Computation of the Galois Groups of the Resolvent Factors for the Direct and Inverse Galois Problems

Annick Valibouze *

L.I.T.P., Université Paris VI,
4 place Jussieu, F-75252 Paris Cedex 05
email : avb@cosme.polytechnique.fr

Abstract. In this paper we present a new method for determining the Galois group of a square free univariate polynomial. This method makes use of a priori computation of the Galois group of the factors of its resolvents, and can also be used for the Galois inverse problem.

1 Introduction

Up to now, essentially three methods to compute the Galois group of a polynomial are known.

1. factorization of the polynomial in successive algebraic extensions (see [26])
2. use *relative resolvents* (see [25])
3. use the partitions of the *absolute resolvents* (or simply *resolvents*) (see [20])

The first one is deterministic, but not very efficient. The second one is also deterministic. It consist in testing the successive inclusions of the Galois group which is supposed to be transitive (i.e. the polynomial must be irreducible). Since it is not possible to use the fundamental Theorem of symmetric functions, this method requires numerical techniques in order to compute the non absolute resolvents. However, there exists a formal technique to compute these resolvents as part of this method 2 (see [14]).

The third method, very efficient, has always been thought to be non deterministic. It is based on the computation a priori of the partition resolvents (i.e. the degrees of the irreducible factors of the resolvents, that are supposed to be simple). Some authors have contributed to the developement of the effective Galois theory with this method ([9], [10], [15], [21], [22], [23], ...). In the paper [1], a formula is given that depends only on the group and that allows the automatic computation of the entire partition matrix of a reference group (which can be any finite group). This partition matrix can be used with non absolute resolvents when the reference group is not the symmetric group and hence accelerates

* Avec le soutien du GDR de Calcul Formel MEDICIS, du GDR-PRC Math-Info, du Centre de Calcul Formel de l'Ecole Polytechnique, et de CEC, ESPRIT BRA contrat 6846 POSSO

method 2. When the reference group is Σ_n, the symmetric group of degree n, the partition matrix gives a deterministic method to compute the Galois group of a polynomial of degree n and since it gives all possible algorithms for method 3 it gives obviously the best algorithm to identifiate the Galois group using only the partition resolvents. A further advantage of this partition matrix is that it is not restricted to irreducible polynomials (i.e. the Galois group are not necessarily transitive). Using the absolute resolvents and the partition matrix it is possible to compute the Galois group of square free polynomials of degree up to 7 (see [5] and [6]), of irreducible polynomials of degree 8,9 and 11, and for the degree 10 the second method must also be used (see [2] [3] and [7]). Note that it is possible to solve the problem for any square free polynomial of degree 8 not necessarily irreducible.

In the present paper a new deterministic method to compute the Galois group of a polynomial is given. It consist in the a priori computation of the matrix of the Galois group of the irreducible factors of all possible resolvents. Section 1 gives the theorems on which the method is based. When we simultaneously use the latter matrix and the partition matrix, we obtain for any separable resolvent the Galois groups and the degrees of its irreducible factors. Obviously this two matrices provide an algorithm which is more efficient than the one using only the partition resolvents. Sections 3 and 4 show this for the degrees 8 and 10. Section 2 gives some information useful to compute absolute resolvents. Section 6 shows how to compute this new matrix with a system like that of [17].

Our method is new, although the idea of considering the Galois groups of the irreducible factors of resolvents can already be found in Berwick (see [10]). This result can be applied to non absolute resolvents but for the sake of clarity we shall only consider absolute resolvents (i.e. the reference group is almost the symmetric group).

This new matrix is also useful for the *Galois inverse problem* since it is possible to know the Galois group of a factor of a resolvent of a polynomial when we know the Galois group of the polynomial. Section 5 gives an example that illustrates this fact.

2 Theoretical Results

Let k be a field of characteristic zero and f a square free univariate polynomial over k of degree n. We look for $\mathrm{Gal}(f)$, the Galois group of f over k.

Let Ψ be a polynomial in $k[x_1, \ldots, x_n]$, where $x_1, \ldots, x_n$ are n indeterminates. We denote by $\tilde{\Psi}$ the evaluation of Ψ at the n roots $\alpha_1, \ldots, \alpha_n$ of f and by Ω the set of these roots. The symmetric group of degree n, Σ_n, acts on $k[x_1, \ldots, x_n]$, in the natural way, and for $\tau \in \Sigma_n$, the image of Ψ under τ is denoted by $\tau\Psi$.

Let H be a subgroup of Σ_n. An *invariant of* H is a primitive element of the fixed field $k(x_1, \ldots, x_n)^H$ over $k(x_1, \ldots, x_n)^{\Sigma_n}$. A necessary and sufficient condition for $\Theta \in k[x_1, \ldots, x_n]$ to be an invariant of H is that $\tau\Theta = \Theta$ if and only if $\tau \in H$.

Let $id = \gamma_1, \ldots, \gamma_e$ be a left transversal of Σ_n mod H and Θ be an invariant of H. The *resolvent of* f *by* Θ, denoted by $\mathcal{L}_{\Theta,f}$, is the following univariate polynomial over k :

$$\mathcal{L}_{\Theta,f}(y) = \prod_{i=1}^{e}(y - \widetilde{\gamma_i \Theta}) \qquad .$$

The group H is called a *testing group* and $\mathcal{L}_{\Theta,f}$ is called an H*-resolvent*.

The results of this paper are based on the theorem of the *conservation of the primitive element* (see [1] Theorème 6.1) :

Theorem 1. *Let f be a square free polynomial of $k[x]$ of degree n. Let H be a subgroup of Σ_n and Θ an invariant of H. If $\tilde{\Theta}$ is a simple root of the resolvent $\mathcal{L}_{\Theta,f}$, then $\tilde{\Theta}$ is a primitive element of the fixed field $k(\Omega)^{Gal(f)\cap H}$ over $k = k(\Omega)^{Gal(f)\cap \Sigma_n}$.*

If $G = \mathrm{Gal}_k(f)$, then by Theorem 1 we have the following diagram:

$$k = k(\Omega)^G \overset{[\mathrm{G:G\cap H}]}{\longrightarrow} \quad k(\Omega)^{G\cap H} = k(\tilde{\Theta}) \overset{|\mathrm{G\cap H}|}{\longrightarrow} k(\Omega) \tag{1}$$

(the degrees of the extensions appear on top of the arrows). Let h be the simple irreducible factor of $\mathcal{L}_{\Theta,f}$ of which $\tilde{\Theta}$ is a root. Suppose that the degree of h is r. The elements of the transversal $id = \gamma_1, \ldots, \gamma_e$ are numbered in such a way that $id = \gamma_1, \ldots, \gamma_r$ is a left transversal of G mod $G \cap H$. The conjugates of $\tilde{\Theta}$ over k are $\widetilde{\gamma_1 \Theta}, \ldots, \widetilde{\gamma_r \Theta}$ which are also the r roots of h.

