The Hacque method and the complete GI-method for computing the Galois group*

Ines Abdeljaouad and Annick Valibouze†

CalFor - LIP6, Université Paris VI,
4 Place Jussieu, F-75252 PARIS CEDEX 05
E-mail: abdeljao@medicis.polytechnique.fr; avb@medicis.polytechnique.fr

1. INTRODUCTION

Two philosophies are proposed for computing the *Galois group* of a univariate polynomial: the algebraic one and the numerical one. The numerical methods provide efficient algorithms even with a high degree of precision (see [19], [7], [13]); the algebraic methods guarantee an exact result in reasonable time (see [21], [6]) and the work undertaken in [3] and [4] is deterministic.

We propose two algebraic methods for computing the Galois group of an irreducible polynomial f which we call the *Hacque method* (in [12]) and the *complete GI-method*. We start by introducing the Hacque method: we give in section 2 a system of characteristic equations of the Galois group as a subgroup of the linear algebraic group. The complete GI-method is introduced in section 3. It computes the Galois group thanks to an algorithm of computation of the decomposition group of the *ideal of relations* (see [20]).

Throughout this article k indicates a field of characteristic zero and f an univariate polynomial irreducible over k. The Hacque method for computing the Galois group of f cannot be used without preliminary computation: in fact, a minimal polynomial of a primitive element of the Galois extension must be computed. Thus, section 4 is devoted to transform the Hacque method into an implementable form. For this, we combine the Hacque method with the first steps of the complete GI-method and we finally compare this two methods.

* Rapport de recherche du LIP6, présentation orale à AAECC'13 en Novembre 1999
† Supported by the *projet Galois* of the *UMS MEDICIS*, Palaiseau, France.

2. GALOIS GROUP AS A SUBGROUP OF $GL_N(K)$

Let K be a finite extension field over k of degree $n > 1$. Let us fix $e = (e_0, e_1, \ldots, e_m)$, a basis of the k-vector space K, such that $e_0 = 1$ and $m = n - 1$.

2.1. Notations and Definitions

The ring of k-endomorphisms over K is denoted by $\mathcal{L}_k(K)$ and the group of the invertible elements of $\mathcal{L}_k(K)$ by $GL_k(K)$. The *Galois group* of the extension $k \mid K$ is, by definition, the group of k-automorphisms over K. It is denoted by $Gal_k(K)$.

We set $\mathcal{M}_n(k)$ to be the ring of $n \times n$ matrices with coefficients in k. We denote by $M[., e]$ the isomorphism of algebra which associates with any k-endomorphism of $\mathcal{L}_k(K)$ its matrix in the basis e:

$$\begin{array}{cccccc} M[.,e] & : & \mathcal{L}_k(K) & \longrightarrow & \mathcal{M}_n(k) & \\ & & f & \mapsto & M[f,e] & . \end{array}$$

We denoted by $GL_n(k)$ the group of the invertible matrices of $\mathcal{M}_n(k)$. Then

$$GL_n(k) \simeq GL_k(K) \qquad . \tag{1}$$

For all $\lambda \in K$, we denote by $\widehat{\lambda}$ the multiplicative endomorphism of λ over K defined by $\widehat{\lambda}(x) = x\lambda$, for all x in K. Remark that the field $\widehat{K} = \{\widehat{\lambda} \in \mathcal{L}_k(K) \mid \lambda \in K\}$ is isomorphic to K.

Let $\mathcal{K} = \{M[\widehat{\lambda}, e] \in \mathcal{M}_n(k) \mid \lambda \in K\}$. The field $\mathcal{K}$ is naturally isomorphic to the field $\widehat{K}$. Thus, we obtain the following isomorphisms:

$$K \simeq \widehat{K} \simeq \mathcal{K} \qquad . \tag{2}$$

The group of the invertible elements of K (resp. of $\widehat{K}$) is labeled by K^* (resp. $\widehat{K}^*$). The group $\widehat{K}^*$ is isomorphic to K^* and, it is a subset of $GL_k(K)$:

$$\widehat{K}^* = \{\widehat{\lambda} \in GL_k(K) \mid \lambda \in K^*\} \ . \tag{3}$$

We set $\mathcal{K}^* = \{M[\widehat{\lambda}, e] \in \mathcal{M}_n(k) \mid \lambda \in K^*\}$. Then $\mathcal{K}^* \subset GL_n(k)$ and we have the following isomorphisms:

$$K^* \simeq \widehat{K}^* \simeq \mathcal{K}^* \quad . \tag{4}$$

Let G and H be two groups such that $H \subset G$. The *normalizer of H in G*, denoted by $Nor[G; H]$, is equal to :

$$Nor[G; H] = \{a \in G \mid aHa^{-1} = H\} \quad .$$

DEFINITION 2.1. Let $g \in GL_k(K)$. The application g is called *K-semi-linear* if for all $x \in K$ and $\lambda \in K$, there exists an $s \in Gal_k(K)$ such that $g(x\lambda) = g(x)s(\lambda)$.

2.2. Properties of the Galois group $Gal_k(K)$ as a subgroup of $GL_n(k)$

PROPOSITION 2.1. *The Galois group $Gal_k(K)$ is the set of the K-semi-linear applications g of $GL_k(K)$ such that $g(1) = 1$.*

$$Gal_k(K) = \{g \in GL_k(K) \mid g \text{ is } K - semi{-}linear \text{ and } g(1) = 1\} \quad . \tag{5}$$

Proof. We note that for all $g \in Gal_k(K)$, g is K-semi-linear and $g(1) = 1$. Conversely, let g be a K-semi-linear application such that $g(1) = 1$, we have to show that $\forall x \in k$, $s(x) = x$. For any $x \in k$, there exists $s \in Gal_k(K)$ such that $g(x) = s(x).g(1) = s(x) = x$. So, $g \in Gal_k(K)$. ▮

The following proposition is a consequence of lemma 2.1 of [11], and we give here a direct proof:

PROPOSITION 2.2. *The normalizer of $\widehat{K}^*$ in $GL_k(K)$ is equal to a set containing all the K-semi-linear applications of $GL_k(K)$.*

$$Nor[GL_k(K); \widehat{K}^*] = \{g \in GL_k(K) \mid g \text{ is } K{-}semi{-}linear\} \quad . \tag{6}$$

Proof. Let $g \in Nor[GL_k(K); \widehat{K}^*]$ be a k-endomorphism, then for all $\lambda \in K^*$, $g \circ \widehat{\lambda} \circ g^{-1} \in \widehat{K}^*$. For all $\lambda \in K^*$, there exist $\mu \in K^*$ verifying $g \circ \widehat{\lambda} = \widehat{\mu} \circ g$; let s be an application from K^* to K^* such that $s(\lambda) = \mu$; s is a bijection of K^* because it is a surjection of K^*. To prove that g is K-semi-linear, we can only prove that g verifies $g(\lambda x) = g(x)s(\lambda)$ where $s \in Gal_k(K)$.

