Calcul de polynômes caractéristiques associés à certains anneaux quotients

Philippe Aubry
Annick Valibouze
LIP6, Université Paris 6
4, Place Jussieu 75252 Paris Cedex 05
Tel : (33) 01 44 27 33 41 (33) 01 44 27 62 43
e-mail : aubry@calfor.lip6.fr avb@calfor.lip6.fr

résumé

Soit k un corps parfait. Ce papier présente un algorithme efficace pour calculer le polynôme caractéristique d'endomorphismes d'anneaux quotients définis à partir de l'anneau polynomial $k[x_1, \dots, x_n]$ par un idéal engendé par un ensemble triangulaire de polynômes. Nous établissons que certains idéaux qui interviennent en théorie de Galois constructive satisfont la condition ci-dessus. Ces résultats sont exploités pour calculer efficacement les résolvantes relatives qui sont un outil fondamental en théorie de Galois constructive.

COMPUTING CHARACTERISTIC POLYNOMIALS ASSOCIATED TO SOME QUOTIENT RINGS

Philippe AUBRY, Annick VALIBOUZE
LIP6, Université Paris VI, 4, place Jussieu, F-75252 Paris Cedex 05
e-mail : aubry@calfor.lip6.fr, avb@calfor.lip6.fr

ABSTRACT. Let k be a perfect field. This paper presents an effective algorithm that computes characteristic polynomials of endomorphisms of quotient rings defined from the polynomial ring $k[x_1, \dots, x_n]$ by an ideal generated by a triangular set of polynomials. We establish that some ideals which occur in Galois theory satisfy the former requirement. These results are exploited to compute efficiently relative resolvents which are a fundamental tool in the effective algebraic Galois theory.

1. INTRODUCTION

Let k be a perfect field and $\bar{k}$ an algebraic closure of k. Let $x_1 < \dots < x_n$ be n ordered variables which are algebraically independent over k.

Let I be a radical zero dimensional ideal included in $k[x_1, \dots, x_n]$. For a polynomial $\Theta \in k[x_1, \dots, x_n]$, the **endomorphism of $A_I = k[x_1, \dots, x_n]/I$ associated with Θ**, and denoted by $\hat{\Theta}$, is defined by:

$$\begin{array}{ccc} A_I & \longrightarrow & A_I \\ P & \mapsto & \overline{\Theta}.P \end{array},$$

where $\overline{\Theta}$ is the class of Θ in A_I.

The characteristic polynomial associated with this endomorphism will be denoted by $C_{\Theta,I}$. Its coefficients lies in the field k like those of the matrice associated with the endomorphism $\hat{\Theta}$. It is well known from the classical theorem of Stikelberger that, when I is a radical ideal, we have:

$$C_{\Theta,I}(X) = \prod_{\beta \in V(I)} (X - \Theta(\beta)) , \tag{1}$$

where $V(I)$ is the algebraic variety of I in $\bar{k}^n$.

This paper presents an algorithm for computing the characteristic polynomial in the particular case where the ideal I admits a *separable triangular set* of generators (see Definition 2.6). This algorithm may be exploited in Galois Theory; it may be related to the computation of *resolvents* (see Definition 6.5) and more generally to the main problem of finding the Galois group of a given polynomial f.

The resolvent is the fundamental tool in the effective Galois theory. It has been introduced by J.L. Lagrange (see [3] and [14]). It is important to note that the resolvents relative to the symmetric group $\mathfrak{S}_n$, called absolute resolvents, can be computed with many algorithms (see [14], [18], [22] and [24]). But, when L is a proper subgroup of $\mathfrak{S}_n$, there exists only numerical methods (see [11] or [23]) and a linear method which requires hard generic computation (see [2] and [9]); the reader can see also [26] for computing linear factors of resolvents. In fact, the resolvent relative to a group L of permutations is immediately obtained from the characteristic polynomial $C_{\Theta,I}$ where I is a so-called *ideal of relations invariant* by L (see Definition 2.1). We show here that the ideal of relations invariant by some group of permutations which contains the Galois group of f is generated by a separable triangular set of polynomials. Thus our algorithm can be used to compute resolvents in Galois theory, and is an efficient tool for the computation of the Galois group of a given polynomial.

The paper is structured as follows. Section 2 introduces our terminology and notations. The third section contains some lemmas of commutative algebra; further proofs will refered to them. In Section 4, we establish a necessary and sufficient condition – related to its variety – for an ideal I to be generated by a separable triangular set. For an ideal I which satisfies this requirement, Section 5 gives the algorithm which computes the characteristic polynomial of an endomorphism of A_I associated with some polynomial Θ. In Section 6 we exploit the former results in Galois theory as mentionned above and illustrate their interest by an example.

2. Definitions, notations

Let f be a univariate polynomial of $k[X]$ supposed separable, with degree n. Let $\Omega = (\alpha_1, \dots, \alpha_n)$ be an ordered set of the n roots of f in $\bar{k}^n$. For $P \in k[x_1, \dots, x_n]$, the evaluation of P in Ω is denoted by $P(\Omega)$. We state $\mathfrak{S}_n$ for the symmetric group of degree n. For $\sigma \in \mathfrak{S}_n$ the action of σ on Ω, denoted by $\sigma.\Omega$ is defined by $\sigma.\Omega = (\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$.

Definition 2.1. *The* **ideal of Ω-relations invariant by a subgroup** *L of the symmetric group $\mathfrak{S}_n$, denoted by I_Ω^L, is defined by*

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

where $(\sigma.R)(x_1, \dots, x_n) = R(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

Definition 2.2. *The ideal $I_\Omega^{\mathfrak{S}_n}$ is called the* **ideal of symmetric relations** *of f. The ideal $I_\Omega^{\{Id\}}$ is called the* **ideal of relations** *of f and is simply denoted by I_Ω.*

Let us recall the definition of the Galois group.

Definition 2.3. *The* **Galois group of** *Ω over k, denoted by G_Ω, is the subgroup of $\mathfrak{S}_n$ defined by*

$$G_\Omega = \{\sigma \in \mathfrak{S}_n \mid (\forall P \in I_\Omega)\ \sigma.P(\Omega) = 0\} \ .$$

Usually G_Ω is also called the Galois group of f over k.

Remark 1. It obviously follows from the definition of the Galois group that

$$I_\Omega^{G_\Omega} = I_\Omega \ .$$

For $i \in [1,n]$ and $E \subset k[x_1,\dots,x_i]$, we denote by $\mathbf{Id}(E)$ the ideal generated by E in $k[x_1,\dots,x_n]$, by $Z_{\bar{k}^i}(E)$ the set of zeros of E in $\bar{k}^i$, and $V(E)$ the variety $Z_{\bar{k}^n}(E)$.

For a variety V in $\bar{k}^n$ we denote $\mathcal{J}(V)$ the radical ideal of $k[x_1,\dots,x_n]$ composed by the polynomials which cancel on V.

Notation 2.4. Let i and j be integers such that $1 \le i \le j \le n$. Let V be a subset of $\bar{k}^j$. We denote by $\pi_{j,i}$ the natural projection map from $\bar{k}^j$ to $\bar{k}^i$, which sends $(a_1,\dots,a_j)$ to $(a_1,\dots,a_i)$. Moreover we state $V_i = \pi_{j,i}(V)$.

Triangular sets of polynomials are an effective tool for solving algebraic systems (see [5]). In this paper we only need to deal with zero-dimensional ideals; the following definition is thus adapted from the terminology of the general case of positive dimension.

Definition 2.5. *A set T of n polynomials in $k[x_1,\dots,x_n]$ is called a* **triangular set** *of $k[x_1,\dots,x_n]$ if $T = \{f_1(x_1),\dots,f_n(x_1,\dots,x_n)\}$, where the i-th polynomial f_i is monic as a polynomial in x_i with degree$(f_i,x_i) > 0$.*

For a triangular set T in $k[x_1,\dots,x_n]$, we will always use in the paper the notation $T = \{f_1,\dots,f_n\}$, where f_i is the unique polynomial of T with x_i as greatest variable. It is clear that the ideal generated by a triangular set is zero-dimensional.

