*ICASTOR Journal of Mathematical Sciences*
*Vol. 11, No. 1 (2017) 15 - 21*

# Computing Galois Groups with Resolvents

**M. C. Obi**

Department of Mathematics,
Federal University of Technology, Owerri.
Imo State,
Nigeria.

## ABSTRACT

Throughout this work, we let $f(X) \in Z|X|$ be a monic irreducible polynomial of degree n. The resolvent polynomial of $f(X)$ is recalled and defined, alongside the Galois group of $f(X)$. While the problem of computing Galois groups is one of serious interest, we describe some methods using resolvents for the determination of the Galois group of $f(X)$ with a solved example.

## INTRODUCTION

The main classical problem about $f(X)$ was its solution, that is expressing its roots as functions of known quantities. In particular, functions involving only rational operations and extractions of roots were looked for. This was completely solved for $n < 4$ already before Galois. In all cases the solution was accomplished by the solution of some auxiliary equations, called resolvent equations. Then, Galois introduced certain general resolvent polynomials, called Galois resolvents, having the property that any root of $f(X)$ is a rational function in the roots of them [3]. It became clear that resolvent polynomials are related to subgroups of the Galois group of $f(X)$; therefore, some resolvent polynomials were used to obtain conditions on the Galois group.

While the techniques used for the identification of Galois groups were known already in the last century [8], the involved calculations made it almost impractical to do computations beyond trivial examples. Today, given high level of development in the area of computing and programming techniques, the interest on resolvent polynomials has greatly grown, due to the corresponding growth in effective computability. Many interesting properties of resolvent polynomials have been found, and practical methods and algorithms are being developed for the determination of Galois group. Moreover, effective characterizations of polynomials with given Galois groups have been given, and more work is on the increase.

***Correspondence: Martins .C. Obi,*** *Department of Mathematics, Federal University of Technology, Owerri, Imo State, Nigeria. E-mail: henrymath1994@gmail.com*

Galois theory stands at the cradle of modern algebra and interacts with many areas of mathematics [1]. The problem of determining Galois groups therefore has been shown to be of serious interest not just in algebra, but also from the point of view of number theory leading to many questions in other areas of mathematics. This work intends to recall the definitions of the Galois group and Galois resolvents, and to describe some of the general methods using resolvents for the determination of the Galois group of $f(X)$.

## 1. Galois Group of $f(X)$

Suppose that $f \in K|X|$ and that $L : K$ is a splitting field extension for $f$ over $K$, then we call Gal $(L : K)$ the Galois group of $f$, denoted by Gal $(f)$. The Galois group of $f$ can be represented as a permutation group on the set of the roots $R$ of $f$. This means that the map Gal $(f) \rightarrow Sym(R)$ defined by $\sigma \rightarrow \sigma|_R$, where $R$ is the set of all the roots of $f$ is an injective group homomorphism. Therefore, we say that the group Gal $(f)$ is a (permutation) group of degree $n$; the number of elements in $R$: We summarize this in the theorem below.

**Theorem [4].** Suppose that $f \in K[X]$ and that $L : K$ is a splitting field extension for $f$ over $K$. Let $R$ denote the set of roots of $f$ in $L$. Each $\sigma$ in Gal $(f)$ defines a permutation of $R$, so that we have a mapping from Gal $(f)$ into the group $S_R$ of permutations of $R$. This mapping is a group homomorphism, and is one to one.

**Proof.** If $\sigma \in$ Gal $(f)$, then $\sigma(f) = f$, since $f$ has its coefficients in $K$. Thus, if $\sigma \in R$, then

$$f(\sigma(\alpha)) = \sigma(f)(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0.$$

Thus sigma maps $R$ into $R$. Since $\sigma$ is one-one and $R$ is finite, $\sigma|_R$ is a permutation. By definition,

$$(\sigma_1\sigma_2)(\alpha) = \sigma_1(\sigma_2(\alpha))$$

so that the mapping $\sigma \rightarrow \sigma|_R$ is a group homomorphism. Finally, if $\sigma(\alpha) = \tau(\alpha)$ for each $\alpha$ in $R$, then $\alpha^{-1}\tau$ fixes $K(R) = L$, so that $\sigma = \tau$.