(i) For $\lambda \in K^*$, we have $g \circ \widehat{\lambda} = \widehat{s(\lambda)} \circ g$; then for any $x \in K$, $g \circ \widehat{\lambda}(x) = \widehat{s(\lambda)} \circ g(x)$ and thus $g \circ \widehat{\lambda}(x) = g(x\lambda) = g(x)s(\lambda)$.

(ii) Let us verify that the bijection s is a k-morphism of K. We set λ, $\mu \in K$ and $x \in K$ then, according to (i), $g(x(\lambda+\mu)) = g(x)s(\lambda+\mu)$. In addition, $g(x(\lambda+\mu)) = g(x\lambda)+g(x\mu) = g(x)s(\lambda)+g(x)s(\mu) = g(x)(s(\lambda)+s(\mu))$. Thus, like $g \neq 0$, $s(\lambda+\mu) = s(\lambda) + s(\mu)$.
In the same way, $g(x(\lambda\mu)) = g(x)s(\lambda\mu)$ and $g(x(\lambda\mu)) = g(x\lambda)s(\mu) = g(x)s(\lambda)s(\mu)$. Since $g \neq 0$, we obtain $s(\lambda\mu) = s(\lambda)s(\mu)$. Lastly, $g(1) = g(1)s(1)$ and thus $s(1) = 1$.

So, $s \in Gal_k(K)$ and the application g is K-semi-linear.

Conversely, let g be a K-semi-linear application. Let prove that for all $\lambda \in K^*$, $g \circ \widehat{\lambda} \circ g^{-1} \in \widehat{K}^*$.
By definition, for $\lambda \in K$ and $x \in K$,there exists $s \in Gal_k(K)$ such that $g(\lambda x) = g(x)s(\lambda)$. Particularly, for each $\lambda \in K^*$ and $x \in K$, $g \circ \widehat{\lambda} \circ g^{-1}(x) = g \circ \widehat{\lambda}(g^{-1}(x)) = g(g^{-1}(x)\lambda) = g(g^{-1}(x))s(\lambda) = xs(\lambda)$. So $g \circ \widehat{\lambda} \circ g^{-1} = \widehat{s(\lambda)}$. Since $\lambda \in K^*$ and $s \in Gal_k(K)$, the element $s(\lambda)$ is invertible (i.e. $s(\lambda) \in K^*$) and we deduce that the application $g \circ \widehat{\lambda} \circ g^{-1} \in \widehat{K^*}$. ▮

THEOREM 2.1. *According to the propositions 2.1 and 2.2, we have :*

$$Gal_k(K) = \{g \in Nor[GL_k(K); \widehat{K}^*] \mid g(1) = 1\} \quad . \tag{7}$$

Thanks to the isomorphism (1), the Galois group as a subgroup of $GL_n(k)$ *is expressed in the following form:*

$$Gal_k(K) = \{A \in Nor[GL_n(k); \mathcal{K}^*] \mid A(e_0) = e_0\} \, . \tag{8}$$

2.3. Characterization of $Gal_k(K)$ with a system of equations

We seek a system of equations which characterizes the Galois group $GL_n(k)$. For that, in all this part, we fix A a matrix of $GL_n(k)$.

LEMMA 2.1. *If the matrix A of $GL_n(k)$ verifies $A(e_0) = e_0$ then we write it in the form:*

$$A = \begin{pmatrix} 1 & \alpha_{1,0} & \dots & \alpha_{m,0} \\ 0 & \alpha_{1,1} & \dots & \alpha_{m,1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_{1,m} & \dots & \alpha_{m,m} \end{pmatrix} \tag{9}$$

where $\alpha_{i,j} \in k$ *for* $(i,j) \in [1,m] \times [0,m]$ *and* $\det(\alpha_{i,j})_{i,j\in[1,m]} \neq 0$.

Proof. Obvious. ▌

2.3.1. Characterization of the field $\mathcal{K}^*$

For $j \in [0,m]$, let set $M_j = M[\widehat{e_j}, e]$ the matrix of $\widehat{e_j}$ in the basis e ($\widehat{e_j}$ is the multiplicative endomorphism of e_j). Let $\lambda \in K$ and $\lambda^0, \dots, \lambda^m \in k$ such that $\lambda = \sum_{j=0}^{m} \lambda^j e_j$.
The writing

$$M[\widehat{\lambda}, e] = \sum\nolimits_{j=0}^{m} \lambda^j M_j \tag{10}$$

gives a characterization of the elements of the field $\mathcal{K}$. Furthermore, λ belongs to the field K^* if and only if λ^j ($j \in [0,m]$) are not all zero.

Thus, $(M_0, M_1, \dots, M_m)$ is a basis of $\mathcal{K}^*$.

2.3.2. Characterization of $Nor[GL_n(k); \mathcal{K}^*]$

The matrix A belongs to $Nor[GL_n(k); \mathcal{K}^*]$ if it verifies $A\mathcal{K}^*A^{-1} = \mathcal{K}^*$. This is equivalent to:

$$\forall i \in [1,m]\ ,\ \exists\ (\mu_{i,0}, \dots, \mu_{i,m}) \in k^n - \{(0,\dots,0)\}\ \ AM_i = \sum\nolimits_{j=0}^{m} \mu_{i,j} M_j A\ . \tag{11}$$

Corollary 2.1. *Let* $A \in GL_n(k)$ *and* (12) *the linear system of equations deduced from* (11)*:*

$$AM_i = \sum\nolimits_{j=0}^{m} x_{i,j}\ M_j A\ ,\ i \in [1,m]\ \ , \tag{12}$$

where $x_{i,j}$ *are unknown. The matrix* A *belongs to* $Nor[GL_n(k); \mathcal{K}^*]$ *if and only if the system of equations* (12) *admits at least one solution* $\mu = (\mu_{i,j})_{i\in[1,m],j\in[0,m]}$ *in* $k^{m\times n}$.

