J. Symbolic Computation (2000) **30**, 635–651
doi:10.1006/jsco.2000.0376
Available online at http://www.idealibrary.com on IDEAL

Using Galois Ideals for Computing Relative Resolvents

PHILIPPE AUBRY AND ANNICK VALIBOUZE

LIP6, Université Paris 6, 4 Place Jussieu, 75252 Paris Cedex 05, France

In this paper we show that some ideals which occur in Galois theory are generated by triangular sets of polynomials. This geometric property seems important for the development of symbolic methods in Galois theory. It may and should be exploited in order to obtain more efficient algorithms, and it enables us to present a new algebraic method for computing relative resolvents which works with any polynomial invariant.

1. Introduction

Let k be a perfect field and $\bar{k}$ an algebraic closure of k. Let f be a separable univariate polynomial of $k[X]$ with degree n, and Ω be an ordered set of the n distinct roots of f in $\bar{k}^n$. In Valibouze (1999) the notion of ideal of Ω-relations invariant by a subset L of the symmetric group of degree n is introduced. It generalizes the notion of *ideal of relations* and the notion of *ideal of symmetric relations.* We call them *Galois ideals.*

This paper presents two major results. First, we prove in Theorem 5.3 that a Galois ideal associated with a group L containing the Galois group of f is generated by a *separable triangular set* of polynomials which forms a reduced Gröbner basis of this ideal for the lexicographical order. We think knowledge of such a property may simplify some problems, and thus it may be a basic tool for making algorithms in Galois theory more efficient. This remark may be taken into account when one is concerned with optimal implementation issues. Moreover, it may lead to new algorithms in Galois theory. The second major result of this paper illustrates this assertion since an algebraic method for computing *relative resolvents* is given (see Section 7). We also specify (Remark 7.11) that when the Galois group of the polynomial f is known, our algorithms may be employed for computing the ideal of relations among the roots of f and consequently for computations in the splitting field of f.

The *resolvent* is a fundamental tool, introduced by Lagrange (1770), in the constructive Galois theory. Later, Stauduhar (1973) extended the definition of J. L. Lagrange. Let us recall that the resolvents relative to the symmetric group Σ_n, called *absolute resolvents*, can be computed by many algorithms (Lagrange, 1770; Soicher, 1981; Soicher and McKay, 1985; Valibouze, 1989a; Casperson and McKay, 1994). For computing resolvents relative to some proper subgroup L of Σ_n, there exists a numerical approach (Stauduhar, 1973; Eichenlaub, 1996) and a p-adic approach (Darmon and Ford, 1989; Yokoyama, 1996; Geissler and Klüners, 2000) used for Galois group computation based on Stauduhar's algorithm. But in these methods, we do not need the resolvents themselves; we compute their integral roots with approximations of the roots of the given

0747–7171/00/120635 + 17 $35.00/0

polynomial. These techniques have shown their efficiency in practice. In particular, the recent implementation of Geissler and Klüners (2000) computes Galois groups for rational polynomials up to degree 15. However, the development of general algebraic methods is important for problems with non-numeric coefficients and knowledge of the algebraic structures. Our method avoids the swell of required precision to get proven results in the numerical approach, and is independent from some ill-conditioned problems for modular techniques. It works over any perfect field and with any polynomial invariant, like the symbolic method presented in Colin (1995).

The method based on the factorization of several absolute resolvents was introduced by Soicher and McKay (1985) and developed further by Arnaudiès and Valibouze (1996) with the construction of tables of partitions related to the subgroups of the symmetric group. Arnaudiès and Valibouze (1996) showed that relative resolvents can be used. It should be more efficient since the degree of the resolvents increases with the order of the group L, and these resolvents have to be factorized for extracting information on the Galois group of f. Moreover, using relative resolvents may avoid some degenerate cases with non-separable absolute resolvents.

Our algorithm requires only the triangular Gröbner basis of the Galois ideal associated with the group L. Due to the particular structure of the Galois ideals, I, considered, our method is in fact easily obtained from a natural algorithm for computing the characteristic polynomial of the multiplication by a polynomial inside the finite quotient algebra $k[x_1, \dots, x_n]/I$ (see Section 6).

The complexity of our method depends essentially on the complexity of computing lexicographical Gröbner bases. The average arithmetic cost for the computation of Gröbner bases in the zero-dimensional case is $d^{O(n)}$, where n is the number of variables and d the maximum degree of input polynomials (Lazard, 1991). Practically, some efficient implementations are available for the computation of Gröbner bases (Faugère, 1999). Note that this part of the computation in our method decreases when the polynomial f is reducible over k. In this case the computation splits into several computations of Gröbner bases with fewer variables. This point will be developed in a future paper.