Remark 2. If the set of polynomials $f_1,\dots,f_n$ exists, it is a triangular reduced Gröbner basis of the ideal I for lexicographical ordering (see [7] or [6]).

For our purposes it is convenient to introduce a stronger concept:

Definition 2.6. *We say that a triangular set $T = \{f_1,\dots,f_n\}$ of $k[x_1,\dots,x_n]$ is a* **separable triangular set** *if each polynomial f_i satisfies the following condition:*
$\forall\beta = (\beta_1,\dots,\beta_{i-1}) \in V_{i-1}$, the univariate polynomial $f_i(\beta_1,\dots,\beta_{i-1},x_i)$ is separable, i.e. it has no multiple root in $\bar{k}[x_i]$.

Remark 3. Generally a zero-dimensional variety V cannot be expressed as zeros of a single separable triangular set, as shown in [15] with the simple following example:
$$V \;=\; V(x_1,x_2) \;\cup\; V(x_1,x_2+1) \;\cup\; V(x_1+1,x_2)\ .$$
However, it always can be splitted into a finite family of separable triangular sets (see [4],[15] and [19]).

3. Preliminaries

In this section we give some basic properties that we will use in proofs in the next section. For a subset E of a ring S, we write $\mathbf{Id}_S(E)$ for the ideal generated in S by E.

Lemma 3.1. *Let $\phi : R \to S$ be a surjective homomorphism of commutative rings. Let I be an ideal in R such that $Ker(\phi) \subseteq I$. We denote by J the ideal $\phi(I)$. Then I is the contraction of J to R under ϕ, that is:*
$$\phi^{-1}(J) = \{r \in R \mid \phi(r) \in J\} = I\ .$$

Proof. Note that J is an ideal of S because the homomorphism ϕ is surjective. We have obviously $I \subseteq \phi^{-1}(J)$. Conversely let $r \in \phi^{-1}(J)$. We have $\phi(r) \in J$. By definition of J there exists an element p in I such that $\phi(r) = \phi(p)$. Then from the assumption $Ker(\phi) \subseteq I$, we easily obtain that $r \in I$. Thus $\phi^{-1}(J) \subseteq I$. $\square$

Corollary 3.2. *With the hypothesis of Lemma 3.1, I is a radical ideal of R iff $\phi(I)$ is a radical ideal of S.*

Proof. We set $J = \phi(I)$. More generally it is known that

$$\phi^{-1}(\sqrt{J}) = \sqrt{\phi^{-1}(J)} \tag{2}$$

when ϕ is an homomorphism and I an ideal of R (see [21], p. 218). Hence if J is radical then I is obviously radical. Conversely let us assume that I is radical. With our hypothesis we have $I = \phi^{-1}(J)$. It follows from Relation (2) that $\phi^{-1}(\sqrt{J}) = \sqrt{I} = I$. Applying the homomorphism ϕ we obtain $\sqrt{J} = \phi(I) = J$. $\square$

Proposition 3.3. *Let $\mathcal{M}$ be an ideal of a ring R and I a proper ideal of $R[x]$ such that $\mathcal{M} \subseteq I$. If $I \neq \mathcal{M}R[x]$ then there exists a monic polynomial $g \in R[x] \setminus R$ such that $I = \mathbf{Id}_{R[x]}(\mathcal{M} \cup \{g\})$.*

Proof. The natural homomorphism from R to $R/\mathcal{M}$ induces a surjective homomorphism ϕ defined by

$$\begin{array}{rccc} \phi: & R[x] & \longrightarrow & (R/\mathcal{M})[x] \\ p = \sum c_k\, x^k & & \mapsto & \sum \overline{c_k}^{\mathcal{M}}\, x^k \end{array}$$

where $\overline{c}^{\mathcal{M}}$ is the class of c in $R/\mathcal{M}$.

The ideal $J = \phi(I)$ is a principal ideal since $R/\mathcal{M}$ is a field. It is not reduced to the null ideal, otherwise $I = \mathcal{M}R[x]$, which contradicts the hypothesis. Therefore J is generated by a monic univariate polynomial of $(R/\mathcal{M})[x]$. Thus there exists $g \in R[x]$ – which can be choosen with monic leading coefficient in x – such that J is generated by $\phi(g)$. However note that g is not equal to 1 since I is a proper ideal by assumption.

It is clear that $\phi^{-1}(J) = \mathbf{Id}_{R[x]}(\mathcal{M} \cup \{g\})$. Hence it follows from Lemma 3.1 that $I = \mathbf{Id}_{R[x]}(\mathcal{M} \cup \{g\})$. $\square$

Proposition 3.4. *Let k be a perfect field. Let $\mathcal{M}$ be a maximal ideal of $k[x_1, \ldots, x_{n-1}]$ and $g \in k[x_1, \ldots, x_n]$ such that degree$(g, x_n) > 0$ and g is monic w.r.t. the variable x_n. Then the following are equivalent:*

(i) *the ideal $\mathbf{Id}(\mathcal{M} \cup \{g\})$ is radical;*
(ii) $\forall \beta = (\beta_1, \ldots, \beta_{n-1}) \in V(\mathcal{M})$, $g(\beta_1, \ldots, \beta_{n-1}, x_n)$ *is a separable polynomial.*

Proof. Let $\beta \in V(\mathcal{M})$. From the isomorphism between the field $K = k(\beta_1, \ldots, \beta_{n-1})$ and $k[x_1, \ldots, x_{n-1}]/\mathcal{M}$ we deduce the following surjective homomorphism:

$$\begin{array}{rccc} \phi: & k[x_1, \ldots, x_n] & \longrightarrow & K[x_n] \\ p = \sum c_k(x_1, \ldots, x_{n-1})\, x_n^k & & \longmapsto & \sum c_k(\beta_1, \ldots, \beta_{n-1})\, x_n^k \end{array}$$

The ideal $\phi(\mathbf{Id}(\mathcal{M} \cup \{g\}))$ is generated in $K[x_n]$ by the image of g. Since the field k is perfect the algebraic extension K is also perfect. Thus $\mathbf{Id}_{K[x_n]}(g(\beta_1, \dots, \beta_{n-1}, x_n))$ is radical if and only if the univariate polynomial $g(\beta_1, \dots, \beta_{n-1}, x_n)$ is separable. Then the assertion follows from Corollary 3.2. □

The following variant of chinese remainder Theorem appears implicitly in [15].

Lemma 3.5. *Let $I_1, \dots, I_m$ be pairwise comaximal ideals in a ring R and $I = \cap_{j=1}^m I_j$. Let $p_1, \dots, p_m$ be monic polynomials of the same positive degree d in $R[X]$. Then there exists a monic polynomial $p \in R[X]$ of degree d such that*

$$(\forall j \in [1, m]) \quad p \equiv p_j \pmod{I_j R[X]} \ . \tag{3}$$

Moreover we have

$$\mathbf{Id}_{R[X]}(I \cup \{p\}) \ = \ \cap_{j=1}^m \mathbf{Id}_{R[X]}(I_j \cup \{p_j\}) \ . \tag{4}$$

Proof. First we show by induction the existence of a polynomial p which satisfies (3). Let $m = 2$. Since I_1 and I_2 are comaximal in R, there exists $a_1 \in I_1$ and $a_2 \in I_2$ such that $a_1 + a_2 = 1$. We state $p = a_2 p_1 + a_1 p_2$. Then p is monic and degree$(p) = d$. Moreover one can easily check that $p \equiv p_j \pmod{I_j R[X]}$ for $j \in \{1, 2\}$. For $m > 2$, it follows from hypothesis that I_1 and $\cap_{i=2}^m I_i$ are comaximal ideals. Therefore we obtain the first property of the lemma by induction.