2.3.3. Characterization of the Galois group

Theorem 2.2. *The matrix* A *of* $GL_n(k)$ *belongs to the Galois group* $Gal_k(K)$ *if and only if*

(a)it is written in the form (9),
(b)the system (12) *admits at least one solution.*

Proof. According to the theorem 2.1, the lemma 2.1 and the section 2.3. ▮

DEFINITION 2.2. Let $B = (b_{i,j})_{i,j\in[1,n]}$ be a matrix of $\mathcal{M}_n(k)$ where $b_{i,j}$ are unknown. Let us put $X = (x_{i,j})_{i\in[1,m],j\in[0,m]}$ where $x_{i,j}$ are also unknown entries. The following system of equations:

$$B(e_0) = e_0 \qquad \text{and} \qquad BM_i = \sum\nolimits_{j=0}^{m} x_{i,j}\ M_jB\ ,\ i \in [1,m] \qquad (13)$$

is called the *system of equations of the Galois group $Gal_k(K)$ in the basis e.*

COROLLARY 2.2. *A matrix A belongs to the Galois group $Gal_k(K)$ if and only if the system* (13) *of equation of Galois group in the basis e admits a solution $B = A$ and $X = \mu$ for a certain $\mu \in k^{m\times n}$.*

2.4. Simplification of the system of equations of $Gal_k(K)$ - Hacque system

Let $u \in K$ be a primitive element of the extension $k \mid K$ (i.e. $k(u) = K$) and let $u^n - (a_m u^m + \ldots + a_1 u + a_0)$ be its minimal polynomial over k. For $j \in [0,m]$, we can put $e_j = u^j$. We denote by M_0 the matrix identity. In the basis $(1, u, \ldots, u^m)$, the matrix M_1 of the endomorphism $\widehat{u}$ is written by:

$$M_1 = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_m \end{pmatrix}$$

And for $j \in [0,m]$, we set $M_j = {M_1}^j$.

LEMMA 2.2. *The system* (13) *of equations of Galois group in the basis $(1, u, \ldots, u^m)$ is equivalent to:*

$$B(e_0) = e_0 \qquad \text{and} \qquad BM_1 = \sum\nolimits_{j=0}^{m} x_j\ M_jB\ , \qquad (14)$$

where $x_j \in k$ *for all* $j \in [0, m]$.

Proof. It is obvious that the system (13) involves the system (14). Reciprocally, let $i \in [2, m]$ and suppose that (14) is verified. Then

$$BM_iB^{-1} = (BM_1B^{-1})^i = (\sum_{j=0}^m x_jM_j)^i = \sum_{j=0}^m y_jM_j \ ,$$

where y_j belongs to $k[x_0, \dots, x_m]$ because $(M_0, M_1, \dots, M_m)$ is a basis of $\mathcal{K}^*$. ▮

LEMMA 2.3. *If a matrix* $A \in GL_n(k)$ *and* $\mu = (\mu_0, \dots, \mu_m)$ *verifies the system* (14), *(i.e.* $B = A$ *and* $(x_0, \dots, x_m) = \mu$ *are solutions), then* A *is written in the form* (9) *and* $\mu_j = \alpha_{1,j}$ *for* $j \in [0, m]$.

Proof. To be convinced, it is enough to express AM_1 and M_1^jA for $j \in [0, m]$, in the basis $(1, u, \dots, u^m)$. ▮

THEOREM 2.3 (Hacque). *A matrix* A *belongs to the Galois group* $Gal_k(K)$ *if and only if the matrix* A *is invertible and*

$$A = \begin{pmatrix} 1 & \alpha_{1,0} & \dots & \alpha_{m,0} \\ 0 & \alpha_{1,1} & \dots & \alpha_{m,1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \alpha_{1,m} & \dots & \alpha_{m,m} \end{pmatrix} \qquad \text{such that} \qquad AM_1 = \sum_{j=0}^m \alpha_{1,j}\ M_jA$$

where $\alpha_{i,j} \in k$ *for* $(i, j) \in [1, m] \times [0, m]$.

DEFINITION 2.3. The system of the theorem 2.3 is called *Hacque system.*

2.5. Example of Hacque system

Let $F = T^6 + 108$ and $A \in GL_6(\mathbf{Q})$ such that $A(e_0) = e_0$, where $(e_0, \dots, e_n)$ is the canonical basis of $GL_6(\mathbf{Q})$. The Hacque system for the Galois extension over $\mathbf{Q}$ of the polynomial $F(T) = T^6 + 108$ is equal to:

$$AM_1 = \alpha_{1,0}M_0A + \alpha_{1,1}M_1A + \alpha_{2,1}M_2A + \alpha_{3,1}M_3A + \alpha_{4,1}M_4A + \alpha_{5,1}M_5A \ ,$$

where:

$$M_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -108 \end{bmatrix} \qquad \text{and} \qquad M_i = M_1^i \text{ for } i \in [0,5] \ .$$

Thus the Hacque system is equivalent to the following system of 30 equations and 30 unknowns:

$$\begin{gathered}
\alpha_{3,0} - \alpha_{1,0}\alpha_{2,0} = 0, \qquad \alpha_{4,0} - \alpha_{1,0}\alpha_{3,0} = 0, \qquad \alpha_{5,0} - \alpha_{1,0}\alpha_{4,0} = 0 \\
-108\alpha_{5,0} - \alpha_{1,0}\alpha_{5,0} = 0, \qquad \alpha_{2,1} - 2\alpha_{1,0}\alpha_{1,1} = 0, \qquad \alpha_{2,0} - \alpha_{1,0}^2 = 0 \\
\alpha_{3,1} - \alpha_{1,0}\alpha_{2,1} - \alpha_{1,1}\alpha_{2,0} = 0, \qquad \alpha_{4,1} - \alpha_{1,0}\alpha_{3,1} - \alpha_{1,1}\alpha_{3,0} = 0 \\
\alpha_{5,1} - \alpha_{1,0}\alpha_{4,1} - \alpha_{1,1}\alpha_{4,0} = 0, \qquad -108\alpha_{5,1} - \alpha_{1,0}\alpha_{5,1} - \alpha_{1,1}\alpha_{5,0} = 0 \\
\alpha_{2,2} - 2\alpha_{1,0}\alpha_{2,1} - \alpha_{1,1}^2 = 0, \qquad \alpha_{2,3} - \alpha_{1,0}\alpha_{2,2} - \alpha_{1,1}\alpha_{2,1} - \alpha_{2,1}\alpha_{2,0} = 0 \\
\alpha_{2,4} - \alpha_{1,0}\alpha_{2,3} - \alpha_{1,1}\alpha_{3,1} - \alpha_{2,1}\alpha_{3,0} = 0, \\
\alpha_{2,5} - \alpha_{1,0}\alpha_{2,4} - \alpha_{1,1}\alpha_{4,1} - \alpha_{2,1}\alpha_{4,0} = 0 \\
-108\alpha_{2,5} - \alpha_{1,0}\alpha_{2,5} - \alpha_{1,1}\alpha_{5,1} - \alpha_{2,1}\alpha_{5,0} = 0, \\
\alpha_{3,2} - 2\alpha_{1,0}\alpha_{3,1} - 2\alpha_{1,1}\alpha_{2,1} = 0 \\
\alpha_{3,3} - \alpha_{1,0}\alpha_{3,2} - \alpha_{1,1}\alpha_{2,2} - \alpha_{2,1}^2 - \alpha_{3,1}\alpha_{2,0} = 0, \\
\alpha_{3,4} - \alpha_{1,0}\alpha_{3,3} - \alpha_{1,1}\alpha_{2,3} - \alpha_{2,1}\alpha_{3,1} - \alpha_{3,1}\alpha_{3,0} = 0 \\
\alpha_{3,5} - \alpha_{1,0}\alpha_{3,4} - \alpha_{1,1}\alpha_{2,4} - \alpha_{2,1}\alpha_{4,1} - \alpha_{3,1}\alpha_{4,0} = 0, \\
\alpha_{4,2} - 2\alpha_{1,0}\alpha_{4,1} - 2\alpha_{1,1}\alpha_{3,1} - \alpha_{2,1}^2 = 0 \\
-108\alpha_{3,5} - \alpha_{1,0}\alpha_{3,5} - \alpha_{1,1}\alpha_{2,5} - \alpha_{2,1}\alpha_{5,1} - \alpha_{3,1}\alpha_{5,0} = 0, \\
\alpha_{4,3} - \alpha_{1,0}\alpha_{4,2} - \alpha_{1,1}\alpha_{3,2} - \alpha_{2,1}\alpha_{2,2} - \alpha_{2,1}\alpha_{3,1} - \alpha_{4,1}\alpha_{2,0} = 0 \\
\alpha_{4,4} - \alpha_{1,0}\alpha_{4,3} - \alpha_{1,1}\alpha_{3,3} - \alpha_{2,1}\alpha_{2,3} - \alpha_{3,1}^2 - \alpha_{4,1}\alpha_{3,0} = 0, \\
\alpha_{4,5} - \alpha_{1,0}\alpha_{4,4} - \alpha_{1,1}\alpha_{3,4} - \alpha_{2,1}\alpha_{2,4} - \alpha_{3,1}\alpha_{4,1} - \alpha_{4,1}\alpha_{4,0} = 0 \\
-108\alpha_{4,5} - \alpha_{1,0}\alpha_{4,5} - \alpha_{1,1}\alpha_{3,5} - \alpha_{2,1}\alpha_{2,5} - \alpha_{3,1}\alpha_{5,1} - \alpha_{4,1}\alpha_{5,0} = 0 \ .
\end{gathered}$$