The paper is structured as follows. Section 2 introduces our terminology and notations. The third section contains some lemmas of commutative algebra; they will be referred to by later proofs. In Section 4, we introduce the concept of an *equiprojectable* variety and we show that it gives a geometrical characterization of the ideals of $k[x_1, \dots, x_n]$ generated by separable triangular sets. In Section 5, this characterization is exploited to prove the main property for Galois ideals that we mentioned above. Section 6 presents the algorithm for computing the characteristic polynomial of the multiplication by a polynomial inside $k[x_1, \dots, x_n]/I$ in the particular case where the ideal I admits a separable triangular set of generators. The former results are exploited in Section 7 to give a method for computing relative resolvents in Galois theory. An explicit way of computing a triangular set of polynomials which generates a Galois ideal is simultaneously presented. Finally, a concrete example in degree 8 illustrates our method.

2. Definitions and Notations

Throughout the paper, k is a perfect field and $\bar{k}$ an algebraic closure of k. Let f be a separable univariate polynomial of $k[X]$ with degree n. Let $\Omega = (\alpha_1, \dots, \alpha_n)$ be a tuple, in $\bar{k}^n$, of the n roots of the polynomial f with some fixed order. Let $x_1 < \cdots < x_n$ be n ordered variables which are algebraically independent over k. For $P \in k[x_1, \dots, x_n]$, the evaluation of P in Ω is denoted by $P(\Omega)$. We denote by Σ_n the symmetric group of degree n. For $\sigma \in \Sigma_n$ the action of σ on Ω, denoted by $\sigma.\Omega$, is defined by $\sigma.\Omega = (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$.

The following definition has been introduced in Valibouze (1999) and generalizes the well known notions of *ideal of relations* and *ideal of symmetric relations*.

Definition 2.1. Let L be a subset of the symmetric group Σ_n. The *Galois (L,Ω)-ideal* is the ideal I_Ω^L of $k[x_1, \ldots, x_n]$ formed by the Ω-relations invariant by L:

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

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

Since the tuple Ω is fixed throughout the paper, the ideal I_Ω^L will also be called the Galois ideal associated with L.

Definition 2.2. The ideal $I_\Omega^{\Sigma_n}$ 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 Σ_n defined by

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

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

Remark 2.4. From the definition of the Galois group, it follows directly that $I_\Omega^{G_\Omega} = I_\Omega$.

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

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

Remark 2.5. The ideal I_Ω^L of Definition 2.1 can also be viewed as $\mathcal{J}(\{\sigma.\Omega \mid \sigma \in L\})$. Thus I_Ω^L is obviously radical.

Notation 2.6. *Let i and j be two integers such that $1 \leq i \leq j \leq n$. 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 $(a_1, \ldots, a_j)$ to $(a_1, \ldots, a_i)$. Moreover, we set $V_i = \pi_{j,i}(V)$.*

Triangular sets of polynomials are effective tools for solving algebraic systems (see Aubry and Moreno Maza, 1999); in particular, the generators of Galois ideals may be computed efficiently by triangular sets based methods as shown in Aubry (1999). In this paper we need to deal with zero-dimensional ideals only; the following definition is thus adapted from the terminology of the general case of positive dimension.

Definition 2.7. A set T of n polynomials in $k[x_1, \ldots, x_n]$ is called a *triangular set* of $k[x_1, \ldots, x_n]$ if $T = \{f_1(x_1), \ldots, f_n(x_1, \ldots, x_n)\}$, where the ith polynomial f_i is monic as a polynomial in x_i with $\deg(f_i, x_i) > 0$.

For a triangular set T in $k[x_1, \dots, x_n]$, we use the notation $T = \{f_1, \dots, f_n\}$, where f_i is the unique polynomial of T with x_i as greatest variable (recall that we fixed the order $x_1 < \cdots < x_n$).

Remark 2.8. If T is a triangular set then $\mathbf{Id}(T)$ is a zero-dimensional ideal and T is a reduced Gröbner basis of $\mathbf{Id}(T)$ for the lexicographical ordering. Moreover, for any integer i in $[1, n]$ we have $\pi_{n,i}(V(T)) = Z_{\bar{k}^i}(f_1(x_1), \dots, f_i(x_1, \dots, x_i))$. (See Becker and Weispfenning (1993) or Buchberger (1965).)

For our purpose it is convenient to introduce a stronger concept.

Definition 2.9. Let $T = \{f_1, \dots, f_n\}$ be a triangular set of $k[x_1, \dots, x_n]$ and $V = V(T)$. We say that T is *separable* 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 $\bar{k}[x_i]$.

We say that an ideal of $k[x_1, \dots, x_n]$ is a *triangular ideal* if it admits a separable triangular set of generators.

Remark 2.10. In general a zero-dimensional k-variety V cannot be expressed as zeros of a single separable triangular set, as shown in Lazard (1992) with the following simple example:

$$V = V(x_1, x_2) \,\cup\, V(x_1, x_2 + 1) \,\cup\, V(x_1 + 1, x_2).$$

However, it can always be decomposed into a finite family of varieties defined by separable triangular sets (see Lazard, 1992, and Aubry and Moreno Maza, 1999).