Now, let us show Relation (4). Let j be an integer in $[1, m]$. By Property (3), we obtain $p \in \mathbf{Id}_{R[X]}(I_j \cup \{p_j\})$. Then $\mathbf{Id}_{R[X]}(I \cup \{p\}) \ \subseteq \ \mathbf{Id}_{R[X]}(I_j \cup \{p_j\})$ obviously follows, and thus $\mathbf{Id}_{R[X]}(I \cup \{p\}) \ \subseteq \ \cap_{j=1}^m \mathbf{Id}_{R[X]}(I_j \cup \{p_j\})$.

Conversely, let $f \in \cap_{j=1}^m \mathbf{Id}_{R[X]}(I_j \cup \{p_j\})$. For each $j \in [1, m]$ there exists q_j in $R[X]$ such that $f - q_j p_j \in \ I_j R[X]$. By chinese remainder Theorem there exists a polynomial q in $R[X]$ such that $q \equiv q_j \pmod{I_j R[X]}$ for each j in $[1, n]$. Consequently we have

$$\begin{aligned} f - qp \ &\equiv \ f - q_j p_j \pmod{I_j R[X]} \\ &\equiv \ 0 \pmod{I_j R[X]} \ . \end{aligned}$$

It follows that $(f - qp) \in IR[X]$ and so $f \in \mathbf{Id}_{R[X]}(I \cup \{p\})$. □

Now, let us recall some properties on zero-dimensional varieties.

Proposition 3.6. *Let V be a zero-dimensional variety in $\bar{k}^n$ and $I = \mathcal{J}(V)$. Then the following hold:*

1. *The ideal I contains a non-constant univariate polynomial in each of the variables in $\{x_1, \dots, x_n\}$, and the elimination ideal $I \cap k[x_1, \dots, x_{n-1}]$ is a zero-dimensional ideal of $k[x_1, \dots, x_{n-1}]$;*
2. *For each i in $[1, n]$, the projection V_i is a variety in $\bar{k}^i$ which is zero-dimensional, and $V_i = Z_{\bar{k}^i}(I \cap k[x_1, \dots, x_i])$;*
3. *The ideal of V_i in $k[x_1, \dots, x_i]$ corresponds to $I \cap k[x_1, \dots, x_i]$.*

Proof. See Lemma 6.50 in [6] for the first point. We obtain assertion 2 by induction from first point and Corollary 4 in p.124 of [10]. The third assertion obviously follows from the relation $V_i = Z_{\bar{k}^i}(I \cap k[x_1, \dots, x_i])$ and the fact that I is radical. □

4. Zero-dimensional varieties and separable triangular sets

In this section, we introduce the concept of *equiprojectable* variety. We show that it characterizes the zero-dimensional varieties which can be expressed as $V(T)$ where T is a separable triangular set. It follows that the ideal of the equiprojectable variety is the ideal generated by T.

Now let us state two properties of triangular sets. First, the projection of the algebraic variety of a triangular set T is easily obtained from the polynomials of T in the following way:

Proposition 4.1. *Let $T = \{f_1, \dots, f_n\}$ be a triangular set of $k[x_1, \dots, x_n]$ and i be an integer in $[1, n]$. Then we have*

$$\pi_{n,i}(V(T)) = Z_{\bar{k}^i}(f_1(x_1), \dots, f_i(x_1, \dots, x_i)) \ .$$

Proof. We clearly have $V(T) \cap \bar{k}^i \subseteq Z_{\bar{k}^i}(f_1, \dots, f_i)$. Now let us assume that $\beta = (\beta_1, \dots, \beta_i) \in Z_{\bar{k}^i}(f_1, \dots, f_i)$. By definition the polynomial $f_{i+1}(\beta_1, \dots, \beta_i, x_{i+1})$ is monic. This univariate polynomial has positive degree; therefore it admits at least one root β_{i+1} in $\bar{k}$. Thus $(\beta_1, \dots, \beta_i, \beta_{i+1})$ is a zero of $\{f_1, \dots, f_{i+1}\}$ in $\bar{k}^{i+1}$. In the same way we can find $\beta_{i+2}, \dots, \beta_n$ such that $(\beta_1, \dots, \beta_n) \in V(T)$, which proves the inclusion $Z_{\bar{k}^i}(f_1, \dots, f_i) \subseteq V(T) \cap \bar{k}^i$. ☐

Proposition 4.2. *Let $n > 0$ and T be a separable triangular set of $k[x_1, \dots, x_n]$. Then* $\mathbf{Id}(T)$ *is radical.*

Proof. We show the result by induction on n. If $n = 1$ we deduce it immediately from the definition of a separable triangular set. Let $n > 1$ and $T = \{f_1, \dots, f_n\}$. We denote by T' the triangular set $\{f_1, \dots, f_{n-1}\}$ of $k[x_1, \dots, x_{n-1}]$. By induction hypothesis the zero-dimensional ideal I' generated by T' in $k[x_1, \dots, x_{n-1}]$ is radical. Hence there exists $\mathcal{M}_1, \dots, \mathcal{M}_r$ maximal ideals of $k[x_1, \dots, x_{n-1}]$ such that $I' = \cap_{j=1}^r \mathcal{M}_j$. Using Lemma 3.5 (with f_n for each p_j), we obtain

$$\mathbf{Id}(T) = \cap_{j=1}^r \mathbf{Id}(\mathcal{M}_j \cup \{f_n\}) \ .$$

Then the assertion follows from Proposition 3.4 ☐

Now we define what is an equiprojectable finite subset V of $\bar{k}^n$.

Definition 4.3. *Let $1 \leq i \leq j \leq n$ and V be a finite subset of $\bar{k}^j$. The set V is said* **equiprojectable on** *V_i, its projection on $\hat{k}^i$, if there exists an integer c such that for each point M in V_i, we have*

$$card(\pi_{j,i}^{-1}(M)) = c \ .$$

The positive integer c will be denoted by $c_i(V)$.

Definition 4.4. *With the notations of Definition 4.3, we say that V is* **equiprojectable** *if V is equiprojectable on V_i for each $i \in [1, j]$.*

An equiprojectable subset of $\bar{k}^n$ may be characterized by induction. This equivalence will be useful for further proofs.

Proposition 4.5. *Let V be a finite subset of $\bar{k}^n$. Then V is equiprojectable iff V_{i+1} is equiprojectable on V_i for each $i \in [1, n-1]$.*

Proof. Let $1 \leq i < j \leq n$ and M be a point of V_i. Clearly we have

$$\pi_{n,i}^{-1}(M) = \bigcup_{M' \in \pi_{j,i}^{-1}(M)} \pi_{n,j}^{-1}(M') ,$$

and this union is disjoint. It follows that

$$\operatorname{card}(\pi_{n,i}^{-1}(M)) = \sum_{M' \in \pi_{j,i}^{-1}(M)} \operatorname{card}(\pi_{n,j}^{-1}(M')) . \tag{5}$$

Let us assume that V is equiprojectable on V_i for each $i \in [1, n]$. Let $i \in [1, n-1]$. For some point M in V_i, we obtain from Relation (5) above, with $j = i+1$, that $c_i(V) = \operatorname{card}(\pi_{i+1,i}^{-1}(M))\ c_{i+1}(V)$. Therefore $\operatorname{card}(\pi_{i+1,i}^{-1}(M))$ does not depend on the choice of the point M of V_i; thus V_{i+1} is equiprojectable on V_i.

Conversely, assume that V_{i+1} is equiprojectable on V_i for each $i \in [1, n-1]$. If $i \in [1, n-1]$ and M is a point of V_i, then an easy induction shows that

$$\operatorname{card}(\pi_{n,i}^{-1}(M)) = \prod_{i \leq j < n} c_j(V_{j+1}) . \tag{6}$$

It follows that V is equiprojectable on V_i. ☐

Before giving the main theorem of this section, we study in the following proposition the case where V is a variety such that V_{n-1} is irreducible. We will refer to this particular case in Theorem 4.7 by splitting V_{n-1} into irreducible components and recombining results with chinese remainders.

