2, eqn4, eqn5\},\{x_1,x_2\}$);

The result:

$$\left\{x_1:=\frac{-\alpha_1 x_3+\alpha_3 x_3+a_1\alpha_3+y_2}{\alpha_2-\alpha_3};\ x_2:=-\frac{-\alpha_1 x_3+\alpha_2 x_3+a_1\alpha_2+y_2}{\alpha_2-\alpha_3};\right\},$$

$$\left\{\begin{array}{l}a_1^2\alpha_2\alpha_3+a_1\alpha_3 y_2\\ +a_1\alpha_3^2 x_3+a_1\alpha_2 y_2+\alpha_2 x_3 y_2+a_1\alpha_2^2 x_3-2\alpha_1 x_3 y_2-\alpha_1\alpha_2 x_3^2-2a_2\alpha_2\alpha_3+\alpha_3^2 x_3^2+a_2\alpha_2^2\\ +a_2\alpha_3^2-\alpha_1\alpha_3 x_3^2-\alpha_2\alpha_3 x_3^2+y_2^2+\alpha_3 x_3 y_2+\alpha_1^2 x_3^2+\alpha_2^2 x_3^2-a_1\alpha_1\alpha_2 x_3-a_1\alpha_1\alpha_3 x_3\end{array}\right\}$$

#Command:

The function delivering the equation containing the required input root x_3 as a function of the output root $y_2=36$.

$$\#\cdot W:=a_1^2\alpha_2\alpha_3+a_1\alpha_3 y_2$$
$$+a_1\alpha_3^2 x_3+a_1\alpha_2 y_2+\alpha_2 x_3 y_2+a_1\alpha_2^2 x_3-2\alpha_1 x_3 y_2-\alpha_1\alpha_2 x_3^2-2a_2\alpha_2\alpha_3+\alpha_3^2 x_3^2+a_2\alpha_2^2$$
$$+a_2\alpha_3^2-\alpha_1\alpha_3 x_3^2-\alpha_2\alpha_3 x_3^2+y_2^2+\alpha_3 x_3 y_2+\alpha_1^2 x_3^2+\alpha_2^2 x_3^2-a_1\alpha_1\alpha_2 x_3-a_1\alpha_1\alpha_3 x_3;$$

Given data

$a_1:=-7;$
$a_2:=14;$
$a_3:=-8;$

$\alpha_1:=4;$
$\alpha_2:=2;$
$\alpha_3:=9;$
$y_2:=36;$

Command

$$W:=a_1^2\alpha_2\alpha_3+a_1\alpha_3 y_2$$
$$+a_1\alpha_3^2 x_3+a_1\alpha_2 y_2+\alpha_2 x_3 y_2+a_1\alpha_2^2 x_3-2\alpha_1 x_3 y_2-\alpha_1\alpha_2 x_3^2-2a_2\alpha_2\alpha_3+\alpha_3^2 x_3^2+a_2\alpha_2^2$$
$$+a_2\alpha_3^2-\alpha_1\alpha_3 x_3^2-\alpha_2\alpha_3 x_3^2+y_2^2+\alpha_3 x_3 y_2+\alpha_1^2 x_3^2+\alpha_2^2 x_3^2-a_1\alpha_1\alpha_2 x_3-a_1\alpha_1\alpha_3 x_3;$$

The function delivering the equation containing the required input root x_3: $W := 92 - 179\,x_3 + 39\,x_3^2$.

$$x_3 = x = \frac{179 + \sqrt{179^2 - 4\cdot 39\cdot 92}}{2\cdot 39} = 4; \quad x_3' = x' = \frac{179 - \sqrt{179^2 - 4\cdot 39\cdot 92}}{2\cdot 39} = \frac{23}{39}.$$

The obtained results have been included in Table 2, below. In this table, the factor φ_{ij} means the values of x_i calculated above in terms of y_j.

Table 2.

Output roots	Input roots including three permutations. The first number before the semicolon is the value verified be an input root, while the next value is not accepted.		
$y_1 = 44$	$x_1 = \varphi_{11} = 1; 116/39$	$x_2 = \varphi_{21} = 2; 23/39$	$x_3 = \varphi_{31} = 4; 23/39$
$y_2 = 36$	$x_2 = \varphi_{22} = 2; 116/39$	$x_3 = \varphi_{32} = 4; 23/39$	$x_1 = \varphi_{12} = 1; 134/39$
$y_3 = 25$	$x_3 = \varphi_{33} = 4; 116/39$	$x_1 = \varphi_{13} = 1; 23/39$	$x_2 = \varphi_{23} = 2; 116/39$

As already mentioned, for expressing more easily, the roots of the given polynomial will be called input roots, and those of the transformed polynomial, i.e. Galois resolvent, output roots. It is worth noting that the output roots have not all the same values, because although the input roots are constant, but their order, when calculating each output root, is different. The system of equations contains 3 input roots and 6 output roots. There follows a set of three equations with three output roots and three input roots, and a set also of three equations, with three output roots, different from the previous ones, and three input ones, the same as the previous ones. According to Galois, as shown in Table 1, all input roots can be obtained from a single output root. However, for knowing any output root, it is necessary to know the values of all input roots which by composition yield the output root, but just these quantities are not given. They could be obtained by solving the resolvent equation, generally difficult, being of a degree greater that the degree of the given equation.

The coefficients of the given equation being: $-7; 14, -8$, it follows that only the results $1; 2, 4$ satisfy the given equation. To each permutation there corresponds a value of the output root y_i. If we use successively two different values of the output roots, we shall obtain two sets of the input roots, but their order may be different. If the considered polynomial is of a prime degree, and each permutation is deduced from the preceding one, then the number of permutations is equal to its degree.

3. Conclusion

If comparing the results of the two tables, there follows that those given by Galois in Table 1, based on certain logical deductions, but not verified, are not clear, their determination requiring a precise calculation, as we carried out. However, it is worth noting that the condition of solvability by radicals, belonging to Galois, namely the equation be metacyclic, [9, p. 2, 6, 12], is not affected. But, if we are interested in the relations among the input and output roots, it is necessary to apply an adequate procedure.

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 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] 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.

[9] A. Nicolaide, Revisiting Certain Procedures of the Galois Theory Using Symbolic Programming, International Journal of Scientific and Innovative Mathematical Research (IJSIMR), Volume 3, Issue 6, June 2015, pp. 1-13.

[10] 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.

[11] 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.

[12] H.M. Edwards, Galois for 21st -Century Readers, Notice of the AMS, Volume 59, Number 7, 2012, pp. 912-923.

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.