3. Commutative Algebra Preliminaries

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

Proposition 3.1. *Let $\mathcal{M}$ be a maximal ideal of a commutative 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 $\phi: \ R[x] \longrightarrow (R/\mathcal{M})[x]$ defined by $\phi(\sum c_k\, x^k) = \sum \overline{c_k}^{\mathcal{M}}\, x^k$ where $\overline{c}^{\mathcal{M}}$ is the class of c in $R/\mathcal{M}$.

By assumption the ideal $J = \phi(I)$ is not the zero ideal of the principal ideal domain $(R/\mathcal{M})[x]$. Therefore J is generated by a monic univariate polynomial of $(R/\mathcal{M})[x]$. Thus, there exists $g \in R[x]$—which can be chosen with a monic leading coefficient in x—such that J is generated by $\phi(g)$. It follows from the correspondence between the ideals in $R[x]$ and the ring $(R/\mathcal{M})[x]$ (see Zariski and Samuel, 1967, III.5, Theorem 7) that $I = \phi^{-1}(J) = \mathbf{Id}_{R[x]}(\mathcal{M} \cup \{g\})$. □

Proposition 3.2. *Let k be a perfect field and $\mathcal{M}$ a maximal ideal of $k[x_1, \dots, x_{n-1}]$. Let $g \in k[x_1, \dots, x_n]$ such that $\deg(g, x_n) > 0$ 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:

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

Let $I = \mathbf{Id}(\mathcal{M} \cup \{g\})$ and $J = \phi(I)$. It is known that $I = \phi^{-1}(J)$ is radical if and only if J is radical (Zariski and Samuel, 1967, III.7, formula (22)). Since k is perfect, the algebraic extension K is also perfect and therefore $J = \mathbf{Id}_{K[x_n]}(\phi(g))$ is radical if and only if the univariate polynomial $g(\beta_1, \ldots, \beta_{n-1}, x_n)$ is separable. □

The following variant of the Chinese remainder theorem appears implicitly in Lazard (1992). Its proof is easily deduced from the proof of the standard version of the Chinese remainder theorem.

Lemma 3.3. *Let* $I_1, \ldots, I_m$ *be pairwise comaximal ideals in a commutative ring* R *and* $I = \cap_{j=1}^m I_j$. *Let* $p_1, \ldots, p_m$ *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*

$$(\forall j \in [1, m]) \quad p \equiv p_j \pmod{I_j R[X]}. \tag{3.1}$$

Moreover, we have

$$\mathbf{Id}_{R[X]}(I \cup \{p\}) = \cap_{j=1}^m \mathbf{Id}_{R[X]}(I_j \cup \{p_j\}). \tag{3.2}$$

Proposition 3.4. *Let* $n > 0$ *and* T *be a separable triangular set of* $k[x_1, \ldots, x_n]$. *Then* $\mathbf{Id}(T)$ *is radical.*

Proof. It is obvious for $n = 1$. By induction, we assume that the ideal generated by $\{f_1, \ldots, f_{n-1}\}$ in $k[x_1, \ldots, x_{n-1}]$ is the intersection of maximal ideals. The result is then obtained for n by applying Lemma 3.3 (with f_n for each p_j) and Proposition 3.2. □

4. A Characterization of Zero-dimensional Triangular Ideals

This section introduces the concept of an *equiprojectable* variety. This concept characterizes the zero-dimensional k-varieties that can be expressed as $V(T)$, where T is a separable triangular set. It follows that the ideal of the equiprojectable k-variety is the ideal generated by T. Our geometrical characterization of triangular ideals provides a tool to prove the triangular structure of Galois ideals in Section 5.

Definition 4.1. Let $1 \le i \le j \le n$ and V be a finite subset of $\bar{k}^j$. The set V is said to be *equiprojectable on* V_i, its projection on $\bar{k}^i$, if there exists an integer c such that for each point M in V_i, we have

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

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

Definition 4.2. A set $V \subseteq \bar{k}^n$ is said simply *equiprojectable* if V is equiprojectable on V_i for each $i \in [1, n]$.

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

Proposition 4.3. *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 the following disjoint union:

$$\pi_{n,i}^{-1}(M) = \cup_{M' \in \pi_{j,i}^{-1}(M)} \, \pi_{n,j}^{-1}(M'). \tag{4.1}$$

We 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, it follows from relation (4.1) above that

$$c_i(V) = \mathrm{card}(\pi_{i+1,i}^{-1}(M)) \; c_{i+1}(V). \tag{4.2}$$

Therefore $\mathrm{card}(\pi_{i+1,i}^{-1}(M))$ does not depend on the choice of the point M of 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

$$\mathrm{card}(\pi_{n,i}^{-1}(M)) = \prod_{i \leq j < n} c_j(V_{j+1}). \tag{4.3}$$

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 k-variety such that V_{n-1} is irreducible. We will refer to this particular case in Theorem 4.5 by splitting V_{n-1} into irreducible components and recombining the results with Chinese remainders.