Proposition 4.6. *Let $n > 1$ and V be a zero-dimensional variety in $\bar{k}^n$ such that V_{n-1} is irreducible over k. Let us denote by $I = \mathcal{J}(V)$ the ideal of V, and $\mathcal{M}$ the ideal of V_{n-1} in $k[x_1, \ldots, x_{n-1}]$. Then V is equiprojectable on V_{n-1} and there exists a polynomial g in $k[x_1, \ldots, x_n]$ of degree d in x_n such that*

(i) $c_{n-1}(V) = d$;
(ii) $I = \mathbf{Id}(\mathcal{M} \cup \{g\})$;
(iii) *g is monic in x_n* ;
(iv) *$g(\beta_1, \ldots, \beta_{n-1}, x_n)$ is a separable polynomial for each $(\beta_1, \ldots, \beta_{n-1})$ in V_{n-1}.*

Proof. By Proposition 3.3 there exists g in $k[x_1, \ldots, x_n]$ for which properties (ii) and (iii) hold. Since the ideal I is radical, property (iv) follows from Proposition 3.4.

Now we prove Relation (i) and consequently that V is equiprojectable on V_{n-1}. Let $M = (\beta_1, \ldots, \beta_{n-1})$ be a point of V_{n-1} and $P = (\beta_1, \ldots, \beta_{n-1}, \beta_n)$ with $\beta_n \in \bar{k}$. We have:

$$\begin{aligned} P \in \pi_{n,n-1}^{-1}(M) \quad &\Longleftrightarrow \quad (\forall f \in \mathbf{Id}(\mathcal{M} \cup \{g\})) \quad f(\beta_1, \ldots, \beta_n) = 0 \\ &\Longleftrightarrow \quad g(\beta_1, \ldots, \beta_n) = 0 . \end{aligned}$$

Thus $P \in \pi_{n,n-1}^{-1}(M)$ iff β_n is a root of $g(\beta_1, \ldots, \beta_{n-1}, x_n)$. It follows that the number of elements in $\pi_{n,n-1}^{-1}(M)$ corresponds to the number of roots of $g(\beta_1, \ldots, \beta_{n-1}, x_n)$. Since this polynomial is separable we have $\mathrm{card}(\pi_{n,n-1}^{-1}(M)) = \mathrm{degree}(g, x_n) = d$. Relation (i) clearly follows. □

Theorem 4.7. *Let V be a zero-dimensional variety in $\bar{k}^n$. Then the following statements are equivalent:*

(1) *there exists a separable triangular set $T = \{f_1, \ldots, f_n\}$ such that $\mathcal{J}(V) = \mathbf{Id}(T)$;*
(2) *V is equiprojectable.*

Furthermore we have $c_i(V_{i+1}) =$ degree(f_{i+1}, x_{i+1}) and $c_i(V) = \prod_{j=i+1}^{n}$ degree(f_j, x_j).

Proof. First, we assume (1). Let $T = \{f_1, \ldots, f_n\}$ and $d_j = \mathrm{degree}(f_j, X_j)$. We want to show that for any i in $[1, n-1]$, the variety V_{i+1} is equiprojectable on V_i. Let us assume that $M = (\beta_1, \ldots, \beta_i)$ is a point of V_i. The polynomial $f_{i+1}(\beta_1, \ldots, \beta_i, x_{i+1})$ has no multiple root, and from Proposition 4.1 we have $V_{i+1} = Z_{\bar{k}^{i+1}}(f_1, \ldots, f_{i+1})$. Since the polynomials $f_1, \ldots, f_i$ cancel for $(\beta_1, \ldots, \beta_i)$, it is clear that the cardinal of $\pi_{i+1,i}^{-1}(M)$ equals d_{i+1}. Therefore V_{i+1} is equiprojectable on V_i. It follows from Proposition 4.5 that V is equiprojectable.

Remark that we also have shown that $\mathrm{degree}(f_{i+1}, x_{i+1}) = c_i(V_{i+1})$. Moreover the equality concerning $c_i(V)$ in the theorem is obtained by Relation (6) above. Thus last part of the theorem is proved.

Reciprocally, let V be an equiprojectable variety. We will show by induction on n that there exists a separable triangular set T which generates $\mathcal{J}(V)$.

If $n = 1$, the result is immediate since $k[x_1]$ is a principal ideal domain. Of course, there exists a monic polynomial f_1 which generates $\mathcal{J}(V)$, and the separability of f_1 follows from the fact that $\mathcal{J}(V)$ is radical and k is perfect.

Let $n > 1$. Let $V_{n-1} = W_1 \cup \ldots \cup W_r$ be the decomposition of the variety V_{n-1} into irreducible components. If we denote $\pi_{n,n-1}^{-1}(W_j) = \cup_{M \in W_j} \pi_{n,n-1}^{-1}(M)$, then we have

$$V = \pi_{n,n-1}^{-1}(W_1) \cup \ldots \cup \pi_{n,n-1}^{-1}(W_r) \ . \tag{7}$$

Let us denote by $\mathcal{M}_j$ the ideal of W_j in $k[x_1, \ldots, x_{n-1}]$; The ideal $\mathcal{M}_j$ is maximal. If I' is the ideal of V_{n-1} in $k[x_1, \ldots, x_{n-1}]$, then

$$I' = \mathcal{M}_1 \cap \ldots \cap \mathcal{M}_r \ .$$

Each $\pi_{n,n-1}^{-1}(W_j)$ is a variety (since it is the inverse image by an homomorphism of a closed set of $\bar{k}^n$ in the Zariski topology) which satisfies the hypothesis of Proposition 4.6. Hence there exists r polynomials $g_1, \ldots, g_r$ of $k[x_1, \ldots, x_n]$ such that for each $j \in [1, r]$

(i) $\mathrm{degree}(g_j, x_n) = \mathrm{card}(\pi_{n,n-1}^{-1}(M))$ where M is a point of W_j;
(ii) $\mathcal{J}(\pi_{n,n-1}^{-1}(W_j)) = \mathbf{Id}(\mathcal{M}_j \cup \{g_j\})$;
(iii) g_j is monic as univariate in x_n;
(iv) $g_j(\beta_1, \ldots, \beta_{n-1}, x_n)$ is a separable polynomial for each $(\beta_1, \ldots, \beta_{n-1})$ in W_j.

Besides, it is clear that the variety V_{n-1} in $\bar{k}^{n-1}$ is equiprojectable. According to the induction hypothesis, its ideal I' is therefore generated by a separable triangular set T'. Now, the equiprojectability of V on V_{n-1} will allow us to combine results (i) to (iv) in order to exhibit a convenient polynomial g with greatest variable x_n to *extend* T' into a triangular set of $k[x_1, \ldots, x_n]$. Thus, if we set $d = c_{n-1}(V)$, then by assertion (i), each g_j

has degree d relatively to x_n. By Lemma 3.5, there exists a polynomial $g \in k[x_1, \ldots, x_n]$, monic w.r.t. the variable x_n with degree$(g, x_n) = d$, such that

$$(\forall j \in [1, r]) \quad g \equiv g_j \pmod{\mathbf{Id}(\mathcal{M}_j)} , \tag{8}$$

and

$$\mathbf{Id}(I' \cup \{g\}) = \cap_{j=1}^{m} \mathbf{Id}(\mathcal{M}_j \cup \{g_j\}) .$$

Together with identity (ii), it follows that

$$\mathbf{Id}(I' \cup \{g\}) = \cap_{j=1}^{m} \mathcal{J}(\pi_{n,n-1}^{-1}(W_j)) ,$$

and by Relation (7)

$$\mathbf{Id}(I' \cup \{g\}) = \mathcal{J}(V) .$$

Thus we have

$$\mathcal{J}(V) = \mathbf{Id}(T' \cup \{g\}) .$$

Hence $\mathcal{J}(V)$ is generated by the triangular set $T = T' \cup \{g\}$.