Remark. Since for $i = 1, \ldots, e$ the invariant $\Theta_i = \gamma_i \Theta$ of $H_i = \gamma_i H \gamma_i^{-1}$ satisfies $\mathcal{L}_{\Theta_i} = \mathcal{L}_{\Theta}$, theorem 1 and the diagram (1) are also true when we substitute the pair (H_i, Θ_i) for (H, Θ). The next theorem follows from this remark.

Theorem 2. *Under the hypotheses of Theorem 1 and with the previous notations, if $\widetilde{\Theta_{i_1}}, \ldots, \widetilde{\Theta_{i_q}}$ are simple roots of $\mathcal{L}_{\Theta,f}$, then the Galois group of $k(\Omega)$ over $k(\widetilde{\Theta_{i_1}}, \ldots, \widetilde{\Theta_{i_q}})$ is $Gal(f) \cap H_{i_1} \cap \cdots \cap H_{i_q}$.*

Proof. Let H and K be two subgroups of Σ_n, and let e and f be the primitive elements of $k(\Omega)^H$ and $k(\Omega)^K$ over k, respectively. Then :

$$k(e, f) = k(\Omega)^{H\cap K} \qquad .$$

Under the hypotheses of our theorem and together with Theorem 1 we have $k(\widetilde{\Theta_{i_1}}, \ldots, \widetilde{\Theta_{i_q}}) = k(\Omega)^{G\cap H_{i_1}\cap\cdots\cap H_{i_q}}$, where $\mathrm{Gal}(f) = G$.

The following theorem is a simple consequence of the one just proved.

Theorem 3. *Under the hypotheses of Theorem 1 and with the previous notations, let V be a normal subgroup of Σ_n given by $V = \bigcap_{i=1}^{e} H_i$. Then the Galois group of $\mathcal{L}_{\Theta,f}$ is isomorphic to $G/G \cap V$.*

Remark. From the above theorem the known results about the cubique resolvent easily follow and for $n \geq 5$ and $H \notin \{\Sigma_n, \mathcal{A}_n\}$, we have Theorem 4.6. of [1] : the Galois group of the resolvent $\mathcal{L}_{\Theta,f}$ is $\mathrm{Gal}(f)$.

Theorem 2 also gives the Galois group of all the factors of a resolvent. In the following theorem we only consider irreducible factors, since these are the ones that matter for the computation of our matrix :

Theorem 4. *If h is a simple irreducible factor of $\mathcal{L}_{\Theta,f}$ of degree r whose roots are $\widetilde{\Theta_1}, \ldots, \widetilde{\Theta_r}$, then its Galois group over k is isomorphic to $G/G \bigcap_{i=1}^{r} H_i$, where each $\Theta_i = \gamma_i \Theta$ is a resolvent of the group $H_i = \gamma_i H \gamma_i^{-1}$ and $Gal(f) = G$.*

Proof. The Galois group of the polynomial h over k is the one of the extension $k(\widetilde{\Theta}_1, \ldots, \widetilde{\Theta}_r)$ over k, which is therefore a Galois extension. Hence $K = G \bigcap_{i=1}^{r} H_i$ is normal in G and the Galois group of h is isomorphic to G/K.

[13] also considers all the different groups relative to a resolvent.

Corollary 5. *The order of the Galois group of h over k is $[G : G \bigcap_{i=1}^{r} H_i]$.*

Remark. Theorem 1 gives a method to compute the partition matrix, since the degree of h is equal to the index $[G : G \cap H_i]$, for each i in $\{1, \ldots, r\}$ (see [8]). By Theorem 4, the Galois group of h is known and can be computed a priori using only the subgroups G and H of Σ_n. Hence we can construct the matrix of the irreducible factors of the resolvents with a system as that of `GAP`.

2.1 Notations

Let H and G be two subgroups of Σ_n and g be a univariate polynomial with Galois group G. $[G, H]$ denotes the list of the Galois groups of the irreducible factors of any separable H-resolvent of g. If we have the degree of just one factor, we write down this degree. If just the degree d of a factor and the order D of its Galois group are known, this group is denoted by $(D)_d$. The exponents $+$ and $-$ refer to the subgroups of $\mathcal{A}_d$ (the alternating group) and to the ones not contained in $\mathcal{A}_d$, respectively. Here d is the degree of the irreducible factor under consideration. We denote by $[G, H]_d$ the sublist of $[G, H]$ relative to the factors of degree d. The group G is called the *candidate group* and H the *testing group*. For example, in Section 3.2 we have $[T_{35}, \mathcal{H}_2] = (\mathcal{D}_4, 8, 16^+)$. Let g be a polynomial of degree 8 and of Galois group T_{35}, and let L be a separable $\mathcal{H}_2$-resolvent of g. The polynomial L has a factor of degree 4 whose Galois group is $\mathcal{D}_4$, a factor of degree 8, and a factor of degree 16 whose Galois group is a subgroup of $\mathcal{A}_{16}$.

The group $T_i^{(j)}$ is the subgroup T_i of Σ_j which appears in the article [11]. The groups $\mathcal{A}_i, \mathcal{D}_i, \mathcal{C}_i$ are, respectively, the alternating, dihedral and cyclic group contained in Σ_i, and V_4 is the Vierer group of Σ_4.

2.2 General Assumptions

In this article, we suppose that all resolvents are separable. If this is not the case, it is possible to use a theorem of multiplicity (see Theorem 6.5 in [1]) and if this is still not sufficient it is also possible to compute a Tschirnhaus separable resolvent of f (i.e. an H-resolvent, where $H = \Sigma_1 \times \Sigma_{n-1}$) whose Galois group is also $\mathrm{Gal}(f)$ (see the above theorem).

3 Computations of the Resolvents

Except for the testing group T_{48} in degree 8, for all the testing groups H which appear in this paper, one or more $H-$resolvents can be computed via the module `SYM` (see [29]), an extension of `MAXIMA` (see [24]). The algorithms and the formulas are described in [27] and [4].