Proposition 4.4. *Let $n > 1$ and V be a zero-dimensional k-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) the polynomial 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 3.1 there exists a 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 3.2.

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

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

Thus, $P \in \pi_{n,n-1}^{-1}(M)$ iff β_n is a root of $g(\beta_1, \ldots, \beta_{n-1}, x_n)$. Since this latter polynomial is separable, we have $\mathrm{card}(\pi_{n,n-1}^{-1}(M)) = \deg(g, x_n) = d$. Relation (*i*) follows clearly. □

Theorem 4.5. *Let V be a zero-dimensional k-variety in $\bar{k}^n$. Then the following statements are equivalent:*

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

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

Proof. We assume that the first assertion is true. Let $d_j = \deg(f_j, x_j)$. Let $i \in [1, n-1]$ and $M = (\beta_1, \dots, \beta_i)$ be a point of V_i. By hypothesis the polynomial $f_{i+1}(\beta_1, \dots, \beta_i, x_{i+1})$ has exactly d_{i+1} distinct roots, and since $V_{i+1} = Z_{\bar{k}^{i+1}}(f_1, \dots, f_{i+1})$, the cardinal of $\pi^{-1}_{i+1,i}(M)$ equals d_{i+1}. Thus, V_{i+1} is equiprojectable on V_i. It follows from Proposition 4.3 that V is equiprojectable.

We remark that we also have shown that $\deg(f_{i+1}, x_{i+1}) = c_i(V_{i+1})$. Moreover, the equality concerning $c_i(V)$ in the theorem is obtained by relation (4.3) above. The last part of the theorem is hence proved.

Conversely, let V be an equiprojectable k-variety. We show by induction on n that $\mathcal{J}(V)$ is a triangular ideal. For $n = 1$, the result follows from the fact that k is perfect. Let $n > 1$ and $d = c_{n-1}(V)$. The zero-dimensional ideal $I = \mathcal{J}(V_{n-1}) = \mathcal{J}(V) \cap k[x_1, \dots, x_{n-1}]$ admits a minimal primary decomposition

$$I = \mathcal{M}_1 \cap \cdots \cap \mathcal{M}_r,$$

where each $\mathcal{M}_j$ is maximal. Let $j \in [1, r]$ and $W_j = Z_{\bar{k}^{n-1}}(\mathcal{M}_j)$. By Proposition 4.4, the k-variety $\pi^{-1}_{n,n-1}(W_j)$ is equiprojectable and there exists a polynomial g_j, monic in x_n, such that $\deg(g_j, x_n) = d$ and

$$\mathcal{J}(\pi^{-1}_{n,n-1}(W_j)) = \mathbf{Id}(\mathcal{M}_j \cup \{g_j\}).$$

It follows from Lemma 3.3 that there exists $g \in k[x_1, \dots, x_n]$, monic in x_n, such that $\deg(g, x_n) = d$ and

$$\mathbf{Id}(I \cup \{g\}) = \cap_{j=1}^{r} \mathbf{Id}(\mathcal{M}_j \cup \{g_j\}) = \mathcal{J}(\cup_{j=1}^{r} \pi^{-1}_{n,n-1}(W_j)) = \mathcal{J}(V)$$

According to the induction hypothesis, I is triangular. Thus, $\mathcal{J}(V)$ is triangular since one verifies easily that $g(\beta_1, \dots, \beta_{n-1}, x_n)$ is separable for each $(\beta_1, \dots, \beta_{n-1})$ in V_{n-1}. □

5. Galois Ideals: a Fundamental Property

This section presents a major result. It is shown that, if a group of permutations L contains the Galois group of Ω (see Definition 2.3), then the Galois ideal I^L_Ω (see Definition 2.1) is triangular. This result may be used to simplify some problems in Galois theory and provides essential information for some implementation issues. The triangular structure of Galois ideals will be exploited in Section 7 to give a new algebraic algorithm for computing relative resolvents.

Notation 5.1. *Let L be a subgroup of Σ_n. For each $i \in [1, n]$ we denote by $L_{(i)}$ the stabilizer of $\{1, \dots, i\}$ under the natural action of L:*

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

Set $L_{(0)} = L$. We thus obtain the stabilizer chain

$$\{Id\} = L_{(n)} < L_{(n-1)} \cdots < L_{(1)} < L_{(0)} = L.$$

The left cosets of L modulo $L_{(i)}$ are the classes of the equivalence relation $\sim_i$, defined by $\tau \sim_i \tau'$ if and only if $\tau(k) = \tau'(k)$ for all k in $[1, i]$. The fact that each equivalence class in $L/\sim_i$ has cardinal $\operatorname{card}(L_{(i)})$, is the main feature of the proof of the following property for the orbits of Ω.