We have to check that the triangular set T is separable. Let $M = (\beta_1, \ldots, \beta_{n-1})$ be a point of V_{n-1}; there exists an index j such that $M \in W_j$. From Relation (8) we easily obtain $g(\beta_1, \ldots, \beta_{n-1}, x_n) = g_j(\beta_1, \ldots, \beta_{n-1}, x_n)$ and deduce with assertion (iv) that T is a separable triangular set. ☐

5. Computation of characteristic polynomials

In this section we denote by K an extension of the field k such that $K \cap k[x_1, \ldots, x_n] = k$. For two polynomials p and q in $K[x_1, \ldots, x_n]$ and for $i \in [1, n]$, we denote by $\mathrm{Res}_{x_i}(p, q)$ the resultant of the polynomials p and q relatively to the variable x_i. The following lemma presents an algorithm which eliminates the variables $x_1, \ldots, x_n$ from a polynomial Ψ in $K[x_1, \ldots, x_n]$ and a separable triangular set of $k[x_1, \ldots, x_n]$. It will be exploited in Theorem 5.2 for computing characteristic polynomials $C_{\Theta,I}$, where Θ is a polynomial in $k[x_1, \ldots, x_n]$ and I is an ideal generated by a separable triangular set.

Lemma 5.1. *Let $T = \{f_1, \ldots, f_n\}$ be a separable triangular set of $k[x_1, \ldots, x_n]$. Let $\Psi \in K[x_1, \ldots, x_n]$. We define inductively the $n+1$ polynomials $\Psi_0, \Psi_1, \ldots, \Psi_n$ relatively to T as follows:*

$$\begin{array}{rcl} \Psi_n & := & \Psi \in K[x_1, \ldots, x_n] \\ \Psi_{i-1} & := & Res_{x_i}(f_i(x_1, \ldots, x_i), \Psi_i(x_1, \ldots, x_i)) \in K[x_1, \ldots, x_{i-1}] , \end{array}$$

Then the element Ψ_0 of K is given by:

$$\Psi_0 = \prod_{\beta \in V(T)} \Psi(\beta) .$$

Proof. At the beginning, $\Psi_0 = \mathrm{Res}_{x_1}(f_1(x_1), \Psi_1(x_1)) = \prod_{\beta_1 \in V_1} \Psi_1(\beta_1)$. Let us denote by V the variety $V(T)$. By induction, we prove that for each $j \in [1, n]$

$$\Psi_0 = \prod_{\{\beta_1, \dots, \beta_j\} \in V_j} \Psi_j(\beta_1, \dots, \beta_j) \ .$$

Supposing that our assertion is valid for $j = i - 1$, we have

$$\Psi_0 = \prod_{\{\beta_1, \dots, \beta_{i-1}\} \in V_{i-1}} \Psi_{i-1}(\beta_1, \dots, \beta_{i-1}) \ . \tag{9}$$

By definition of Ψ_{i-1}, the identity (9) becomes

$$\Psi_0 = \prod_{\{\beta_1, \dots, \beta_{i-1}\} \in V_{i-1}} \mathrm{Res}_{x_i}(f_i(\beta_1, \dots, \beta_{i-1}, x_i), \Psi_i(\beta_1, \dots, \beta_{i-1}, x_i)) \ .$$

Then the result follows from Proposition 4.1 and the fact that, by assumption, $f_i(\beta_1, \dots, \beta_{i-1}, x_i)$ is monic and separable in $\bar{k}[x_i]$. □

Theorem 5.2. *Let T be a separable triangular set and I the zero-dimensional ideal of $k[x_1, \dots, x_n]$ generated by T. Let $\Theta \in k[x_1, \dots, x_n]$. Then the characteristic polynomial $C_{\Theta,I}(X)$ of $k[X]$ is computable by the algorithm presented in Lemma 5.1.*

Proof. We just apply Lemma 5.1 with $\Psi = (X - \Theta) \in k[X][x_1, \dots, x_n]$. Thus we compute by successive resultants the polynomial $\Psi_0 = \prod_{\beta \in V(T)}(X - \Theta(\beta))$. Since the ideal I is radical (by Proposition 4.2) the characteristic polynomial $C_{\Theta,I}(X)$ is given by Relation (1) of Introduction and corresponds to Ψ_0. □

6. Application to Galois theory

In this section it is shown that if a group of permutations L contains the Galois group of f, then the ideal I_Ω^L (see Definition 2.1) is generated by a separable triangular set. We deduce that in this case, the *resolvents of f relative to L* can be obtained by computing characteristic polynomials with the algorithm described in Section 5. For computing such a relative resolvent, the triangular set which generates I_Ω^L must be known; but conversely, it is possible to obtain this triangular set from the generators of an ideal I_Ω^M, where $L < M$, if we are able to compute resolvent relative to M. An example will illustrate this link between the computation of relative resolvents and the computation of ideals of relations invariant by a group of permutations. It shows how it can be applied to find the Galois group of f.

6.1. Ideals of invariant Ω-relations and triangular sets.

Notation 6.1. Let L be a subgroup of $\mathfrak{S}_n$. We denote by $L_{(i)}$ the stabilizer of $\{1, \dots, i\}$ under the natural action of L.

$$L_{(i)} = \{\tau \in L \mid \forall k \in [1, i],\ \tau(k) = k\} \ .$$

Thus we obtain a chain of subgroups of L:

$$L_{(n)} = \{Id\} < L_{(n-1)} \dots < L_{(1)} < L \ .$$

Now let us study the left classes of L modulo $L_{(i)}$, that is, the classes of the equivalence relation $\sim_i$, defined by $\tau \sim_i \tau'$ if and only if $\tau^{-1}\tau' \in L_{(i)}$. We can characterize these classes as follows:

Lemma 6.2. *Let L be a subgroup of $\mathfrak{S}_n$ and $(\tau, \tau') \in L^2$. Then*

$$\tau \sim_i \tau' \iff \forall k \in \{1, \dots, i\},\ \tau(k) = \tau'(k)$$

and each equivalence class in $L/\sim_i$ has cardinality card$(L_{(i)})$.

Proof. We easily have the following equivalences:

$$\begin{aligned} \tau \sim_i \tau' &\iff \tau^{-1}\tau' \in L_{(i)} \\ &\iff (\forall k \in \{1, \dots, i\}) \quad \tau^{-1}\tau'(k) = k \\ &\iff (\forall k \in \{1, \dots, i\}) \quad \tau'(k) = \tau(k). \end{aligned}$$

The second part of this lemma is a basic result on left classes of a group L modulo a subgroup of L. $\square$

Lemma 6.2 applies to a particular family of subsets of $\bar{k}^n$ defined from subgroups of $\mathfrak{S}_n$ as follows:

Proposition 6.3. *Let f be a separable polynomial of $k[X]$ and Ω an ordered set of roots of f. If L is a subgroup of $\mathfrak{S}_n$, then the subset V of $\bar{k}^n$ defined by*

$$V = \{\sigma.\Omega \mid \sigma \in L\}$$

is equiprojectable.

Proof. Let $i \in [1, n]$ and $M \in V_i$. It is sufficient to show that the cardinality of $\pi_{n,i}^{-1}(M)$ is independant from the choice of the point M.

It follows from the definition of V that there exists a permutation τ in L such that $M = (\tau(1), \dots, \tau(i))$. Then the inverse image of M by $\pi_{n,i}$ may be defined by

$$\pi_{n,i}^{-1}(M) = \{\sigma.\Omega \mid \sigma \in L \text{ and } (\forall k \in \{1, \dots, i\})\ \ \sigma(k) = \tau(k)\}$$

Since the points of V are all distincts we have

$$\text{card}(\pi_{n,i}^{-1}(M)) = \text{card}(\{\sigma \in L \mid \sigma \sim_i \tau\}) = \text{card}(L_{(i)}) \ .$$

Thus the assertion is proved. $\square$

Remark 4. In general, the set V defined in Proposition 6.3 is not a variety over k. However it is a variety when $G_\Omega \subseteq L$.