$\alpha_{5,2}-\alpha_{1,0}\alpha_{5,1}-\alpha_{1,1}(\alpha_{4,1}-108\alpha_{5,1})-\alpha_{2,1}(\alpha_{3,1}-108\alpha_{4,1}+11664\alpha_{5,1})-\alpha_{3,1}(\alpha_{2,1}-108\alpha_{3,1}+11664\alpha_{4,1}-1259712\alpha_{5,1})-\alpha_{4,1}(\alpha_{1,1}-108\alpha_{2,1}+11664\alpha_{3,1}-1259712\alpha_{4,1}+136048896\alpha_{5,1})-\alpha_{5,1}(\alpha_{1,0}-108\alpha_{1,1}+11664\alpha_{2,1}-1259712\alpha_{3,1}+136048896\alpha_{4,1}-14693280768\alpha_{5,1}) = 0$

$\alpha_{5,3}-\alpha_{1,0}\alpha_{5,2}-\alpha_{1,1}(\alpha_{4,2}-108\alpha_{5,2})-\alpha_{2,1}(\alpha_{3,2}-108\alpha_{4,2}+11664\alpha_{5,2})-\alpha_{3,1}(\alpha_{2,2}-108\alpha_{3,2}+11664\alpha_{4,2}-1259712\alpha_{5,2})-\alpha_{4,1}(\alpha_{2,1}-108\alpha_{2,2}+11664\alpha_{3,2}-1259712\alpha_{4,2}+136048896\alpha_{5,2})-\alpha_{5,1}(\alpha_{2,0}-108\alpha_{2,1}+11664\alpha_{2,2}-1259712\alpha_{3,2}+136048896\alpha_{4,2}-14693280768\alpha_{5,2}) = 0$

$\alpha_{5,4}-\alpha_{1,0}\alpha_{5,3}-\alpha_{1,1}(\alpha_{4,3}-108\alpha_{5,3})-\alpha_{2,1}(\alpha_{3,3}-108\alpha_{4,3}+11664\alpha_{5,3})-\alpha_{3,1}(\alpha_{2,3}-108\alpha_{3,3}+11664\alpha_{4,3}-1259712\alpha_{5,3})-\alpha_{4,1}(\alpha_{3,1}-108\alpha_{2,3}+11664\alpha_{3,3}-1259712\alpha_{4,3}+$

$136048896\alpha_{5,3}) - \alpha_{5,1}(\alpha_{3,0} - 108\alpha_{3,1} + 11664\alpha_{2,3} - 1259712\alpha_{3,3} + 136048896\alpha_{4,3} - 14693280768\alpha_{5,3}) = 0$

$\alpha_{5,5} - \alpha_{1,0}\alpha_{5,4} - \alpha_{1,1}(\alpha_{4,4} - 108\alpha_{5,4}) - \alpha_{2,1}(\alpha_{3,4} - 108\alpha_{4,4} + 11664\alpha_{5,4}) - \alpha_{3,1}(\alpha_{2,4} - 108\alpha_{3,4} + 11664\alpha_{4,4} - 1259712\alpha_{5,4}) - \alpha_{4,1}(\alpha_{4,1} - 108\alpha_{2,4} + 11664\alpha_{3,4} - 1259712\alpha_{4,4} + 136048896\alpha_{5,4}) - \alpha_{5,1}(\alpha_{4,0} - 108\alpha_{4,1} + 11664\alpha_{2,4} - 1259712\alpha_{3,4} + 136048896\alpha_{4,4} - 14693280768\alpha_{5,4}) = 0$

$-108\alpha_{5,5} - \alpha_{1,0}\alpha_{5,5} - \alpha_{1,1}(\alpha_{4,5} - 108\alpha_{5,5}) - \alpha_{2,1}(\alpha_{3,5} - 108\alpha_{4,5} + 11664\alpha_{5,5}) - \alpha_{3,1}(\alpha_{2,5} - 108\alpha_{3,5} + 11664\alpha_{4,5} - 1259712\alpha_{5,5}) - \alpha_{4,1}(\alpha_{5,1} - 108\alpha_{2,5} + 11664\alpha_{3,5} - 1259712\alpha_{4,5} + 136048896\alpha_{5,5}) - \alpha_{5,1}(\alpha_{5,0} - 108\alpha_{5,1} + 11664\alpha_{2,5} - 1259712\alpha_{3,5} + 136048896\alpha_{4,5} - 14693280768\alpha_{5,5}) = 0$

The Galois group of $F(T) = T^6 + 108$ is the set of matrices A verifying the Hacque system. After the identification of this system with subgroups of $GL_6(\mathbf{Q})$, we deduce that the regular representation of the Galois group of F over $\mathbf{Q}$ is isomorphic to $\mathcal{S}_3$.
We will see, in section 4, that the identification process of Galois group using Hacque system is accelerated when we use the result of the first steps of GI-method.