Proposition 5.2. *Let f be a separable polynomial of $k[X]$ and $\Omega = (\alpha_1, \dots, \alpha_n)$ a n-tuple of the roots of f with some fixed order. If L is a subgroup of Σ_n, then the orbit*

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

of Ω under the action of L is equiprojectable.

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

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

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

Since the points of V are all distinct, we have

$$\operatorname{card}(\pi_{n,i}^{-1}(M)) = \operatorname{card}(\{\sigma \in L \mid \sigma \sim_i \tau\}) = \operatorname{card}(L_{(i)}).\Box \qquad (5.1)$$

In general, the set V defined in Proposition 5.2 is not a variety over k. However, it is a k-variety when L contains the Galois group of f. In this case, Galois ideals have the following basic property.

Theorem 5.3. *Let Ω be an ordered set of roots of a separable univariate polynomial f, and G_Ω the Galois group of f. Let L be a subgroup of Σ_n which contains G_Ω. Then there exists a separable triangular set $T = \{f_1, \dots, f_n\}$ such that*

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

Moreover, the degree of each f_i in x_i is given by

$$\deg(f_i, x_i) = \operatorname{card}(L_{(i-1)}) / \operatorname{card}(L_{(i)}).$$

Proof. When L contains the Galois group of Ω, it is shown in Valibouze (1999) that $V(I_\Omega^L) = \{\sigma.\Omega \mid \sigma \in L\}$. This set is therefore a k-variety. Since $I_\Omega^L = \mathcal{J}(\{\sigma.\Omega \mid \sigma \in L\})$ (see Remark 2.5) the result follows immediately from Proposition 5.2 and Theorem 4.5. The degree of f_i in x_i is easily obtained from relations (5.1) and (4.2). □

The above result specifies the structure of Galois ideals. Therefore it may be exploited to develop and optimize algorithms in Galois theory. Knowledge of the degrees of the polynomials in T may also be useful for improving the efficiency of some techniques.

Remark 5.4. The above result is well known when L is the group Σ_n. Let us recall that $I_\Omega^{\Sigma_n}$ is generated by the separable triangular set $\{f_1,\ldots,f_n\}$ of *Cauchy moduli* of f, defined by induction as follows:

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

6. An Algorithm for Computing Characteristic Polynomials

In this section I is a radical zero-dimensional ideal of $k[x_1,\ldots,x_n]$ and Θ is a polynomial of $k[x_1,\ldots,x_n]$. The finite quotient algebra $k[x_1,\ldots,x_n]/I$ is denoted by A_I and the class of Θ in A_I is denoted by $\overline{\Theta}$. When I is a triangular ideal, there is a natural algorithm for computing the characteristic polynomial of the multiplication by $\overline{\Theta}$ in A_I. This algorithm is presented below and will be exploited with Galois ideals for computing relative resolvents (see Section 7).

Let us denote by $\hat{\Theta}$ the following endomorphism of the quotient ring A_I:

$$\begin{aligned} \hat{\Theta} : A_I &\longrightarrow A_I\\ P &\mapsto \overline{\Theta}.P \end{aligned}$$

and by $C_{\Theta,I}$ the characteristic polynomial of $\hat{\Theta}$. The coefficients of $C_{\Theta,I}$ lie in the field k like the entries of the matrix of the endomorphism $\hat{\Theta}$. Since I is a radical ideal, the classical theorem of Stickelberger implies that

$$C_{\Theta,I}(X) = \prod_{\beta\in V(I)} (X-\Theta(\beta)). \tag{6.1}$$

Let K be 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 p and q with respect to the variable x_i.

Theorem 6.1. *Let I be a triangular ideal of $k[x_1,\ldots,x_n]$ generated by a separable triangular set $T=\{f_1,\ldots,f_n\}$.*

(1) If $\Psi\in K[x_1,\ldots,x_n]$ and $\Psi_0,\Psi_1,\ldots,\Psi_n$ are defined inductively as follows:

$$\begin{aligned} \Psi_n &= \Psi\in K[x_1,\ldots,x_n],\\ \Psi_{i-1} &= \mathrm{Res}_{x_i}(f_i(x_1,\ldots,x_i),\Psi_i(x_1,\ldots,x_i))\in K[x_1,\ldots,x_{i-1}], \end{aligned}$$

then the element Ψ_0 of K is given by $\Psi_0=\prod_{\beta\in V(T)}\Psi(\beta)$.