For m a positive integer, the Vandermonde determinant in the m indeterminates $x_1, \ldots, x_m$ is $\delta_m = \delta_m(x_1, \ldots, x_m) = \prod_{1 \leq i < j \leq m}(x_i - x_j)$

It is important to recall that if a resolvent $\mathcal{L}_{\Theta,f}$ is computed and factorised, it is immediate to compute partial factors of the resolvent $\mathcal{L}_{\delta_n \Theta, f}$. For example, let f be a polynomial of degree 8 of Galois group T_{45}; the partition of $\mathcal{L}_{b_8,f}$ is $(16, 32)$ (see Section 3). A factor of degree 32 of $\mathcal{L}_{\delta_8 b_8, f}$ is obtained by a simple resultant. This factor factorizes into two irreducible factors of degree 16. This new resolvents, introduced in [4], is of interest in practice for two reasons. First, it can be computed quickly, and second we can compute only the factors we need.

It is also important to remark that the product, or the monomial resolvents, can be computed quickly. Hence in the pratice, the resolvents are preferable to the sum or to linear resolvents. We can also compute these particular resolvents with the fast algorithms of [12].

4 Degree 8

In this section we show the interest of the Galois group of the resolvent factors for the identification of the Galois group of an irreducible polynomial of degree 8.

In May 1993, with Jean-Marie Arnaudiès we have computed a submatrix of the partition matrix for the reference group Σ_8 (except for the testing groups of degree > 672 and the candidate groups which are not transitive). In our article [2] we have only given the result for the group H whose H-resolvent can be computed with `SYM`.

All the computations are performed with [17], that can compute all the conjugacy classes of subgroups of Σ_8. For simplicity, we have adopted the notation of [11] for the group $T_1, \ldots, T_{50}$, the transitive subgroups of Σ_8 (up to conjugacy).

The testing groups are the following ones, and are given with the type of their invariants, except for the testing group T_{48} of index 30 an invariant of which can be computed with the algorithm of [16].

Let the subgroups A= [(1,2)(3,4,5,6), (1,4)(2,6,3,5),(7,8)(5,6)] and B= [(1,7,4,2,3),(1,2,4,7,3),(5,6,8),(4,7)(6,8)].

Classes	Index	Type	Invariants
$\mathcal{H}_1$	16	$\mathcal{A}_7 \times \Sigma_1$	δ_7 or $\delta_8 x_8$
$\mathcal{H}_2$	28	$\Sigma_2 \times \Sigma_6$	$s(x_1, x_2)$
$\mathcal{H}_3$	35	T_{47}	$b_8 = x_1x_2x_3x_4 + x_5x_6x_7x_8$
$\mathcal{H}_4$	56	A	$\delta_8\, s(x_1, x_2)$
$\mathcal{H}_5$	56	$\Sigma_6 \times Id_2$	$m(x_1, x_2),\ l(x_1, x_2),\ \delta_2$
$\mathcal{H}_6$	56	$\mathcal{A}_6 \times \Sigma_2$	$\delta_8\delta_2$ ou δ_6
$\mathcal{H}_7$	56	$\Sigma_3 \times \Sigma_5$	$s(x_1, x_2, x_3)$
$\mathcal{H}_8$	70	T_{45}	$\delta_8\, b_8$
$\mathcal{H}_{11}$	70	B	$\delta_8 s(x_5, x_6, x_8)$

In this table $s(x_1, \ldots, x_r)$ is a symmetric function in $x_1, \ldots, x_r$; $l(x_1, x_2) = ax_1 + bx_2$ where $b \neq a \neq -b$ and $m(x_1, x_2) = x_1^a x_2^b$ where $a \neq b$ $(a, b \in k)$.

Remark. The testing groups are all non trivial groups of index less than 56 in Σ_n and the groups whose invariant has the form $\delta_n\Theta$ where Θ in an invariant of the previous groups. Hence for the testing groups $\mathcal{H}_4$, $\mathcal{H}_8$ and $\mathcal{H}_{11}$, we can compute fastly some factors of the associated resolvents with the factors of the respective resolvents associated with the testing group $\mathcal{H}_2$, $\mathcal{H}_3$ and $\mathcal{H}_7$ (see Section 2).

4.1 Comments about the Tables of 3.2

It is difficult (but not impossible) to decide between T_{45} and T_{42}. With the absolute resolvents, there exist three methods for this purpose :

- $[T_{45}, T_{48}]_3 = \Sigma_3^2$ and $[T_{42}, T_{48}]_3 = \Sigma_3 \times \mathcal{A}_3$; the T_{48}-resolvents must be computed with a numerical approximation of the roots of f ;
- $[T_{45}, \mathcal{H}_{16}]_6 = H_{15}^{(6)}$ and $[T_{42}, , \mathcal{H}_{16}]_6 = H_{24}^{(6)}$, where $\mathcal{H}_{16} = \mathcal{D}_8 \times \Sigma_4$; $x_1x_2x_3^2x_4^2$ is an invariant of $\mathcal{H}_{16}$ and the associated resolvent can be computed rapidly; but its degree 210 is big ;
- $[T_{45}, \mathcal{H}_{12}] = (16, 96)$ and $[T_{42}, \mathcal{H}_{12}] = (8^2, 96)$; where $\mathcal{H}_{12} = \mathcal{A}_3 \times \Sigma_5$; the formal $\mathcal{H}_{12}$-resolvent $\mathcal{L}_{\delta_3}$ is partially tabulated but the computation of $\mathcal{L}_{\delta_3,f}$ is very long ; its degree 112 can be lowered to 56 since $\mathcal{L}_{\delta_3,f}$ is an even polynomial.

With the tables of Section 3.2, the algorithm based only on the partitions of the resolvents is very accelerated except for the following candidate groups which can be determined quickly using only the partitions : $T_{50}, T_{49}, T_{47}, T_{46}, T_{34}$, T_{43}, T_{22}, T_{11} and T_5. For the other candidate groups, this new table allows an important progress in their determination. For the following groups, the computation now requires only a few seconds or a few minutes instead of many hours : T_{48}, T_{36}, T_{25}, $T_{44}, T_{38}, T_{40}, T_{41}$, T_{33}, T_{29}, T_{19}, T_{24}, T_{13}.