3. THE COMPLETE GI-METHOD

Let f be a polynomial over k of degree n and Ω_f be a n-tuple of n roots of f in an algebraic closure $\hat{k}$ of k. We propose an algorithm which computes the decomposition group of a given ideal and we prove that, applied to the ideal of Ω_f-relations I_{Ω_f}, the algorithm computes the Galois group $Gal_k(K) = G_{\Omega_f}$.

3.1. Notations and definitions

We denoted by $\mathcal{S}_n$ the symmetric group of degree n and $\mathcal{I}_n$ the identity group of $\mathcal{S}_n$. For $\sigma \in \mathcal{S}_n$ and $\beta = (\beta_1, \dots, \beta_n)$ a n-tuple in $\hat{k}$, we put $\sigma.\beta = (\beta_{\sigma(1)}, \dots, \beta_{\sigma(n)})$. We denote by $k[x_1, \dots, x_n]$ the ring of polynomial in the variable $x_1, \dots, x_n$ over the field k and $k[T]$ the ring of polynomial in the variable T over the field k.

The action of the permutation group of degree n on $k[x_1, \dots, x_n]$ is defined by:

$$\begin{array}{ccc} \mathcal{S}_n \times k[x_1,\ldots,x_n] & \longrightarrow & k[x_1,\ldots,x_n] \\ (\sigma, P) & \mapsto & \sigma.P(x_1,\ldots,x_n) = P(x_{\sigma(1)},\ldots,x_{\sigma(n)}) \end{array} .$$

For $\sigma \in \mathcal{S}_n$, β a n-tuple in $\hat{k}$ and $P \in k[x_1,\ldots,x_n]$, we have: $\sigma.P(\beta) = P(\sigma \circ \beta)$. Let J be a subset of $k[x_1,\ldots,x_n]$ and $\sigma \in \mathcal{S}_n$ then $\sigma(J) = \{\sigma.P \mid P \in J\}$.

DEFINITION 3.1. Let L be a subgroup of $\mathcal{S}_n$ and H a subgroup of L. The polynomial $\Theta \in k[x_1,\ldots,x_n]$ is an *L-primitive H-invariant* if

$$H = \{\sigma \in L \mid \sigma.\Theta = \Theta\} .$$

DEFINITION 3.2. The *ideal of the Ω_f-relations*, denoted by I_{Ω_f}, is defined by:

$$I_{\Omega_f} = \{P \in k[x_1,\ldots,x_n] \mid P(\Omega_f) = 0\} .$$

DEFINITION 3.3. The *Galois group* of Ω_f is defined by:

$$G_{\Omega_f} = \{\sigma \in \mathcal{S}_n \mid \forall P \in I_{\Omega_f} \ , \ \sigma.P(\Omega_f) = 0\} .$$

3.2. Galois Ideal and decomposition group

Let $\alpha = (\alpha_1,\ldots,\alpha_n)$ be a n-tuple in $\hat{k}$. A polynomial $P \in k[x_1,\ldots,x_n]$ is an *α-relation* if $P(\alpha) = 0$.

DEFINITION 3.4. Let L be a subgroup of $\mathcal{S}_n$. The ideal I_α^L of L-invariant α-relations defined by:

$$I_\alpha^L = \{R \in k[x_1,\ldots,x_n] \mid (\forall \sigma \in L) \ \sigma.R(\alpha) = 0\} ,$$

is called an *(L, α)-Galois ideal*.

The ideal $I_\alpha^{\mathcal{S}_n}$ is called the *ideal of symmetric relations* and, according to definition 3.2, $I_\alpha^{\mathcal{I}_n} = I_\alpha$, the *ideal of α-relations*.

EXAMPLE 3.1. Let f be a polynomial over k of degree n and Ω_f be a n-tuple of ne roots of f in an algebraic closure of k. If $e_1,\ldots,e_n$ represents the n elementary symmetric functions, then the polynomials $e_1 - e_1(\Omega_f)$, $\dots$,$e_n - e_n(\Omega_f)$, called *Cauchy modulus of* f, form a Gröbner basis of $I_{\Omega_f}^{\mathcal{S}_n}$.

DEFINITION 3.5. The *decomposition group* $Gr(I)$ *of an ideal* $I \subset k[x_1, \dots, x_n]$ is defined by:

$$Gr(I) = \{\sigma \in \mathcal{S}_n \mid \sigma(I) = I\} \ .$$

Remark 3. 1. $Gr(I)$ is a group and it verifies the following equality:

$$Gr(I) = \{\sigma \in \mathcal{S}_n \mid \sigma(I) \subset I\} \ .$$

Remark 3. 2. According to the definition 3.3, the Galois group of Ω_f is the decomposition group of the ideal I_{Ω_f} of Ω_f-relations:

$$G_{\Omega_f} = \{\sigma \in \mathcal{S}_n \mid \sigma(I_{\Omega_f}) = I_{\Omega_f}\} = Gr(I_{\Omega_f}) \ .$$

Remark 3. 3. We have $I_{\Omega_f}^{G_{\Omega_f}} = I_{\Omega_f}$ and if H is a subgroup of G_{Ω_f} then $I_{\Omega_f}^{H} = I_{\Omega_f}$.

3.3. Computation of the Decomposition group of an ideal

THEOREM 3.1. *Let* $g_1, \dots, g_s$ *be generators of an ideal* I *in* $k[x_1, \dots, x_n]$. *The decomposition group* $Gr(I)$ *of* I *is the biggest subgroup* G *of* $\mathcal{S}_n$ *verifying:*

$$\forall\, i \in [1, s] \text{ and } \forall\, j \in [1, r] \quad \tau_j \,.\, g_i \in I \ , \tag{15}$$

where $\tau_1, \dots, \tau_r$ *are generators of* G.