(2) If $\Theta\in k[x_1,\ldots,x_n]$ then the characteristic polynomial $C_{\Theta,I}(X)$ of $k[X]$ is computable by the algorithm CharPol(T,Θ) *below.*

```
CharPol($T,\Theta$):
    $\Psi := X-\Theta$
    for $i$ from $n$ to 1 repeat
        $f :=$ the only polynomial in $T$ with greatest variable $x_i$
        $\Psi := \mathrm{Res}_{x_i}(f,\Psi)$
    output($\Psi$)
```

Proof. (1) 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 $j \in [1, n]$

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

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

$$\Psi_0 = \prod_{\{\beta_1,\ldots,\beta_{i-1}\} \in V_{i-1}} \Psi_{i-1}(\beta_1, \ldots, \beta_{i-1}). \tag{6.2}$$

By the definition of Ψ_{i-1}, the identity (6.2) becomes

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

The result follows from Remark 2.8 and the fact that, by assumption, $f_i(\beta_1, \ldots, \beta_{i-1}, x_i)$ is monic and separable in $\bar{k}[x_i]$.

(2) Since I is radical (Remark 2.5), Relation (6.1) applies and $C_{\Theta,I}(X)$ is given by Ψ_0 in the first part of this theorem for $\Psi = (X - \Theta)$. □

7. Algebraic Computation of Relative Resolvents

Let L be a subgroup of Σ_n which contains the Galois group of Ω (see Definition 2.3). In this section we define the L-relative resolvent by a polynomial Θ, and specify the obvious connection with the characteristic polynomial C_{Θ,I_Ω^L}. We deduce an algorithm for computing relative resolvents from the algorithm of Section 6.

The idea underlying our algorithm appears in Rennert and Valibouze (1999) for the algebraic computation of absolute resolvents. Indeed it is based on the triangular structure of the Cauchy moduli. Here we show that a similar method may be devised for computing relative resolvents, and that the efficient improvements presented in Lehobey (1997) and Rennert and Valibouze (1999) for absolute resolvents are also available for our algorithm. The crucial point is that the ideal I_Ω^L is triangular.

Our algorithm depends on the computation of triangular sets of generators of Galois ideals. But we show that, reciprocally, it is possible to obtain these triangular sets by using our algorithm (Theorem 7.10 and Remark 7.11). Thus, we also present an algorithm, which is based on a recent result from Valibouze (1999) (Lemma 7.8), for computing the generators of Galois ideals. With these algorithms, it is possible to obtain a Gröbner basis of the ideal of relations and then compute in the splitting field of f.

7.1. resolvent and characteristic polynomial

Henceforth we denote the Galois group of the polynomial f by G_Ω.

Definition 7.1. Let $\Theta \in k[x_1, \ldots, x_n]$ and L a subgroup of Σ_n which contains G_Ω. 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 $L = \Sigma_n$, the resolvent $\mathcal{L}_{\Theta,I_\Omega^{\Sigma_n}}$ is called the *absolute resolvent* of f by Θ.

Remark 7.2. In the literature the polynomial $\mathcal{L}_{\Theta,I_\Omega^L}$ is usually called an L-relative resolvent of f by Θ. The fact that the coefficients of $\mathcal{L}_{\Theta,I_\Omega^L}$ lie in k follows easily from Galois theory.

Definition 7.3. 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

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

It is said to be *separable* if $H = \{\sigma \in L \mid \sigma.\Theta(\Omega) = \Theta(\Omega)\}$.

The following results are well known.

Lemma 7.4. *Let L and H be two subgroups of Σ_n such that $G_\Omega < L$ and $H < L$. Let Θ be an L-primitive H-invariant and $d = \mathrm{card}(H)$. Then the degree of $\mathcal{L}_{\Theta,I_\Omega^L}(X)$ is the index of H in L and*

$$C_{\Theta,I_\Omega^L} = (\mathcal{L}_{\Theta,I_\Omega^L})^d. \tag{7.1}$$

Since k is a perfect field, the above lemma gives another proof that the coefficients of the L-relative resolvent of Ω by Θ belong to k and when this resolvent is separable, it is exactly the minimal polynomial of the endomorphism $\hat{\Theta}$.

7.2. some algorithms

Since the characteristic polynomial is a power of the resolvent, it is possible to obtain a resolvent from a characteristic polynomial by nth root computation. Let p be a monic polynomial in $k[X]$ and $q = p^d$, where d is an integer. Let us call $\mathsf{nthRoot}(q, d)$ a function which returns the polynomial p; it is based on the work of Henrici (1956) and Lehobey (1997). In view of the fact that the Galois ideals considered are triangular, a theoretical algorithm for computing relative resolvents is easily obtained from the algorithm CharPol of Section 6. It gives the main idea for the computation of L-relative resolvents but practically, thanks to the optimizations described in Remark 7.6, we do not need to compute the characteristic polynomial itself.