For example, to decide between the candidate groups T_{48} and T_{36} using only the partition resolvents, the testing group of smallest index is $H = \mathcal{A}_3 \times \Sigma_5$

and the degree of an H-resolvent is 112. Now to decide between T_{48} and T_{36} it is sufficient to determine the Galois group of the irreducible factor of degree 7 of an $\mathcal{H}_3$-resolvent instead the previous H-resolvent. The $\mathcal{H}_3$-resolvent can be computed and factorized quickly and so is the determination of the Galois group in the degree 7 (see [11]).

4.2 The tables in Degree 8

In the following tables we do not give the Galois groups of the factors that we have computed when the candidate group can be determined without them. But it is very easy to compute these groups with the program `GAP` of Section 6.

For all subgroup T of $\mathcal{A}_8$ we have $[T, \mathcal{H}_1] = (8^+, 8^+)$.

$[T, \mathcal{H}_1]$	$\not\leq \mathcal{A}_8, = T_{49}$
16	$T_{50}\ T_{47}\ T_{44}\ T_{38}\ T_{40}\ T_{35}\ T_{30}\ T_{27}\ T_{31}\ T_{43}\ T_{26}\ T_{17}\ T_{23}\ T_{15}\ T_8\ T_6$
8^2	$T_{46}\ T_{28}\ T_{16}\ T_{21}\ T_7\ T_1$

$[T, \mathcal{H}_8]$	$\not\leq \mathcal{A}_8$	$\leq \mathcal{A}_8$
70	T_{50}	
$T_3^{(6)}, T_{33}^2, 48$	$, T_{38}$	
$T_3^{(6)}, T_{41}^2, 48$	T_{44}	
$T_2^{(6)}, T_{34}^2, 48$	T_{40}	
$T_2^{(6)}, T_{14}^2, 48$	T_{23}	
$14^2, 42$	T_{43}	
$2, 32, 36$	$T_{47}\ T_{46}$	
35^2		T_{49}
$2, 4, 8^2, 16, 32$	$T_{35}\ T_{30}\ T_{27}$	
$2, 4, 8^4, 32$	T_{28}	
$7^2, 28^2$		$T_{48}\ T_{36}\ T_{25}$
$3^2, 4^4, 24^2$		$T_{39}\ T_{32}\ T_{12}$
$7^4, 21^2$		T_{37}
$1^2, 16^2, 18^2$		$T_{45}\ T_{42}$
$2^3, 8^2, 16^3$	$T_{31}\ T_{26}\ T_{17}$	
	$T_{15}\ T_8$	
$1^2, 6^2, 12^2, 16^2$		$T_{41}\ T_{33}$
$2^3, 8^4, 16^2$	$T_{16}\ T_{21}\ T_7$	
$1^2, 2^2, 4^4, 8^2, 16^2$		$T_{29}\ T_{19}\ T_{20}$
$1^2, 6^6, 16^2$		T_{34}
$1^2, 2^6, 4^6, 16^2$		$T_{18}\ T_{10}$
$2^3, 4^4, 8^4, 16$	T_6	
$1^2, 3^4, 4^2, 12^4$		$T_{13}\ T_{24}$
$1^2, 3^4, 4^2, 6^4, 12^2$		T_{14}
$1^6, V_4^4, 8^6$	T_1	$T_{22}\ T_{11}\ T_5$
$1^6, 2^4, 4^6, 8^4$		$T_9\ T_2$
$1^6, 2^8, 4^8, 8^2$		T_4
$1^{14}, 4^{14}$		T_3

$[T, T_{48}]$	$\not\leq \mathcal{A}_8$	$\leq \mathcal{A}_8$
30	T_{50}	
$6, 24$	$T_{47}\ T_{46}$	
$2, 12, 16$	$T_{44}\ T_{38}$	
	$T_{40}\ T_{23}$	
$2, 4, 8, 16$	$T_{35}\ T_{30}$	
	$T_{28}\ T_{27}$	
$2, \mathcal{D}_4^3, 16$	$T_{31}\ T_{26}$	
$2, \mathcal{D}_4^2, \mathcal{C}_4, 16$	$T_{16}\ T_{21}\ T_{17}$	
$2, \mathcal{D}_4^2, V_4, 16$	$T_8\ T_{15}$	
$2, \mathcal{C}_4, V_4, 16$	T_7	
15^2		T_{49}
$2, 14^2$	T_{43}	
$1, 7, 8, 14$		$T_{48}\ T_{36}\ T_{25}$
${\Sigma_3}^2, 12^2$		T_{45}
$\mathcal{A}_3, \Sigma_3, 12^2$		T_{42}
$1, 2, \mathcal{A}_3, \Sigma_4, 8, 12$		T_{41}
$1, 2, \mathcal{C}_3, \mathcal{A}_4, 8, 12$		T_{33}
$1^3, 3, 4^3, 12$		T_{34}
$1^2, 6^2, 8^2$		$T_{39}\ T_{32}\ T_{12}$
$2^3, 4^2, 8^2$	$T_6\ T_1$	
$1^2, 2^2, \mathcal{D}_4^2, 8^2$		$T_{29}\ T_{20}$
$1^2, 2^2, \mathcal{C}_4, \mathcal{D}_4, 8^2$		T_{19}
$1^2, 2^6, 8^2$		$T_{22}\ T_{11}\ T_5$
$1^2, 2, 3^2, 6^2, 8$		$T_{24}\ T_{13}$
$1^4, 2, 4^4, 8$		$T_{18}\ T_{10}$
$1^4, 2^5, 4^2, 8$		$T_9\ T_2$
$1^8, 2^7, 8$		T_3
$1^2, 7^4$		T_{37}
$1^4, 3^2, 4^2, 6^2$		T_{14}
$1^6, 2^4, 4^4$		T_4

$[T, \mathcal{H}_7]$	$\not\leq \mathcal{A}_8$	$\leq \mathcal{A}_8$
56	$T_{50}\ T_{43}$	$T_{49}\ T_{48}\ T_{36}\ T_{37}\ T_{25}$
$T, 48$	$T_{47}\ T_{46}$	$T_{45}\ T_{42}\ T_{41}\ T_{34}\ T_{33}$
$24, 32$	$T_{44}\ T_{38}\ T_{40}$	$T_{39}\ T_{32}$
$T, 16, 32$	$T_{35}\ T_{30}\ T_{28}\ T_{26}\ T_{17}$	$T_{29}\ T_{19}$
$T^3, 32$	$T_{27}\ T_{31}\ T_{16}\ T_{21}$	$T_{20}\ T_{22}$
$8, 24^2$	T_{23}	$T_{24}\ T_{12}\ T_{14}\ T_{13}$
$T, 16^3$	T_{15}	T_{18}
$8^3, 16^2$	$T_8\ T_6\ T_7$	$T_{11}\ T_{10}\ T_9$
8^7	T_1	$T_5\ T_4\ T_2\ T_3$