Theorem 6.4. *Let Ω be an ordered set of roots of a univariate polynomial f supposed separable. Let L be a subgroup of $\mathfrak{S}_n$ which contains G_Ω. Then there exists a separable triangular set T such that*

$$I_\Omega^L = \mathbf{Id}(T).$$

Proof. If L contains the Galois group of Ω, it is known that $V(I_\Omega^L) = \{\sigma.\Omega \mid \sigma \in L\}$ (see [25]). Besides it is easy to verify that I_Ω^L is radical; thus $I_\Omega^L = \mathcal{J}(V(I_\Omega^L))$. Then the result follows immediately from Proposition 6.3 and Theorem 4.7. □

Remark 5. The above result is well known when L is the group $\mathfrak{S}_n$. Let us recall that $I_\Omega^{\mathfrak{S}_n}$ is generated by the separable triangular set $\{f_1, \dots, f_n\}$ of *Cauchy moduli* defined by induction as follows:

$$\begin{aligned} f_1(x_1) &= f(x_1) \\ f_i(x_1, \dots, x_i) &= \frac{f_{i-1}(x_1, \dots, x_{i-2}, x_i) - f_{i-1}(x_1, \dots, x_{i-2}, x_{i-1})}{x_i - x_{i-1}} . \end{aligned}$$

The reader can refer to [20].

6.2. Characteristic polynomial and resolvent.

In the following, L is a subgroup of $\mathfrak{S}_n$ which contains G_Ω, the Galois group of Ω, and Θ is a polynomial of $k[x_1, \dots, x_n]$.

Definition 6.5. *The L-***relative resolvent of** Ω **by** Θ*, denoted by $\mathcal{L}_{\Theta, I_\Omega^L}$, is the following polynomial of $k[X]$:*

$$\mathcal{L}_{\Theta, I_\Omega^L}(X) = \prod_{\Phi \in L.\Theta} (X - \Phi(\Omega)) \ ,$$

where $L.\Theta$ is the natural orbit of the polynomial Θ under the action of the group L. When $L = \mathfrak{S}_n$ the resolvent $\mathcal{L}_{\Theta, I_\Omega^{\mathfrak{S}_n}}$ is called an **absolute resolvent** *of f by Θ.*

Remark 6. In literature the polynomial $\mathcal{L}_{\Theta, I_\Omega^L}$ is used to be called an L-relative resolvent of f by Θ. The fact that the coefficients of $\mathcal{L}_{\Theta, I_\Omega^L}$ are in k easily follows from Galois theory.

Lemma 6.6. *Let L be a subgroup of $\mathfrak{S}_n$ such that $G_\Omega < L$. Let $\Theta \in k[x_1, \dots, x_n]$. We set $d = card(H)$. Then we have:*

$$C_{\Theta, I_\Omega^L} = \mathcal{L}^d_{\Theta, I_\Omega^L} \ . \tag{10}$$

Proof. We saw in the proof of Theorem 6.4 that $V(I_\Omega^L) = \{\sigma.\Omega \mid \sigma \in L\}$ when $G_\Omega < L$. Hence Relation (1) of Introduction becomes

$$C_{\Theta, I_\Omega^L}(X) = \prod_{\sigma \in L} (X - \sigma.\Theta(\Omega)) \ .$$

The result easily follows. □

Remark 7. When the L-relative resolvent of Ω by Θ is separable, it is exactly the minimal polynomial of the endomorphism $\hat{\Theta}$.

Definition 6.7. *Let H be a subgroup of L and $\Theta \in k[x_1, \dots, x_n]$. The polynomial Θ is an L-**primitive** H-**invariant** if*

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

The following lemma is of prime importance for computing ideals of relations invariant by a subgroup of $\mathfrak{S}$. The reader will refer in [25] for the proof. It shows that if we can compute $\mathcal{L}_{\Theta, I_\Omega^L}$ then it is possible to construct a system of generators of I_Ω^H from a system of generators of I_Ω^L.

Lemma 6.8. *Let H be a subgroup of L such that $G_\Omega H$ is a group and Θ be an L-primitive H-invariant. We set $\theta = \Theta(\Omega)$. Let $Min_{\theta,k}$ be the minimal polynomial of θ over k. If θ is a simple root of the resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$ then*

$$I_\Omega^H = I_\Omega^L + \mathbf{Id}(Min_{\theta,k}(\Theta)) .$$

Remark 8. In Lemma 6.8 the minimal polynomial $\mathrm{Min}_{\theta,k}$ is a simple factor of the resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$.

Remark 9. The fact that θ must be a simple root of the resolvent in Lemma 6.8 is not really restrictive. Indeed it is known that if k is infinite then there exists an L-primitive H-invariant Θ such that $\mathcal{L}_{\Theta, I_\Omega^L}$ is separable (see [3]). In this case we see below that the problem of finding a system of generators of an ideal I_Ω^L and the problem of computing an L-relative resolvent resolve mutually.

Proposition 6.9. *Let k be a perfect field which is infinite. The L-relative resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$ of Ω by Θ can be computed by using the algorithm of Section 5.*

Proof. First, we need a system of generators of the ideal I_Ω^L. Let us assume without restriction that we know a system of generators of an ideal I_Ω^M for a subgroup M of $\mathfrak{S}_n$ which contains L: of course, we can choose $M = \mathfrak{S}_n$ (see Remark 5). According with Remark 9 we may assume that we have an M-primitive L-invariant Ψ such that $\mathcal{L}_{\Psi, I_\Omega^M}$ is separable. The value $\Psi(\Omega)$, which belongs to k, is then obtained by the factorization of $\mathcal{L}_{\Theta, I_\Omega^M}$. It follows from Lemma 6.8 that we know a generator system of I_Ω^L.

According with Theorem 6.4 the ideal I_Ω^L is generated by a separable triangular set $\{f_1, \dots, f_n\}$. Now, by Remark 2, the polynomials $f_1, \dots, f_n$ can be determined by the computation of a Gröbner basis of I_Ω^L from our system of generators of this ideal.

The basis $\{f_1, \dots, f_n\}$ being known, it follows from Theorem 5.2 that the characteristic polynomial C_{Θ, I_Ω^L} can be computed by the algorithm of Section 5. The resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$ is then immediately obtained with Formula (10). □

Remark 10. In the proof of Proposition 6.9 we obtain a system of generators of I_Ω^L by the computation of an absolute resolvent. But practically, if we want to avoid computing resolvents with high degree, we may obtain I_Ω^L by several steps with intermediate computations of relative resolvents and ideals of Ω-relations invariant by some subgroups of $\mathfrak{S}_n$ (see the example of Paragraph 6.4).

6.3. Implementation.

The algorithm presented in this paper for computing relative resolvents is analogous to a well-known method for computing absolute resolvents when L is the symmetric group of degree n (see [20]). This latter method becomes very efficient when the coefficients are reduced by the ideal $I_\Omega^{\mathfrak{S}_n}$ in each step. Thus the growth of coefficients is controlled and some variables may be eliminated before the computation of the corresponding resultant. Moreover extraneous powers which appears during the computation of resultants in the algorithm can be suppressed in each step by the method given in [17].

Both these previous principles can be applied for computing the resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$ in the case where $L \neq \mathfrak{S}_n$. Thus the method proposed here can be efficient in order to obtain the Galois group of f in the way suggested in Remark 10. It is always possible to compute only absolute resolvents; however it is better to compute relative resolvents $\mathcal{L}_{\Theta, I_\Omega^L}$ for $L \neq \mathfrak{S}_n$ since the degree of these resolvents increases with the order of L, and since these resolvents have to be factorized for extracting informations on the Galois group of f.