Theorem 7.5. *Let L be a subgroup of Σ_n such that $G_\Omega < L$, let $T_L = \{f_1,\dots,f_n\}$ be a separable triangular set which generates the ideal I_Ω^L, let H be a subgroup of L and Θ an L-primitive H-invariant. Then the algorithm* $\mathsf{Resolvent}(L, T_L, H, \Theta)$ *presented below computes the L-relative resolvent $\mathcal{L}_{\Theta,I_\Omega^L}$ of Ω by Θ.*

```
Resolvent($L, T_L, H, \Theta$):
    $d := \mathrm{card}(H)$
    $C :=$ CharPol($T_L, \Theta$)
    output(nthRoot($C, d$))
```

Proof. Use Theorem 6.1 and formula (7.1). □

Remark 7.6. For an efficient implementation, the extraneous power d is eliminated during the successive computations of resultants described in the algorithm charPol. This is realized by a direct extension of the results in Lehobey (1997).

Another drawback is the growth of the number of terms. The computation may be performed modulo the ideal I_Ω^L as described in Rennert and Valibouze (1999) for the particular case where $L = \Sigma_n$. Thus the growth of coefficients is controlled and some variables may be eliminated before the computation of the corresponding resultant. But the following degenerate case may occur in the computation modulo the ideal I_Ω^L: the resolvent is not the result of the computation but a power of the result (see Section 6 in Rennert and Valibouze, 1999); however, since its degree is known, the resolvent is immediately obtained from the result of the computation as illustrated in Example 7.13 of Section 7.

A detailed review of these techniques cannot be given here; their adaptation consists mainly of replacing the Cauchy moduli by a triangular set which generates I_Ω^L in the proofs of the original papers mentioned above.

Remark 7.7. By computing a lexicographical Gröbner basis of $I_\Omega^L + \mathbf{Id}(X - \Theta)$ $(X < x_1 < \cdots < x_n)$, one can obtain the minimal polynomial of $\Theta(\Omega)$ and therefore, the factors of the resolvent. Since we already have a Gröbner basis of I_Ω^L, this computation involves only the normal forms and S-polynomials related to the polynomial $X - \Theta$, but it is better to perform successive resultants by reducing after each step. For instance, the computation of the resolvent in Example 7.12 is performed in 0.1 s by our method instead of 0.6 s by computing a Gröbner basis with Magma. Besides, for rational polynomials, it would not be difficult most of the time to construct the resolvent from its roots by using p-adic or numeric approximations of the roots of f.

For practical computation of the resolvent, we need the triangular set T_L. Of course it suffices to know any system of generators of the ideal I_Ω^L in order to obtain T_L by a Gröbner basis computation. The following lemma is of prime importance for computing a system of generators of I_Ω^L.

Lemma 7.8. *Let M and L be two subgroups of Σ_n such that $G_\Omega < M$ and $G_\Omega L$ is a group. Let Θ be an M-primitive L-invariant with $\theta = \Theta(\Omega)$ and $\min_{\theta,k}$ be the minimal polynomial of θ over k. If θ is a simple root of the resolvent $\mathcal{L}_{\Theta,I_\Omega^M}$, then*

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

Proof. See Valibouze (1999). □

The requirement that θ must be a simple root of the resolvent in Lemma 7.8 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 (Arnaudiès and Valibouze, 1996, Theorem 6); such an invariant may be obtained by a Tschirnhausen transformation after a finite number of tests as explained in (Colin, 1995, Section 3.3).

From now on, we assume that k is infinite. Thus, separable invariants may always be computed. Let $\mathsf{Groebner}(PS)$ denote a function that computes a reduced lexicographical Gröbner basis of the ideal generated by a finite subset PS of $k[x_1, \ldots, x_n]$. The triangular Galois ideals may be obtained by computing relative resolvents.

Theorem 7.9. *Let M and L be two subgroups of Σ_n such that $G_\Omega < L < M$ and let T_M*

be a separable triangular set of generators of the Galois ideal I_Ω^M. Then the algorithm TriangSet(L, M, T_M) *given below computes a separable triangular set of generators of I_Ω^L.*

```
TriangSet$(L, M, T_M)$:
    $\Theta :=$ an $M$-primitive $L$-invariant separable for $\Omega$
    $\mathcal{L} :=$ Resolvent$(M, T_M, L, \Theta)$
    factorize $\mathcal{L}$
    $\theta :=$ the root of a linear factor of $\mathcal{L}$
    output(Groebner$(T_M \cup \{\Theta - \theta\})$)
```

Proof. Let $\theta = \Theta(\Omega)$. The polynomial Θ is invariant by the Galois group of Ω since Θ is an M-primitive L-invariant, therefore we have $\theta \in k$ and $\min_{\theta,k} = X - \theta$. On the other hand θ is a simple root of the resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$. It follows that the value of θ is provided by the factorization of L. Finally, the output is a reduced lexicographical Gröbner basis of I_Ω^L by Lemma 7.8. It is a triangular set by Theorem 5.3 and Remark 2.8. □

With the notation of Theorem 7.9, we can always choose Σ_n for M and the Cauchy moduli of f for T_M. Hence the Galois ideal I_Ω^L is always computable by the algorithm TriangSet. The following theorem is deduced.