H	$[T_{45}, H]$	$[T_{42}, H]$
$\mathcal{H}_2$	$(12^+, 16^+)$	$(12^+, 16^+)$
$\mathcal{H}_3$	$(1, 12^+, 18^+)$	$(1, 12^+, 18^+)$
$\mathcal{H}_5$	$(24^+, 32^+)$	$(24^+, 32^+)$
$\mathcal{H}_6$	$(24^+, 32^+)$	$(24^+, 32^+)$

$[T,\mathcal{H}_2]$	$\not\leq \mathcal{A}_8$	$\leq \mathcal{A}_8$
28	$T_{50}\ T_{43}$	$T_{49}\ T_{48}\ T_{36}\ T_{37}\ T_{25}$
$\Sigma_4, 24$	$T_{44}\ T_{40}\ T_{23}$	T_{39}
$\mathcal{A}_4, 24$	T_{38}	$T_{32}\ T_{12}$
$12, 16$	$T_{47}\ T_{46}$	$T_{45}\ T_{42}\ T_{41}\ T_{34}\ T_{33}$
$\mathcal{D}_4, T, 16$	$T_{35}\ T_{30}\ T_{28}$	$T_{29}\ T_{19}$
	$T_{26}\ T_{17}$	
	$T_{15}\ T_8$	
$\mathcal{C}_4, T, 16$	$T_{27}\ T_{16}\ T_7$	T_{20}
$\mathcal{D}_4^3, 16$		T_{18}
$\mathcal{C}_4, \mathcal{D}_4^2, 16$		T_{10}
$\Sigma_4, (12^+)^2$		T_{24}
$\Sigma_4, 12^+, 12^-$		T_{14}
$\mathcal{A}_\triangle, 12^2$		T_{13}
V_4, T^3	$T_{31}\ T_{21}$	$T_{22}\ T_{11}\ T_5$
$\mathcal{D}_4, 8^3$	T_6	
$\mathcal{C}_4, 8^3$	T_1	
$V_4, \mathcal{D}_4^2, 8^2$		T_9
V_4^3, T_2^2		T_2
$\mathcal{D}_4^4, V_4, 8$		T_4
V_4^7		T_3

$[T,\mathcal{H}_{11}]$	$\not\leq \mathcal{A}_8$	$\leq \mathcal{A}_8$
112	$T_{50}\ T_{43}$	
16,96	T_{47}	
48,64	$T_{44}\ T_{38}\ T_{40}$	
16,32,64	T_{35}	
$16^3, 64$	$T_{30}\ T_{27}\ T_{31}\ T_{26}$	
56^2		$T_{49}\ T_{48}\ T_{36}$
		$T_{37}\ T_{25}$
$16, 48^2$	T_{23}	
$T^2, 48^2$	T_{46}	$T_{45}\ T_{42}\ T_{41}$
		$T_{34}\ T_{33}$
$8^2, 16^2, 32^2$	T_{28}	$T_{29}\ T_{19}$
$16^3, 32^2$	$T_{17}\ T_{15}$	
$8^6, 32^2$	$T_{16}\ T_{21}$	$T_{20}\ T_{22}$
$24^2, 32$		$T_{39}\ T_{32}$
$8^2, 24^4$		$T_{24}\ T_{12}$
		$T_{14}\ T_{13}$
16^7	$T_8\ T_6$	
$8^2, 16^6$		T_{18}
$8^6, 16^4$	T_7	$T_{11}\ T_{10}\ T_9$
8^{14}	T_1	$T_5\ T_4\ T_2\ T_3$

$[T,\mathcal{H}_3]$	$\not\leq \mathcal{A}_8$	$\leq \mathcal{A}_8$
35	T_{50}	T_{49}
$T_5^{(7)}, 28$		T_{48}
$T_3^{(7)}, 28$		T_{36}
$T_1^{(7)}, 28$		T_{25}
$\Sigma_3, T_{41}, 24$	T_{44}	
$\mathcal{A}_3, T_{33}, 24$	T_{38}	
$\Sigma_3, T_{34}, 24$	T_{40}	
$\Sigma_3, T_{14}, 24$	T_{23}	
$\mathcal{A}_3, \Sigma_4^2, 24$		T_{39}
$\mathcal{A}_3, \mathcal{A}_4^2, 24$		$T_{32}\ T_{12}$
14,21	T_{43}	
$T_5^{(7)}, H_{18}^{(7)}, 21$		T_{37}
$1, 16, 18$	$T_{47}\ T_{46}$	$T_{45}\ T_{42}$
$1, T_7^{(6)}, 12, 16$		T_{41}
$1, T_4^{(6)}, 12, 16$		T_{33}
$1, 2, 8^2, 16$	$T_{35}\ T_{30}\ T_{28}\ T_{27}\ T_{16}\ T_7$	
$1, 2, T_{26}, T_{18}, 16$	T_{26}	
$1, 2, T_{17}, T_{10}, 16$	T_{17}	
$1, 2, T_{15}, T_9, 16$	T_{15}	
$1, 2, T_8, T_4, 16$	T_8	
$1, 2, \mathcal{C}_4, \mathcal{D}_4, 8, 16$		T_{19}
$1, 2, \mathcal{D}_4^2, 8, 16$		$T_{29}\ T_{20}$
$1, 6^3, 16$		T_{34}
$1, 3^3, 4, 6^2, 12$		T_{14}
$1, 2^3, \mathcal{D}_4^3, 16$		T_{18}
$1, 2^3, \mathcal{D}_4^2, \mathcal{C}_4, 16$		T_{10}
$1, 3^2, 4, 12^2$		$T_{24}\ T_{13}$
$1^3, 8^4$	$T_{31}\ T_{21}$	
$1, 2, 4^2, 8^3$	$T_6\ T_1$	T_2
$1^3, V_4^2, T^3$		$T_{22}\ T_{11}\ T_5$
$1^3, 2^2, 4^3, 8^2$		T_9
$1^3, 2^4, 4^4, 8$		T_4
$1^7, 4^7$		T_3