It thus follows that the representation of Gal $(f)$ as a permutation group on $\{1, \dots, n\}$ is defined up to conjugation. In fact, taking different orderings of the roots is the same as considering equivalent representations of Gal $(f)$ as permutation group on $\{1, \dots, n\}$.

## 2. Resolvent Polynomials

We give several definitions of resolvent polynomials. In the classic literature, a rational resolvent polynomial of $f(X)$ is any irreducible polynomial $V(X) \in \mathbb{Q}[X]$ which splits into linear factors in $L[X]$. In other words, all the roots of $V$ belong to the splitting field of $f$, that is they can be written as rational functions of the roots of $f$ [10; 5; 13]. In particular, a Galois resolvent of $f$ is an irreducible polynomial $V \in \mathbb{Q}[X]$ such that $L =$

$\mathbb{Q}(\beta)$, for any root $\beta$ of $V$ . The best known Galois resolvents are the minimal polynomials of certain elements of the kind $m_1\alpha_1 + \cdots + m_n\alpha_n$ with $m_1, \dots, m_n$ rational integers. On the other hand, an irrational resolvent polynomial of $f$ is any irreducible polynomial $V \in \mathbb{Q}[X]$ which splits into linear factors over some finite extension $E$ of $L$. In other words, all the roots of $V$ belong to a finite extension $E$ of the splitting field of $f$, that is they can be written as rational functions of the roots of $f$ and of finitely more algebraic numbers [11].

A well known example of irrational resolvents are the Lagrange resolvents, whose roots all belong to the field $L(\varsigma)$, where $\varsigma$ is a suitable root of unity.

More so, fix a polynomial $F \in \mathbb{Z}[X_1, \dots, X_n]$ and fix an ordering of the roots of $f$. We define the resolvent of $f$ with respect to $F$ [14],

$$\begin{aligned} V(F,f)(X) &= \textstyle\prod_{s\in S_n/S}\big(X - sF(\alpha_1, \dots, \alpha_n)\big) \\ &= \textstyle\prod_{j=1}^{m}\left(X - s_jF(\alpha_1, \dots, \alpha_n)\right) \\ &= \textstyle\prod_{j=1}^{m}\left(X - F_j(\alpha_1, \dots, \alpha_n)\right) \end{aligned}$$

$V\ (F,f)$ is a monic polynomial of degree $[S_n\colon S]$, with integral coefficients. In fact, since $V\ (F,f)$ is left fixed by any permutation of the roots of $f$, its coefficients are symmetric polynomials in the roots of $f$, hence they can be written as integral polynomials in the elementary symmetric polynomials of the roots of $f$, that is in the coefficients of $f$. Furthermore, it is easily seen that the definition of $V\ (F,f)$ does not depend on the choice of the ordering of the roots of $f$. If we _x an ordering of the roots of f, the group Gal $(f)$ is uniquely determined. So we can fix a subgroup $H$ of $S_n$ such that $G \subset H$. Maintaining the above notations, we can define the resolvent of $f$ with respect to $F$ in $H$,

$$\begin{aligned} V_H(F,f)(X) &= \textstyle\prod_{s\in H/S_H}\big(X - sF(\alpha_1, \dots, \alpha_n)\big) \\ &= \textstyle\prod_{j=1}^{m'}\left(X - s'_{j'}F(\alpha_1, \dots, \alpha_n)\right) \\ &= \textstyle\prod_{j'=1}^{m'}\left(X - F'_{j'}(\alpha_1, \dots, \alpha_n)\right) \end{aligned}$$

$V_H(F,f)$ is a monic polynomial of degree $[H\colon S_H]$, and it has integral coefficients as well. In fact, $V_H(F,f)$ is left fixed by any element in Gal $(f)$, because $G \subset H$, hence it is left fixed by any element of the Galois group Gal $(f)$. It follows that the coefficients of $V_H(F,f)$ are rational, so, being algebraic integers, they are rational integers. Note that the definition of $V_H(F,f)$ does depend on the choice of the ordering of the roots of $f$ (on the other hand, the choice of $H$ already depends on the ordering).