Proof. Let $g_1, \dots, g_s$ be a generating system of the ideal I in $k[x_1, \dots, x_n]$. Let $\sigma \in Gr(I)$ then $\sigma(I) = I$, in particular for each generator g_i of I we have $\sigma(g_i) \in I$. Thus, $Gr(I)$ verifies the condition (15).
In addition let prove that $Gr(I)$ is the biggest subgroup verifying (15): Let

$\tau \in \mathcal{S}_n$ such that:

$$\forall i \in [1,s]\ \tau.g_i \in I \quad . \tag{16}$$

Let $g \in I$ then, $g_1, \ldots, g_s$ are generators of I so, there exist $t_1, \ldots, t_s$ in $k[x_1, \ldots, x_n]$ such that $g = t_1 g_1 + \ldots + t_s g_s$. Thus $\tau.g$ is also a linear combination of $\tau.g_1, \ldots \tau.g_s$ over $k[x_1, \ldots, x_n]$. Thus, using identity (16), we have $\tau.g \in I$ for all $g \in I$. Then $\tau \in Gr(I)$. ▮

We propose an algorithm called **IDG** which computes the decomposition group of an ideal I defined by a Gröbner basis of I. It also needs a list of groups which contains the Decomposition group of I. This list is called a *Candidate List* and it can contains the symmetric group $\mathcal{S}_n$.
The function **return(**G**)** gives us the decomposition group G of the ideal I and the function **Add(**G,g**)** adds the permutation g to the set G. Let $g_1, \ldots, g_s$ be a Gröbner basis of the ideal I and L a set of all the generators of the groups in the *Candidate List*.

ALGORITHM 1 (IDG($< g_1, \ldots, g_s >$, L)).

1. **begin**
2.   **for** $f \in I$ **do**
3. $G := \{\}$
4.   **for** $g \in L$ **do**
5.   **if** $g.f \in I$ **then** **Add(**G,g**)**; **end if**
6.   **end for**
7. $L := G$
8.   **end for**
9.   **return(**G**)**
10. **end**.

The group G is the decomposition group $Gr(I)$ of the ideal I.

Proof. In each step of the algorithm, the group L decreases. In fact, this group converges towards the decomposition group of the ideal I and according to theorem 3.1, the algorithm **IDG** switches off in a finished number of steps.
The step 5. of the algorithm is possible when we take a Gröbner basis of I. In fact, $g.f \in I$ if and only if the remainder of the reduction of $g.f$ under the ideal I is equal to zero.
Let g be an element of L that does not verify the step 5. The optimization

of the algorithm can be done by removing all the factors of the elements g in L.

∎

3.4. Determination of the generators of I_{Ω_f} for the computation of G_{Ω_f}

The algorithm **IDG** applied to the ideal of Ω_f-relations gives the Galois group of G_{Ω_f}. So, in order to compute the G_{Ω_f} using the complete GI-method, we initially have to compute a Gröbner basis of the ideal of Ω_f-relations.
A first method, due to N. Yokoyama (see [16]), consists on given a factor of the polynomial f in some successive extension of k until the field of decomposition of f. The disadvantage of this method, applied to our problem, is that its cost is very high.
The *GI-method* is closely related to the computation of G_{Ω_f} (see Algorithm 4.2 in [20]). It consists on computing the generators of Galois ideals using relative resolvents. It is the method exposed in this paragraph in order to compute the ideal of relations.

Definition 3.6. Let $\Theta \in k[x_1, \ldots, x_dn]$ and L a subgroup of $\mathcal{S}_n$ containing G_{Ω_f}. The *L-relative resolvent of Ω_f by Θ* is the univariate polynomial over k given by:

$$\mathcal{L}_{\Theta,\Omega_f,L} = \prod_{\psi \in L.\Theta} (T - \psi(\Omega_f)) \ .$$

When $L = \mathcal{S}_n$, this resolvent, denoted by $\mathcal{L}_{\Theta,f}$, is called the *absolute resolvent of f by Θ* .

Definition 3.7. Let H and L be two subgroups of $\mathcal{S}_n$ such that $H \subset L$ and let Θ be an L-primitive H-invariant. The invariant Θ is *L-separable for Ω_f* if and only if $\Theta(\Omega_f)$ is a square-free root of the resolvent $\mathcal{L}_{\Theta,\Omega_f,L}$. When $L = \mathcal{S}_n$, Θ is called *separable for Ω_f*.

Let $E \subset k[x_1, \ldots, x_n]$. The ideal generated by E in $k[x_1, \ldots, x_n]$ is denoted by $< E >$.

Theorem 3.2 (Valibouze). *Let H and L be two subgroups of $\mathcal{S}_n$ such that $H \subset L$ and $G_{\Omega_f} \subset L$. Let Θ be an L-primitive H-invariant L-separable for Ω_f and let F be a minimal polynomial of $\Theta(\Omega_f)$ over k. Then $I^H_{\Omega_f} = I^L_{\Omega_f} + < F(\Theta) >$.*

By assumption, the polynomial F is a square-free factor, irreducible over k, of the resolvent $\mathcal{L}_{\Theta,\Omega_f,L}$.

Proof. See theorem 3.27 in [20]. ▮

Now, first steps of the GI-method produces (like for the Hacque method) a group L containing the Galois group G_{Ω_f}, it also gives $I_{\Omega_f}^L$ and *Candidate List* a list of subgroups of L candidate to be the Galois group. We compute a polynomial F square-free factor, irreducible over k, of the L-resolvent $\mathcal{L}_{\Theta_H,\Omega_f,L}$, where H and Θ verify the conditions of theorem 3.2 and H can be an element of *Candidate List*. So, we reduce the *Candidate List* using theorem 3.2. If moreover H is a subgroup of G_{Ω_f} then, by remark 3.3, we have: $I_{\Omega_f} = I_{\Omega_f}^L + < F(\Theta_H) >$, it is in particular the case of $H = \mathcal{I}_n$. If the *Candidate List* contains one element then it is the Galois group, otherwise, we compute a Gröbner basis for the lexicographic order of I_{Ω_f} using a very fast algorithm developed by J. C. Faugère (see **FGB** in [8] or [9] for more details on Gröbner basis) and we apply the algorithm **IDG** to this Gröbner basis and to *Candidate List* in order to compute the Galois group G_{Ω_f} of f.

4. THE CONSTRUCTIVE HACQUE METHOD

Let f be a square-free univariate polynomial over k of degree d and let K be its decomposition field over k. The field K is of degree n as supposed in the preceding section.
We see in section 2.4 that the Hacque system, cannot be implementable without the minimal polynomial of a primitive element of the Galois extension of k.
The Galois resolvent allows us to compute a minimal polynomial of a primitive element of $k \mid K$, but as we will see in this section, its computation is practically impossible. Furthermore, to be effective, the Hacque method should not have impracticable preconditions. Thus, we search to take a particular factor of the Galois resolvent to determine a minimal polynomial of a primitive element of the Galois extension.