$[T,\mathcal{H}_4]$	$\not\leq \mathcal{A}_8$	$\leq \mathcal{A}_8$
56	$T_{50}\ T_{43}$	
$T_{24}, 48$	T_{44}	
$8, 48$	T_{38}	
$T_{14}, 48$	$T_{40}\ T_{23}$	
$24, 32$	T_{47}	
$T_9, 16, 32$	T_{35}	
$T_4, 16, 32$	T_{30}	
$8, 16, 32$	T_{27}	
$12^2, 32$	T_{46}	
$4^2, 8^2, 32$	T_{28}	
28^2		$T_{49}\ T_{48}\ T_{36}$
		$T_{37}\ T_{25}$
$\Sigma_4^2, 24^2$		T_{39}
$\mathcal{A}_4^2, 24^2$		$T_{32}\ T_{12}$
$8, 16^3$	T_{31}	
$T_4, 16^3$	$T_{26}\ T_{17}$	
	$T_{15}\ T_8$	
${12^+}^2, {16^+}^2$		$T_{45}\ T_{42}$
$12^2, 16^2$		$T_{41}\ T_{34}\ T_{33}$
$\mathcal{C}_4^2, T^2, 16^2$	$T_{16}\ T_7$	T_{20}
$\mathcal{D}_4^2, T^2, 16^2$		$T_{29}\ T_{19}$
$V_4^2, T^2, 16^2$	T_{21}	
${\mathcal{D}_\triangle}^6, 16^2$		T_{18}
${\mathcal{C}_\triangle}^2, {\mathcal{D}_\triangle}^4, 16^2$		T_{10}
$8^5, 16$	T_6	
$\Sigma_4^2, 12^4$		$T_{24}\ T_{14}$
$\mathcal{A}_4^2, 12^4$		T_{13}
V_4^2, T^6		$T_{22}\ T_{11}\ T_5$
$4^2, 8^6$	T_1	
$\mathcal{D}_4^4, V_4^2, T_9^4$		T_9
$\mathcal{C}_4^4, V_4^2, T_2^4$		T_2
$4^{10}, 8^2$		T_4
4^{14}		T_3

$[T, \mathcal{H}_5]$	$\not\leq \mathcal{A}_8$	$\leq \mathcal{A}_8$
56	$T_{50}\,T_{43}$	$T_{49}\,T_{48}\,T_{36}$ $T_{37}\,T_{25}$
$T, 48$	$T_{44}\,T_{38}\,T_{40}\,T_{23}$	$T_{39}\,T_{32}$
$24, 32$	$T_{47}\,T_{46}$	$T_{45}\,T_{42}\,T_{41}$ $T_{34}\,T_{33}$
$8, 16, 32$	$T_{35}\,T_{30}\,T_{28}$	
$T, 16, 32$	$T_{26}\,T_{15}$	$T_{29}\,T_{19}$
$8^3, 32$	T_{17}	T_{18}
$8, 24^2$		$T_{24}\,T_{12}\,T_{14}\,T_{13}$
$8, 16^3$	$T_{27}\,T_{31}\,T_{16}$ $T_{21}\,T_8\,T_6$	$T_{20}\,T_{22}$
$8^3, 16^2$	T_7	$T_{11}\,T_{10}\,T_9$
8^7	T_1	$T_5\,T_4\,T_2\,T_3$

$[T, \mathcal{H}_6]$	$\not\leq \mathcal{A}_8$	$\leq \mathcal{A}_8$
56	$T_{50}\,T_{43}$	$T_{49}\,T_{48}\,T_{36}\,T_{37}\,T_{25}$
$8, 48$	$T_{44}\,T_{38}\,T_{40}$	$T_{39}\,T_{32}$
$24, 32$	T_{47}	$T_{45}\,T_{42}\,T_{41}\,T_{34}\,T_{33}$
$T, 16, 32$	$T_{35}\,T_{27}\,T_{26}\,T_{17}$	$T_{29}\,T_{19}$
$8^3, 32$	T_{15}	T_{18}
$8, 24^2$	T_{23}	$T_{24}\,T_{12}\,T_{14}\,T_{13}$
$16^2, 24$	T_{46}	
$8, 16^3$	$T_{30}\,T_{28}\,T_{31}\,T_{16}$	$T_{20}\,T_{22}$
$8^3, 16^2$	$T_8\,T_6\,T_7$	$T_{11}\,T_{10}\,T_9$
$8^5, 16$	T_{21}	
8^7	T_1	$T_5\,T_4\,T_2\,T_3$

4.3 Information about Non Separable Resolvents

It is not necessary that all resolvents be separable. By the theorem of multiplicity, only the interesting factors must be simple. For example, we have $[T_3, \mathcal{H}_2] = \{V_4\}^7$. Let f be a polynomial of degree 8 whose Galois group is T_3. If a $\mathcal{H}_4$-resolvent is not separable, but its factor of degree 4 is simple then its Galois group is V_4. Conversely if f is a polynomial such that a $\mathcal{H}_2$-resolvent of f has a simple factor of degree 4 whose Galois group is not V_4, then $Gal_k(f) \neq T_3$.

5 Degree 10

The groups $T_1, \ldots, T_{45}$ are the transitive groups of degree 10 which appear in [11].

In the article [7] we have completed the tables of partitions in degree 10 and 11 given in [22]. The degree 10, for the transitive candidate groups cannot be dealt with only with this submatrix of the matrix of partitions, with Σ_{10} as reference group; the computation of relative resolvents is needed.

This section gives the Galois groups of the factor resolvents of degree less than 10 in the submatrix of partition of [7]. Hence, it is now possible to identify the candidate groups T_{11}, T_{34}, T_{36}, T_{37}, T_{38}, T_{39} and accelerate the algorithm of [7] in many cases.