6.4. An explicit example.

This example illustrates our method for computing relative resolvents and its interest for computing the ideal of relations I_Ω (see Definition 2.2), which is equivalent to compute the Galois group G_Ω. It shows how both problems are linked together. We consider the polynomial $f = x^6 + 2$, irreducible over $\mathbb{Q}$, whose Galois group is a transitive subgroup of $\mathfrak{S}_6$. We will compute the ideal of relations between the roots of f using relative resolvents. In this subsection, for a subset E of $\mathbb{Q}[x_1, \dots, x_n]$ we will denote by $< E >$ the ideal generated by E in $\mathbb{Q}[x_1, \dots, x_n]$.

The first step consists in computing a triangular set which generates the ideal I_Ω^M for $M = \mathfrak{S}_6$. This set is given by the the Cauchy moduli of the polynomial f:

$$\begin{aligned} I_\Omega^{\mathfrak{S}_6} \quad = \quad & < x_6 + x_5 + x_4 + x_3 + x_2 + x_1, \\ & x_5^2 + x_4x_5 + x_3x_5 + x_2x_5 + x_1x_5 + x_4^2 + x_3x_4 + x_2x_4 + x_1x_4 + x_3^2 + x_2x_3 \\ & + x_1x_3 + x_2^2 + x_1x_2 + x_1^2, \\ & x_4^3 + x_3x_4^2 + x_2x_4^2 + x_1x_4^2 + x_3^2x_4 + x_2x_3x_4 + x_1x_3x_4 + x_2^2x_4 + x_1x_2x_4 + x_1^2x_4 \\ & + x_3^3 + x_2x_3^2 + x_1x_3^2 + x_2^2x_3 + x_1x_2x_3 + x_1^2x_3 + x_2^3 + x_1x_2^2 + x_1^2x_2 + x_1^3, \\ & x_3^4 + x_2x_3^3 + x_1x_3^3 + x_2^2x_3^2 + x_1x_2x_3^2 + x_1^2x_3^2 + x_2^3x_3 + x_1x_2^2x_3 + x_1^2x_2x_3 \\ & + x_1^3x_3 + x_2^4 + x_1x_2^3 + x_1^2x_2^2 + x_1^3x_2 + x_1^4, \\ & x_2^5 + x_1x_2^4 + x_1^2x_2^3 + x_1^3x_2^2 + x_1^4x_2 + x_1^5, \ x_1^6 + 2 > \quad . \end{aligned}$$

Let L =PGL$(2,5)$ the transitive maximal subgroup of $\mathfrak{S}_6$ of degree 120. We denote by Θ_3 the primitive L-invariant given in [13] (we do not give the explicite expression of this very big invariant). The computation of the separable absolute resolvent of f by Θ_3 is realized by an implementation of the method given in [20] for which the present paper is a generalization. Its factorization over $\mathbb{Q}$ is the following:

$$\mathcal{L}_{\Theta_3, I_f^{\mathfrak{S}_6}}(X) = (X-42)(X-24)^2(X+6)^3 \ .$$

In this case we know by partition matrix method (see [3]) that the Galois group of f is one of the following groups: PGL$(2,5)$, PSL$(2,5)$, the dihedral group $\mathcal{D}_6$ or the cyclic group $\mathcal{C}_6$, which are included in PGL$(2,5)$. By Lemma 6.8 the ideal I_Ω^L is the ideal generated by the union of the ideal $I_\Omega^{\mathfrak{S}_6}$ and the ideal $< \Theta_3 - 42 >$, where 42 is the value given by the linear factor over $\mathbb{Q}$ of $\mathcal{L}_{\Theta_3, I_f^{\mathfrak{S}_6}}$. The separable triangular set which generates the ideal I_Ω^L is obtained by computing a Gröbner base for the lexicographical ordering of this ideal. Thus we have:

$$\begin{aligned}
I_\Omega^{\mathrm{PGL}(2,5)} \quad = \quad & < 24x_6 + x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + 6x_3^3x_2x_1^3 + 5x_3^3x_1^4 + 8x_3^2x_2^3x_1^2 + 4x_3^2x_2^2x_1^3 \\
& +8x_3^2x_2x_1^4 + 6x_3x_2^3x_1^3 + 8x_3x_2^2x_1^4 - 4x_3x_2x_1^5 + 12x_3 + 5x_2^3x_1^4 + 12x_2 + 14x_1, \\
& 24x_5 - 5x_3^3x_2^4 - 7x_3^3x_2^3x_1 - 16x_3^3x_2^2x_1^2 - 7x_3^3x_2x_1^3 - 5x_3^3x_1^4 - 8x_3^2x_2^4x_1 \\
& -12x_3^2x_2^3x_1^2 - 12x_3^2x_2^2x_1^3 - 8x_3^2x_2x_1^4 - 12x_3x_2^4x_1^2 - 16x_3x_2^3x_1^3 - 12x_3x_2^2x_1^4 \\
& +8x_3 - 5x_2^4x_1^3 - 5x_2^3x_1^4 - 2x_2 - 2x_1, \\
& 24x_4 + 5x_3^3x_2^4 + 6x_3^3x_2^3x_1 + 8x_3^3x_2^2x_1^2 + x_3^3x_2x_1^3 + 8x_3^2x_2^4x_1 + 4x_3^2x_2^3x_1^2 \\
& +8x_3^2x_2^2x_1^3 + 12x_3x_2^4x_1^2 + 10x_3x_2^3x_1^3 + 4x_3x_2^2x_1^4 + 4x_3x_2x_1^5 + 4x_3 + 5x_2^4x_1^3 \\
& +14x_2 + 12x_1, \\
& x_3^4 + x_3^3x_2 + x_3^3x_1 + x_3^2x_2^2 + x_3^2x_2x_1 + x_3^2x_1^2 + x_3x_2^3 + x_3x_2^2x_1 + x_3x_2x_1^2 \\
& +x_3x_1^3 + x_2^4 + x_2^3x_1 + x_2^2x_1^2 + x_2x_1^3 + x_1^4, \\
& x_2^5 + x_2^4x_1 + x_2^3x_1^2 + x_2^2x_1^3 + x_2x_1^4 + x_1^5, \ x_1^6 + 2 > \quad .
\end{aligned}$$

Remark 11. We used the very powerful Gröbner engine FGb (see [12]) developed by J.C. Faugère to obtain this Gröbner base quickly.

Now, set M =PGL$(2,5)$. We choose the subgroup $L = \mathcal{D}_6$ (one of the conjugates) of M in order to compute an associated resolvent. We are in the following situation:

$$I_\Omega^{\mathfrak{S}_n} \subset I_\Omega^M \subset I_\Omega^L \subset I_\Omega^{\{Id\}} \ .$$

The polynomial $\Theta_4 = x_1x_4 + x_4x_5 + x_5x_2 + x_2x_3 + x_3x_6 + x_6x_1$ is a primitive $\mathcal{D}_6$-invariant, and a fortiori a PGL$(2,5)$-primitive $\mathcal{D}_6$-invariant. The PGL$(2,5)$-relative resolvent of f by Θ_4 has degree $10 = [M : L]$; its computation is performed modulo the ideal $I_\Omega^{\mathrm{PGL}(2,5)}$ by our method as follows:

- Let $R_0(X, x_1, \ldots, x_6) = X - \Theta_4$. The reduction of R_0 modulo the ideal I_Ω^M (given by successive euclidean divisions) eliminates the variables x_6, x_5 and x_4. Let $W_0(X, x_1, x_2, x_3)$ be the result of this reduction.