4.1. Minimal polynomial of a primitive element of $k \mid K$

In order to compute a primitive element of the extension field $k \mid K$ or, more exactly, its minimal polynomial on k, the historical method consists on the computation and the factorization of the *Galois resolvent* of the

polynomial f (see [21]). In fact, any square-free factor, irreducible over k, of this resolvent is the minimal polynomial of a primitive element of the extension $k \mid K$. This resolvent being of degree $d!$, it is quite obvious that its computation is doomed to failure over the degree $d = 6$.
The idea, presented here, is to compute only one factor in k of the Galois resolvent in order to reduce the complexity of the problem. For this, we will use *relative resolvents* defined below.

DEFINITION 4.1. Let $V \in k[x_1, \ldots, x_d]$. A resolvent $\mathcal{L}_{V,f}$ is called *Galois resolvent* if

- it has only square-free roots,
- V is an $\mathcal{S}_d$-primitive $\mathcal{I}_d$-invariant.

PROPOSITION 4.1. *There always exist many polynomials V such that the resolvent $\mathcal{L}_{V,f}$ is a Galois resolvent. For such a V, each root of the Galois resolvent is a primitive element of the algebraic extension $k \mid K$.*

Proof. Since k is a perfect infinite field and f is square-free, see [10]. ▮

Remark 4. 1. With the assumptions of definition 3.6 and for Θ an L-primitive H-invariant ($H \subset L$), the L-relative resolvent $\mathcal{L}_{\Theta,\Omega_f,L}$ is of degree $[H : L]$ and it is a factor of the absolute resolvent $\mathcal{L}_{\Theta,f}$.

Let us consider a polynomial $V \in k[x_1, \ldots, x_d]$ such that $\mathcal{L}_{V,f}$ be a Galois resolvent and let F one of its square-free factor irreducible over k. Without loss of informations, we can suppose that $V(\Omega_f)$ is one of the roots of F and thus, F is his minimal polynomial over k.
If L is a subgroup of $\mathcal{S}_d$ containing the Galois group G_{Ω_f} then by remark 4.1 the degree of the resolvent $\mathcal{L}_{V,\Omega_f,L}$ is the order of L and $\mathcal{L}_{V,\Omega_f,L}$ is a factor over k of the Galois resolvent $\mathcal{L}_{V,f}$.
If the order of the group L is sufficiently small, it is possible to compute the resolvent $\mathcal{L}_{V,\Omega_f,L}$ (see [15], [18] and the GI-method in [20]). Thus, to find such group L it is necessary to apply first steps of the complete GI-method until the computation of the Galois ideal $I^L_{\Omega_f}$.

4.2. Comparing Hacque method and Complete GI-method

Recall that the *GI-method* is the algorithm of [20] which produces the ideal of Ω_f-relations and a list, called *Candidate List*, containing groups

candidate to be the Galois group (see section 3.4). If the *Candidate List* contains only one element, it is the Galois group G_{Ω_f}.
As the Hacque method requires the first steps of GI-method to compute some group L, it is natural to compare the Hacque method and the *complete GI-method* (see section 3). In fact, suppose that first steps of GI-method computes a Galois ideal $I^L_{\Omega_f}$ and a *Candidate List* which contains a group L verifying conditions of section 4.1.

Let set V an L-primitive $\mathcal{I}_n$-invariant. For the Hacque method, we first must compute and factorize the resolvent $\mathcal{L}_{V,\Omega_f,L}$. Next, we identify the Hacque system (see theorem 2.3) with some group of *Candidate List* to have the Galois group.
Besides, the *complete GI-method* (see section 3) computes the resolvent $\mathcal{L}_{V,\Omega_f,L}$. After that, we give a Gröbner basis of the ideal of Ω_f-relations: $I_{\Omega_f} = I^L_{\Omega_f} + < F(V) >$ where F, a minimal polynomial of $V(\Omega_f)$ over k, is a square-free factor, irreducible over k, of $\mathcal{L}_{V,\Omega_f,L}$. But, we prefer to compute and factorize the resolvent $\mathcal{L}_{\Theta_H,\Omega_f,L}$ where Θ_H is an L-primitive H-invariant and H a subgroup of L contained in G_{Ω_f} (the group H may be found using *Candidate List* see also theorem 3.2 and section 3.4). So, here, we compute relative resolvents of degree smaller than the degree of the resolvent $\mathcal{L}_{V,\Omega_f,L}$ computed in the Hacque method.
Furthermore, after the computation of the ideal of Ω_f-relations, we must compute a Gröbner basis of it in order to apply the algorithm **IDG**.

5. EXAMPLE OF COMPUTATION OF THE GALOIS GROUP FOR $N = 6$

For $n = 6$, let $f = x^6 + 2$. The GI-method applied to f gives a list of groups candidate to be Galois group of f (this list contains some subgroups of $PGL(2,5)$), it also gives the ideal $I^{PGL(2,5)}_{\Omega_f}$ (see [20]):

$$\begin{aligned}
I^{PGL(2,5)}_{\Omega_f} \;=\; & < 24x_6 + x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + 6x_3^3x_2x_1^3 + 5x_3^3x_1^4 + \\
& 8x_3^2x_2^3x_1^2 + 4x_3^2x_2^2x_1^3 + 8x_3^2x_2x_1^4 + 6x_3x_2^3x_1^3 + \\
& 8x_3x_2^2x_1^4 - 4x_3x_2x_1^5 + 12x_3 + 5x_2^3x_1^4 + 12x_2 + 14x_1, \\
& 24x_5 - 5x_3^3x_2^4 - 7x_3^3x_2^3x_1 - 16x_3^3x_2^2x_1^2 - 7x_3^3x_2x_1^3 \\
& -5x_3^3x_1^4 - 8x_3^2x_2^4x_1 - 12x_3^2x_2^3x_1^2 - 12x_3^2x_2^2x_1^3 \\
& -8x_3^2x_2x_1^4 - 12x_3x_2^4x_1^2 - 16x_3x_2^3x_1^3 - 12x_3x_2^2x_1^4 \\
& +8x_3 - 5x_2^4x_1^3 - 5x_2^3x_1^4 - 2x_2 - 2x_1, \\
& 24x_4 + 5x_3^3x_2^4 + 6x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + x_3^3x_2x_1^3
\end{aligned}$$

$$+8x_3^2x_2^4x_1 + 4x_3^2x_2^3x_1^2 + 8x_3^2x_2^2x_1^3 +$$
$$12x_3x_2^4x_1^2 + 10x_3x_2^3x_1^3 + 4x_3x_2^2x_1^4 + 4x_3x_2x_1^5 +$$
$$4x_3 + 5x_2^4x_1^3 + 14x_2 + 12x_1,$$
$$x_3^4 + x_3^3x_2 + x_3^3x_1 + x_3^2x_2^2 + x_3^2x_2x_1 + x_3^2x_1^2 +$$
$$x_3x_2^3 + x_3x_2^2x_1 + x_3x_2x_1^2 + x_3x_1^3 + x_2^4 + x_2^3x_1 +$$
$$x_2^2x_1^2 + x_2x_1^3 + x_1^4,$$
$$x_2^5 + x_2^4x_1 + x_2^3x_1^2 + x_2^2x_1^3 + x_2x_1^4 + x_1^5,$$
$$x_1^6 + 2 > \quad .$$