5.1 The testing Groups

The following testing groups is a subset of the testing groups which appear in the paper [7]. Let A, B et C be the following subgroups of Σ_{10} :
$A = [(1,2,8),(1,3,8),(1,4,8),(1,5,8),(1,6,8),(1,7,8),(1,2)(9,10)]$;
$B = [(3,4,5,6,7),(1,2,3),(8,9,10),(9,10)(1,2)]$;
$C = (1,2,3,4,5),(1,2),(6,7,8,9,10),(6,7),(1,6)(2,7)(3,8)(4,9)(5,10)]$

Groups		Index	Invariants
H_1	$\mathcal{A}_{10}$	2	δ_{10}
H_2	$\mathcal{A}_9 \times Id$	20	δ_9
H_3	$\Sigma_2 \times \Sigma_8$	45	$s(x_1, x_2)$
H_4	$\Sigma_3 \times \Sigma_7$	120	$s(x_1, x_2, x_3)$
H_5	$Id_2 \times \Sigma_8$	90	$\delta_2\, , l(x_1, x_2)\, , m(x_1, x_2)$
H_6	$\Sigma_4 \times \Sigma_6$	210	$s(x_1, x_2, x_3, x_4)$
H_7	$\Sigma_5 \times \Sigma_5$	252	$s(x_1, x_2, x_3, x_4, x_5)$
H_9	A	90	$\delta_8\delta_2(x_9, x_{10})\, , \delta_{10}s(x_9, x_{10})$
H_{10}	B	240	$\delta_{10}s(x_1, x_2, x_3)$
H_{11}	C	126	$b_{10} = x_1 \cdots x_5 + x_6 \cdots x_{10}$
H_{12}	$\mathcal{A}_8 \times \Sigma_2$	90	$\delta_8\, , \delta_{10}\delta_2(x_9, x_{10})$
H_{14}	G_4	252	$\delta_{10}b_{10}$

5.2 Tables in Degree 10

For $\Theta = x_1 - x_2$ or $\Theta = x_1x_2$, a factor of degree 5 of the resolvent $\mathcal{L}_{\Theta,f}$ gives rapidly the factor of degree 10 of $\mathcal{L}_{\delta_{10}\Theta,f}$ (see Section 2).

T	T_{39}	T_{38}	T_{29}	T_{25}	T_{23}	T_{16}
$[T, H_{12}]_{10}$	T_{37}	T_{38}	T_{24}^+	T_{25}^-		
$[T, H_9]_{10}$			T_5	(20)	T_3	T_2

$[T, H_3]_5$	T
Σ_5	T_{37} T_{39} T_{38} T_{22} T_{12}
$\mathcal{A}_5$	T_{34} T_{36} T_{11}
$\mathcal{M}_5$	T_{24} T_{29} T_{25} T_5
$\mathcal{C}_5$	T_{14} T_8 T_1
$T_2^{(5)}$	T_{23} T_{16} T_{15} T_3

5.3 Comments

If we compare with [7], using the following tables we do not compute:

- $\mathcal{L}_{b_{10},f}$ to determine T_{29}, T_{36} or T_{24}
- $\mathcal{L}_{x_1-x_2,f}$ to determine T_5, T_8, T_{11}, T_{12} T_{14}, T_{15} and T_{22}
- $\mathcal{L}_{\delta_{10}x_1x_2,f}$ to determine T_1 and T_3.

For the six sets $\{T_{43}, T_{33}\}$, $\{T_{41}, T_{40}\}$, $\{T_{28}, T_{18}\}$, $\{T_{21}, T_{10}, T_9\}$, $\{T_{22}, T_{12}\}$ and $\{T_{27}, T_{20}, T_{19}, T_{17}\}$ is necessary to compute relative resolvents to decide between the candidate groups in each set ($Id_3 \times \Sigma_7$ determines T_{43} and T_{33}, but its index is 720). With the function `Index` of [17], we have the following results: T_{33} is a subgroup of index 36 in T_{43} ; T_{40} is a subgroup of index 2 in T_{41} ; T_{20}, T_{19} and T_{17} are subgroups of index 2 in T_{27} ; T_{12} is a subgroup of index 2 in T_{22} and T_{10} and T_9 are subgroups of index 2 in T_{21}.

6 Galois Inverse Problem

There exist some lists of irreducible polynomials (see [23] [18], [2], [3], the list of Mattman,J. McKay and G. Smith in degree 8, the list of Alexander Hulpke in degree 10 ...). The list of Alexander Hulpke is not complete and allows 33 groups. With GAP, we have computed the Galois groups associated with the parts of degree 10 in all partition matrices of the reference group Σ_n ($n = 4, \dots, 10$) that we have tabulated them. Many of them give a Galois group that is not Σ_{10}. In particular T_{26} is the Galois group of $\tau(x) = x^{10} - 28116x^8 + 263503152x^6 - 4216050432x^5 - 823183846848x^4 + 59269236973056x^3 - 164584085603401728x + 4443770311291846656$. The list of Alexander Hulpke has no group for T_{26}. Actually, with GAP we compute $[\Sigma_1 \times \mathcal{A}_6, \Sigma_1 \times T_{13}^{(6)}]_{10} = T_{26}^{(10)}$. The polynomial $b_6 = x_1x_2x_3 + x_4x_5x_6$ is an invariant of $\Sigma_1 \times T_{13}^{(6)}$ and $\Sigma_1 \times \mathcal{A}_6$ is the Galois group of the polynomial $(x-1)x^5(x-6) + 3124$ (We have used the polynomials given by G. Smith). The factor of degree 10 of the resolvent $\mathcal{L}_{b_6,p}$ computed with SYM is the polynomial τ.

7 Computation Using GAP

With the system GAP, it is easy to compute our group.

Consider the partition $I = [G, H] = (d_1^{m_1}, \dots, d_q^{m_q})$ in the partition matrix of Σ_n, with $m_i > 0$ for $i = 1, \dots q$. Let $m = m_1$ and $d = d_1$. We look for the m groups of $[G, H]_d$ corresponding to d^m in the partition I.