## 3. Forming a Galois Resolvent.

Given that the coefficients of $V\ (F,f)$ can be written as integral polynomials in the coefficients of $f$, it would be hence possible to write down such polynomials, for any given $F$. Nevertheless, for large n such polynomials turn out to be of high degree and with large coefficients. Hence, in practice, a different method is followed for the computation of the resolvents. This method profits by the fact that the coefficients of $V\ (F,f)$ are rational integers. We fix some numerical approximations of the roots of $f$, $\{a_1,\dots,a_n\}$, and we compute the following product ($S_n$ acts on the $a_i'$ is by permuting their indices in the same way as it does on the $\alpha_i's$):

$$\prod_{s\in S_n/S}\left(X - sF\left(\alpha_{1,\dots,}\alpha_n\right)\right)$$

If the above approximations are "accurate enough", then the coefficients of this product are approximations of the coefficients of $V\ (F,f)$ within an absolute error less than $1/2$. So, they uniquely determine the coefficients of $V\ (F,f)$, which we know to be rational integers [14]. Such a method can be also applied to the computation of $V_H(F,f)$. However, in this case, we have to make the representation of Gal $(f)$ as permutation group on $R$ explicit: that is, we have to explicitly determine $G$ in relation with the chosen ordering of the roots of $f$.

**Example** Let $u(x) = x^3 - 2$. This is an irreducible polynomial with simple roots. Let the roots of $u$ be $a, b, c$. We form the Galois resolvent, choosing coefficients that are integers. To make the calculations easier for this example, the coefficients have been chosen with the prior knowledge that they yield different values of the resolvent for each conjugation. Normally, such a calculation would need to be carried out without explicit values for the coefficient. Let the resolvent and its conjugates be

$$V_0 = a + 2b + 3c,\ V_1 = c + 2a + 3b\ V_2 = b + 2c + 3a$$
$$V_3 = b + 2a + 3c,\ V_4 = c + 2b + 3a\ V_5 = a + 2c + 3b.$$

Then the polynomial with the values of the resolvent and its conjugates as roots is

$$\begin{aligned}U(X) &= (X - t_0)(X - t_1)(X - t_3)(X - t_4)(X - t_5)\\
&= X^6 - (t_0 + t_1 + t_2 + t_3 + t_4 + t_5)X^5\\
&+[(t_0 + t_1)(t_2 + t_3 + t_4 + t_5) + (t_2 + t_3)(t_4 + t_5)]X^4\\
&+[t_0t_1 + t_2t_3 + t_4t_5]X^4\\
&-[t_0t_1(t_2 + t_3 + t_4 + t_5) + t_2t_3(t_4 + t_5) + t_4t_5(t_2 + t_3)]X^3\\
&+\left[(t_0 + t_1)\left(t_2t_3 + t_4t_5 + (t_2 + t_3)(t_4 + t_5)\right)\right]X^3\\
&+\left[t_2t_3t_4t_5 + (t_0 + t_1)\left(t_2t_3(t_4 + t_5)\right)\right]X^2\\
&+\left[\left(t_4t_5(t_2 + t_3)\right) + t_0t_1\left((t_2 + t_3)(t_4 + t_5) + t_2t_3 + t_4t_5\right)\right]X^2\\
&-\left[(t_0 + t_1)t_2t_3t_4t_5 + t_0t_1\left(t_2t_3(t_4 + t_5) + t_4t_5(t_2 + t_3)\right)\right]X\\
&+t_0t_1t_2t_3t_4t_5.\end{aligned}$$

If we expand the coefficients of $U$ in terms of the roots $a, b$ and $c$ we find that they are symmetric polynomials in the roots. For example the terms for $X^5$ and $X^4$ are

$12(a + b + c)X^5$
$[58(a^2 + b^2 + c^2) + 122(ab + ac + bc)]X^4$

Using the information on symmetric polynomials [2] our polynomial becomes

$$\begin{aligned} U(X) &= X^6 + t_0t_1t_2t_3t_4t_5 \\ &= X^6 + 108 \end{aligned}$$

which is irreducible in $\mathbb{Q}$.

In general the polynomial $F$ will not always be irreducible but will decompose into irreducible factors so that $F(X) = G_1(X)G_2(X)G_3(X) \dots G_s(X)$. Note that since the roots of $F$ are the conjugates of the resolvent then each of the factors must have some of the conjugates as its roots, and each factor has roots distinct from the roots of each other factor. We choose $G_1$ to be the factor that has $V_0 = t_0$ as a root.