the Hacque method

Let $V = x_3 + 2\,x_2 + 3\,x_1$ be a $PGL(2,5)$-primitive $\mathcal{I}_6$-invariant computed with the algorithm **PrimitiveInvariant** in [1] (see [2] and [14] for the computation of primitive invariants). The relative resolvent of f by V is computed with the generalization of algorithm in [17] (see [5]):

$$\begin{aligned}\mathcal{L}_{V,\Omega_f,PGL(2,5)} &= (T^{12} + 15444\,T^6 + 343064484)(T^{12} - 21164\,T^6 + 188183524)\\ &\quad (T^{12} - 572\,T^6 + 470596)(T^6 - 3456)^2(T^6 + 128)^2\\ &\quad (T^6 + 2)^2(T^{12} + 1012T^6 + 19307236)^2(T^6 - 54)^4 \quad .\end{aligned}$$

The resolvent $\mathcal{L}_{V,\Omega_f,PGL(2,5)}$ of degree 120 is a factor of the Galois resolvent $\mathcal{L}_{V,f}$ of degree $6! = 720$. The computation time and the factorization of the resolvent $\mathcal{L}_{V,\Omega_f,PGL(2,5)}$ is immediate (less than two seconds). Let $F = T^{12} - 572\,T^6 + 470596$ be a square-free factor, irreducible over $\mathbf{Q}$, of $\mathcal{L}_{V,\Omega_f,PGL(2,5)}$. So, the Galois group is a transitive group of order 12 and $G_{\Omega_f} \subset PGL(2,5)$.
The Hacque system of F is a system of $12^2 = 144$ equations and as much unknowns. By identification in the list of candidate containing all subgroups of $PGL(2,5)$, the Galois group of F and for f is isomorphic to D_6 the dihedral group of $\mathcal{S}_6$.

the Complete GI-method

It is sufficient to compute a discriminant resolvent of degree 20 instead of the resolvent of degree 120 for Hacque. In fact, we compute the $PGL(2,5)$-resolvent associated to Θ_{C_6} a $PGL(2,5)$-relative C_6-invariant, where C_6 is a cyclic group of order 6 in $\mathcal{S}_6$. We also compute a Gröbner basis of $I_{\Omega_f} = I_{\Omega_f}^{PGL(2,5)} + < F(\Theta_{C_6}) >$, where F is a square-free factor, irreducible over $\mathbf{Q}$, of the $PGL(2,5)$-resolvent associated to Θ_{C_6}.

6. CONCLUSION

The Hacque method is a new approach of the Galois theory and it characterizes it with a system of equations. To be efficient, this method can be used in the final step of the complete GI-method.
The complete GI-method mirrors the descent method of Stauduhar and we can say that the difference is that the test for rationality of an evaluated invariant is replaced by a test for invariance of an ideal. It is necessary to compute a Gröbner basis of the ideal of relations to obtain the Galois group. In this case, if the degree of the Galois group is reasonable, it would be preferable to use Hacque method (the Hacque system will not be so large). Otherwise, like the example of section 5, it is sometimes more efficient to compute a discriminating resolvent that will reduce the list *Candidate List* to one element : the Galois group.
The complete GI-Method is also used to compute the ideal of relations which allows us to make algebraic computations on the splitting field of the polynomial. So, if we want to compute on the splitting field, the complete GI-method is the best method.

REFERENCES

1. I. Abdeljaouad. Package PrimitiveInvariant sous GAP. *pub/gap/gap-3.4.4/deposit/gap/priminv.g*, 1997.
2. I. Abdeljaouad. Calculs d'Invariants Primitifs de groupes finis. *RAIRO - Informatique Thorique et Programmation, EDP-Science*, 33(1), 1999.
3. J.M. Arnaudiès and A. Valibouze. Lagrange resolvents. *Rapport Interne LITP, 93-61*, December 1993.
4. J.M. Arnaudiès and A. Valibouze. Computation of the Galois group of the Resolvent Factors for the Direct and Inverse Galois problem. *AAECC'95 Conference. LNCS 948, Paris*, pages 456–468, July 1995.
5. P. Aubry and A. Valibouze. Computing characteristic polynomials associated to some quotient ring. *MEGA'98*, 1998.
6. E.H. Berwick. On soluble sextic equations. *Proc. London Math. Soc.*, 2(29), 1929.
7. Y. Eichenlaub and M. Olivier. Computation of Galois groups for polynomial with degree up to eleven. *Mathematics Subject Classification. 11Y40*, 1991.
8. J.C. Faugère. New generations of Gröbner bases algorithms. *Colloque MEGA'98, to appear in Workshop Solving Systems of Equations, MSRI, Berkeley*, 1998.
9. R. Fröberg. *An Introduction to Gröbner bases.* Pure and Applied Mathematics, A Wiley-Interscience Series of Texts, Monographs, and Tracts, 1998.
10. E. Galois. *Oeuvres Mathmatiques.* publies sous les auspices de la SMF, Gauthier Villard, 1879.
11. M. Hacque. Thorie de Galois des anneaux presque-simples. *Journal of Algebra*, 108, 1987.

12. M. Hacque. Caractrisation des groupes de Galois comme sous-groupes de groupes algbriques linaires. Private communication, 1995.

13. Geissler K. and Klüners J. Galois group Computation for Rational polynomials. *Journal of Symbolic Computation*, 11:1–23, 2000.

14. G. Kemper. Calculating invariant rings of finite groups over arbitrary fields. *J. Symbolic Computation*, 1995.

15. F. Lehobey. Resolvent computation by resultants without extraneous powers. *Journal of Pure and Applied Algebra*, 1997.

16. M. Noro and K. Yokoyama. Factoring polynomials over algebraic extension fields. to appear, 1997.

17. N. Rennert and A. Valibouze. Calcul de rsolvantes avec les modules de Cauchy. *Experimental Mathematics*, 8(4):351–366, 1999.

18. L. Soicher and J. McKay. Computing Galois groups over the rationals. *Journal of number theory*, 20:273–281, 1985.

19. R.P. Stauduhar. The computation of Galois groups. *Math.Comp.*, 27, 1973.

20. A. Valibouze. Etude des relations algbriques entre les racines d'un polynme d'une variable. *Bulletin of the Belgian Mathematical Society Simon Stevin*, 6:507–535, 1999.

21. B.L. Van Der Waerden. *A Modern Algebra*, volume 1. Ungar, New York, 1953.