Let $\Gamma = \{\gamma_1, \dots, \gamma_e\}$ be a transversal of Σ_n mod H and $\mathcal{H} = \{\widetilde{H_1}, \dots, \widetilde{H_{dm}}\}$ the dm subgroups $G \cap \gamma_i H \gamma_i^{-1}$ of Σ_n, such that the index in G of $\widetilde{H_i}$ is equal to d. Then, it is possible to number $\mathcal{H}$ such that for $i = 1, \dots m$, if $\tau_1, \dots, \tau_d$ is a transversal of G mod $\widetilde{H_{id}}$, then, $\{\tau_1 \widetilde{H_{id}} \tau_1^{-1}, \dots, \tau_d \widetilde{H_{id}} \tau_d^{-1}\}$, the set of the conjugates (no necessarily distincts) of $\widetilde{H_{id}}$ is equal to the subset $\{\widetilde{H_{id-d+1}}, \widetilde{H_{id-d+2}}, \dots, \widetilde{H_{id}}\}$ of $\mathcal{H}$. Let $U_i = G \bigcap_{j=id-d+1}^{id} \widetilde{H_j}$, for $i = 1, \dots, m$. Hence the m Galois groups of the factors of degree d of the H-resolvents of polynomials whose the Galois group is G are in set $[G, H]_d = \{G/U_1, \dots, G/U_m\}$ and can be calculated using the following algorithm GroupeResolvante (in pseudo-GAP) :

```
Inputs : S_n , G , H , d
Outputs  : sol=[G/U_1 , G/U_2 , ... , G/U_m]
lesconj := List(RightCosets(S_n,H),
               rc->Intersection(G,H^Representative(rc)));
lesconj:=Filtered(lesconj, ghi->Index(G,ghi)=d);
sol:=[];
while Length(lesconj)>d-1 do
   gh:= lesconj[1];
   lesconj_g := List(RightCosets(g,gh),
                    rc->gh^Representative(rc));
   for ghj in lesconj_g do
       lesconj_aux :=[];
       while not(ghj=lesconj[1]) do
             Add(lesconj_aux,lesconj[1]);
             lesconj:=Sublist(lesconj,[2..Length(lesconj)]);od;
```

```
      lesconj:=Sublist(lesconj,[2..Length(lesconj)]);
      Append(lesconj,lesconj_aux);     od;
   for ghj in Sublist(lesconj_g,[2..degre_resol]) do
      gh := Intersection(gh,ghj);       od;
   Add(sol,FactorGroup(G,gh));  od;
return sol;
```

8 Conclusions

This paper proves the interest of the computation of the Galois group of the irreducible factors of a resolvent, and also that this computation is easy.

With I. Gilles, we have computed polynomials of degree 12 using the method of Section 5. The degrees 4 to 8, for square free polynomials can also be accelerated using this new method. We are now computing the corresponding groups.

Acknowledgement

I wish to thank the GDR MEDICIS. Without its servers, none of the computations of this paper could have been performed successfully.

References

1. Arnaudiès, J.M., Valibouze, A.: Résolvantes de Lagrange. Rapport LITP **93.61** (1993)
2. Arnaudiès, J.M., Valibouze, A.: Groupes de Galois de polynômes en degré 8. Rapport LITP **94.25** Mars 1994
3. Arnaudiès, J.M., Valibouze, A.: Groupes de Galois de polynômes en degré 9. Rapport LITP **94.30** Mai 1994
4. Arnaudiès, J.M., Valibouze, A.: Calculs de résolvantes. Rapport LITP **94.46** Juillet 1994
5. Arnaudiès, J.M., Valibouze, A.: Groupes de Galois de polynômes de degré 4 à 6. Rapport LITP **94.48** Juillet 1994
6. Arnaudiès, J.M., Valibouze, A.: Groupes de Galois de polynômes de degré 7. Rapport LITP **94.49** Juillet 1994
7. Arnaudiès, J.M., Valibouze, A.: Groupes de Galois de polynômes de degré 10 et 11. Rapport LITP **94.50** Juillet 1994
8. Arnaudiès, J.M., GAP, Valibouze, A.: Calculs de groupes de matrices de partitions. (preprint). Juillet 1994
9. Berwick, E.H.: The Condition That A Quintic Equation Should Be Soluble By Radicals. Proc. London Math. Soc. (2) **14** (1915) 301-307.
10. Berwick, E.H.: On Soluble Sextic equations. Proc. London Math. Soc. (2) **29** (1929) 1-28.
11. Gregory Butler and John McKay : The transitive groups of degree up to 11. Comm. Algebra **11** (1983) 863-911.
12. Casperson, D., McKay, J.: Symmetric functions, m-sets, and Galois groups. To appear in Math. Comp. (1994)

13. Antoine Colin : Théorie de Galois effective et implantation en AXIOM. Mémoire de DEA, colin@cosme.polytechnique.fr (1994)
14. Colin, A.: Formal computation of Galois groups using relative resolvent polynomials. These proceedings.
15. Foulkes, H.O.: The resolvents of an equation of seventh degree. Quart. J. Math. Oxford Ser. (2) (1931) 9-19
16. Girstmair, K.: On invariant Polynomials and Their Application in Field Theory Maths of Comp., vol. 48, no 178 (1987) 781-797
17. G.A.P.: Groups, Algorithms and Programming. Martin Schönert and others, Lehrstuhl D für Mathematik,
Rheinisch-Westfälische Technische Hochschule, Aachen, **93**
18. Helmut Geyer : Programme zur Berechnung des Galoisgruppen von Polynomen 8. und 9. Grades ; Dokumentation. Preprint 93-10 LWR Heidelberg, Mars 1993
19. Hulpke, A. : Alexander.Hulpke@math.rwth.aachen.de
20. Lagrange, J.L.: Réflexions sur la résolution algébrique des équations. Mémoires de l'Académie de Berlin, 205-421, (Oeuvres de Lagrange **tome IV** 205-421)
21. E. Luther : Ueber die Factoren des algebraisch lsbaren irreducible Gleichungen vom sechsten Grade und ihren Resolvanten. Journal fr Math. **37** (1848) 193-220.
22. J. McKay et E.Regener : Actions of permutation groups on r-sets. Communications in Algebra, **13(3)** (1985) 619-630
23. John McKay and Leonard Soicher : Computing Galois Groups over the rationals. Journal of number theory **20** (1985) 273-281.
24. Maxima DOE maintenu par William SCHELTER
25. R.P. Stauduhar: The determination of Galois groups. Math. Comp. **27** (1973) 981-996.
26. N. Tchebotarev : Grundzge des Galois'shen Theorie. P. Noordhoff, 1950
27. Valibouze, A.: Manipulations de fonctions symétriques. Thèse de l'Université Paris VI. (1988)
28. Valibouze, A.: Symbolic computation with symmetric polynomials, an extension to Macsyma. Conférence Computers and Mathematics (1989, MIT, Cambridge, Mass.). Springer-Verlag, (1989) 308-320.
29. Valibouze, A.: Extension `SYM` de `MACSYMA`, manuel de l'utilisateur. (manuscrit)

This article was processed using the LaTeX macro package with LLNCS style