Before we precede further to find the Galois group of $u(x)$, we quote the following theorem:

**Theorem [2] :** Let an equation be given whose m roots are $a, b, c, \dots$ There will always be a group of permutations of the letters $a, b, c, \dots$ which will have the following property:

1. That each function invariant under the substitutions of this group will be known rationally,
2. Conversely, that every function of the roots which can be determined rationally will be invariant under these substitutions.

We have $F(X) = G_1(X)G_2(X)G_3(X) \dots G_s(X)$. Let deg $G_1$ be m so the roots of $G_1$ are $m$ of the $t_i$ including $t_0$. The given equation $f$ has n roots that can all be represented as functions of the $t_i$. We can construct a table as below:

$$\begin{array}{llll} h_1(t_0), & h_2(t_0), & h_3(t_0), \dots, h_n(t_0) \\ h_1(t_i), & h_2(t_i), & h_3(t_i), \dots, h_n(t_i) \\ \vdots & \vdots & \vdots \\ h_1(t_j), & h_2(t_j), & h_3(t_j), \dots, h_n(t_j) \end{array}$$

This table has $m$ rows representing the $m$ conjugates of the resolvent and $n$ columns representing the roots of the given equation $f$. This table gives us the Galois group since each row represents one arrangement of the roots. We can demonstrate this by using our example $u(x\ ) = x^3 - 2$ once again. The table of functions of the $t_i$ is

$$\begin{array}{lll} h_1(t_0), & h_2(t_0), & h_3(t_0) \\ h_1(t_1), & h_2(t_1), & h_3(t_1) \\ h_1(t_2), & h_2(t_2), & h_3(t_2) \\ h_1(t_3), & h_2(t_3), & h_3(t_3) \end{array}$$

$h_1(t_4)$, $h_2(t_4)$, $h_3(t_4)$
$h_1(t_5)$, $h_2(t_5)$, $h_3(t_5)$

which gives

$a \quad b \quad c$
$c \quad a \quad b$
$b \quad c \quad a$
$b \quad a \quad c$
$c \quad b \quad a$
$a \quad c \quad b$

These permutations are those contained in the whole of the symmetric group $S_3$. So the Galois group is of $u$ is $S_3$.

## REFERENCE

1. Cangelmi. L., Resolvents and Galois groups, Rend. Sem. Mat. Univ. Pol. Torino 53, 3(1995) pp. 207-222.
2. Edwards H. M. Galois Theory Springer-Verlag, New York, 1984.
3. Galois E., M_emoire sur les conditions de r_esolubilit_e des equations par rad- icaux, English transl. in [2, Appendix 1].
4. Garling D. J. H., A course in Galois theory, Cambridge University Press (1993)
5. Geissler K, Kl uners J., Galois group computation for rational polynomials J. Symbolic Computation, 30(2000) pp. 653-674
6. Girstmair K., On the computation of resolvents and Galois groups, Manuscripta Math. 43 (1983), pp. 289-307.
7. Hulpke A., Galois groups through invariant relations. In Groups 97 Bath/St. Andrews (C.M. Campbell, E.F. Robertson, G.C. Smith, eds.). Cambridge University Press, to appear.
8. Lefton P., Galois resolvents of permutation groups, Amer. Math. Monthly 84 (1977), pp.642-644.
9. Landau, S., Miller, G.: Solvability by radical is in polynomial time. J. Comput. System Sci. 30 (1985) pp. 179 208.
10. Pierpont J., Galois theory of algebraic equations. Part I. Rational resol- vents, Ann. of Math. (2) 1 (1899-1900), pp. 113-143.

11. Pierpont J., Galois theory of algebraic equations. Part II Irrational resolvents, Ann. of Math. (2) 2 (1900-1901), pp. 22-55.

12. Serre J. P., Topics in Galois theory, notes written by H. Darmon, Jones and Bartlett Publishers, Boston (1992).

13. Soicher L., McKay J., Computing Galois groups over the rationals, Journal of Number Theory, 20(1985) pp. 273-281.

14. Stauduhar R.P., The determination of Galois groups, Math. Comp. 27 (1973), pp. 981-996.