- We set $R_1(X, x_1, x_2) = \mathrm{Res}_{x_3}(f_3, W_0)$. The reduction of R_1 modulo the ideal I_Ω^M does not eliminate the variables x_1 and x_2 of respective degrees 32 and 28 in R_1, but produces a new polynomial W_1 of degree 4 in each variables x_1 and x_2.
- The elimination of the variable x_2 is given by $R_2(X, x_1) = \mathrm{Res}_{x_2}(f_2, W_1)$. The reduction of R_2 modulo the ideal I_Ω^M produces a univariate polynomial of degree 20 whose factorization is the following:

$$X^2(X^3-2)^2(X^3+2)^4 .$$

- The factorization over $\mathbb{Q}$ of the resolvent is:

$$\mathcal{L}_{\Theta_4, I_\Omega^M}(X) = X(X^3-2)(X^3+2)^2 .$$

The partitions matrix associated with M indicates that the Galois group of f is $\mathcal{D}_6$ or $\mathcal{C}_6$. The ideal fixed by $\mathcal{D}_6$ is given by:

$$I_\Omega^{\mathcal{D}_6} = I_\Omega^{\mathrm{PGL}(2,5)} + < \Theta_4 - 0 > ,$$

where 0 is the value given by the simple linear factor over $\mathbb{Q}$ of the resolvent $\mathcal{L}_{\Theta_4, I_\Omega^M}$. In the same way as for the ideal fixed by $\mathrm{PGL}(2,5)$, from a generator system of the ideal I_Ω^M and the polynomial Θ_4,we compute with FGb the following triangular set of generators of our ideal $I_\Omega^{\mathcal{D}_6}$:

$$I_\Omega^{\mathcal{D}_6} =< x_6 - x_3 - x_1, x_5 + x_3 + x_1, x_4 + x_3, x_3^2 + x_1x_3 + x_1^2, x_2 + x_1, x_1^6 + 2 > .$$

Now we set $M = \mathcal{D}_6$ and choose $L = \mathcal{C}_6$. Let $\Theta_5 = x_4x_5^2 + x_3x_6^2 + x_5x_2^2 + x_2x_3^2 + x_6x_1^2 + x_1x_4^2$ be an M-primitive L-invariant. The degree of an M-relative resolvent is 2, the index of L in M.

The reduction of Θ_5 modulo the ideal $I_\Omega^{\mathcal{D}_6}$ produces the value 0. We are in a degenerated case: the resolvent equals X^2 and the computation of the resolvent modulo the ideal $I_\Omega^{\mathcal{D}_6}$ produces the polynomial X. Many $\mathcal{D}_6$-primitive $\mathcal{C}_6$-invariants computed by Abdeljaouad's package (see [1]) are in this case. In order to find a $\mathcal{D}_6$-primitive $\mathcal{C}_6$-invariant which is not degenerated, we adopt Colin's method exposed in [9]. We replace the invariant $\Theta_5(x_1, \ldots, x_6)$ by the invariant $\Psi = \Theta_5(p(x_1), \ldots, p(x_6))$ where $p(x) = x^2 + 1$. The computation of the $\mathcal{D}_6$-relative resolvent of f by Ψ is realized using two reductions modulo the ideal $I_\Omega^{\mathcal{D}_6}$ and one resultant. It is the following irreducible polynomial:

$$\mathcal{L}_{\Psi, I_\Omega^{\mathcal{D}_6}}(X) = X^2 - 24X + 252 .$$

Since this resolvent is irreducible over $\mathbb{Q}$, the Galois group of f over $\mathbb{Q}$ is $\mathcal{D}_6$ and the ideal of relations among the roots of f is $I_\Omega^{\mathcal{D}_6}$.

7. Conclusions

Another algebraic method for computing the resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$, when L is not the symmetric group is proposed in [3]. In [9] an effective algorithm is given for this method. But this computation induces the formal computation of the coefficients of the polynomial $\prod_{\Psi \in L.\Theta}(x - \Psi)$. The method proposed in this paper is less expensive, since it needs only the computation of a Gröbner basis for lexicographical ordering of the ideal I_Ω^L, which can be realized by the algorithm given in [7] (see also [12] for an efficient method).

The numerical method proposed in [23] in order to compute resolvents is based on approximations of roots of f. It leads to some problems when the roots of f are close. This algebraic method avoids this problem and gives a general algorithm for arbitrary degrees and polynomials.

References

[1] Abdeljaouad, I. (1997). *Calcul d'invariants primitifs de groupes finis*, LIP6 Report 1997/020, Université Paris 6.

[2] Arnaudiès, J.M. (1976). *Sur la résolution explicite des équations de degré 5, quand elles sont résolubles par radicaux*, Bull. Sc. Math. 2^e série, vol. **100**, 241-254.

[3] Arnaudiès, J.M., Valibouze, A. (1996). *Lagrange resolvents*, special issue of MEGA'96 (A. Cohen and M.F. Roy Eds), Journ. of Pure and Appl. Alg. **117&118**, 23-40.

[4] Aubry, A. (1998). Ensembles triangulaires de polynômes, PhD thesis, Université Paris 6, preprint.

[5] Aubry, A., Moreno Maza, M. (1997). *Triangular sets for solving polynomial systems: A comparison of four methods*, LIP6 Report 1997/009, Université Paris 6, submitted to J. Symb. Comp.

[6] Becker, T., Weispfenning, V. (1993). Gröbner Bases, Springer-Verlag, Graduate texts in math. **141**.

[7] Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal, Phd Thesis, University of Innsbruck.

[8] Butler, G., McKay, J. (1983). *The transitive groups of degree up to 11*, Comm. Algebra **11**, 863-911.

[9] Colin, A. (1995). *Formal computation of Galois groups with relative resolvents*, Conference AAECC'10 (Paris, July 1995), LNCS **948**, 169-182.

[10] Cox, D., Little, J., O'Shea, D. (1992). Ideals, varieties and algorithms, Springer-Verlag, Undergraduate texts in mathematics.

[11] Eichenlaub, Y. (1996). Problèmes effectifs de théorie de Galois en degrés 8 à 11, PhD thesis, Université de Bordeaux 1.

[12] Faugère, J.C. (1997). *A new efficient algorithm for computing Gröbner Basis (F4)*, Task 3.3.2.1 Frisco report, preprint.

[13] Girstmair, K. (1987). On invariant polynomials and their application in field theory, Maths of Comp., vol. **48** (178), 781-797.

[14] Lagrange, J.L. (1770). *Réflexions sur la résolution algébrique des équations*, Mémoires de l'Académie de Berlin, 205-421.

[15] Lazard, D. (1992). *Solving zero–dimensional algebraic systems*, J. Symb. Comp., vol. **13**, 117-132.

[16] Lazard, D. (1991). *A new method for solving algebraic systems of positive dimension*, Discr. App. Math, vol. **33**, 147-160.

[17] Lehobey, F. (1997). *Resolvent computations by resultants without extraneous powers*, ISSAC'97 Conference (Hawai, July 1997).

[18] McKay, J., Soicher, L. (1985). Computing Galois Groups over the rationals, Journal of number theory **20**, 273-281.

[19] Moreno Maza, M. (1997). Calculs de pgcd au-dessus des tours d'extensions simples et résolution des systèmes d'équations algébriques, PhD thesis, Université Paris 6.

[20] Rennert, N., Valibouze, A. (1997). *Calcul de résolvantes avec les modules de Cauchy*, submitted to Exp. Math. (extension of LITP Report 95-62, (1995)).

[21] Samuel, P., Zariski, O. (1967). Commutative Algebra, vol. **I**, Van Nostrand Company.

[22] Soicher, L. (1981). The computations of Galois groups, PhD thesis, Concordia University, Montreal.

[23] Stauduhar, R.P. (1973). *The determination of Galois groups*, Math. Comp. **27**, 981-996.

[24] Valibouze, A. (1989). *Résolvantes et fonctions symétriques.* Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation, ISSAC'89 (Portland, Oregon). ACM Press, 390-399.

[25] Valibouze, A. (1997). Galois theory. Course given in departement of mathematics of the University of Pisa, (April 1997), preprint.

[26] Yokoyama, K. (1996) *A modular method for computing the Galois groups of polynomials*, special issue of MEGA'96 (A. Cohen and M.F. Roy Eds), Journ. of Pure and Appl. Alg. **117&118**, 617-636.