Theorem 7.10. *Let L be a subgroup of Σ_n which contains G_Ω, and let H be a subgroup of L and Θ an L-primitive H-invariant. Then the relative resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$ may be computed by the algorithm* RelativeResolvent(L, H, Θ) *below.*

```
RelativeResolvent$(L, H, \Theta)$:
    $T :=$ the Cauchy moduli of $f$ (see Remark 5.4)
    $T_L :=$ TriangSet$(L, \Sigma_n, T)$
    output(Resolvent$(L, T_L, H, \Theta)$)
```

Remark 7.11. To avoid computing resolvents of high degrees, the computation of $\mathcal{L}_{\Theta, I_\Omega^L}$ (and of I_Ω^L) can be performed in several steps with intermediate computations of relative resolvents and Galois ideals. Let $L = L_e < \cdots < L_0 = \Sigma_n$ be a chain of subgroups of Σ_n with $G_\Omega < L$. For each $j \in [0, e]$ we denote by T_j the triangular set that generates L_j. By repeating the algorithm TriangSet(L_{j+1}, L_j, T_j) for j in $[0, e-1]$, we obtain $T_L = T_e$; then the algorithm Resolvent(L, T_L, H, Θ) computes the relative resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$. Note that if $L = G_\Omega$, the last triangular set T_e computed by the algorithm TriangSet generates the ideal of relations I_Ω.

Our algorithm is convenient for the computation of relative resolvents which are involved in the incremental method presented in Valibouze (1999) for computing the Galois group and the ideal of relations of a polynomial f. It may also be easily inserted in a method for computing Galois groups by using partition and group matrices (Valibouze, 1995).

The complexity of the computation of a relative resolvent $\mathcal{L}_{\Theta, I_\Omega^L}$ by our method depends on the order of L and the parity of Θ (the number of indeterminates occurring in Θ). Thus, the computation becomes easier for smaller groups. Some experiments on the worst case corresponding to $L = \Sigma_n$, are related in Rennert and Valibouze (1999, Section 9), which gives the timings for computing several resolvents associated with the polynomials $x^6 - 243x^2 + 729$ and $x^7 + 8x^6 - 5x^4 - 18x^2 + x - 1$.

7.3. examples

The two examples presented below illustrate the algorithms of Section 7. In these examples we consider the polynomial $f = x^8 + x^4 + 2$, irreducible over $\mathbb{Q}$, whose Galois group is a transitive subgroup of Σ_8.

Our algorithm for computing relative resolvents has been implemented by N. Rennert in the aldor language. We have used the PrimitiveInvariant package for GAP (Abdeljaouad, 1999) to compute invariants and the very powerful Gröbner engine FGb (Faugère, 1999) to obtain our Gröbner bases. The computations were performed with a 233 MHz Pentium II processor running under Red Hat Linux 5.2.

Below we use the names of the groups given in Butler and McKay (1983) and denote the generators of I_Ω^L by $\mathcal{T}_L$ to avoid confusions with the notation of the groups.

Example 7.12. Let $L = T_{47}$ be the transitive maximal subgroup of Σ_8 of order 1152 and H the group T_{35} of order 128. We have $H < L$. The polynomial

$$\Theta_1 = x_8\, x_7 + x_6\, x_5 + x_4\, x_3 + x_2\, x_1$$

is a T_{47}-primitive T_{35}-invariant. We want to compute the T_{47}-relative resolvent of f by Θ_1, which has degree $9 = [L : H]$.

First, we need the triangular set of generators $\mathcal{T}_L$ of I_Ω^L. We denote by Θ_L the polynomial $x_1\, x_2\, x_3\, x_4 + x_5\, x_6\, x_7\, x_8$ which is a primitive L-invariant. The Cauchy moduli are immediately obtained from the polynomial f and the computation of the separable absolute resolvent of f by Θ_L, by a method specific to this invariant and implemented in the module SYM of MACSYMA (Valibouze, 1989b), gives the following factorization over $\mathbb{Q}$:

$$\mathcal{L}_{\Theta_L, I_f^{\Sigma_8}}(X) = X^8\ (X-1)\ (X^2-8)^5\ (X^4 - 8\,X^2 + 14)^4.$$

The simple linear factor $(X - 1)$ proves that $G_\Omega < L$. As specified in our algorithm, we deduce that I_Ω^L is generated by the union of the ideal $I_\Omega^{\Sigma_8}$ and the ideal $\langle \Theta_L - 1\rangle$. The computation of the reduced Gröbner basis for the lexicographical ordering of I_Ω^L provides the following triangular set in 0.3 s:

$$\begin{aligned} I_\Omega^L = \langle & x_1^8 + x_1^4 + 2,\ x_2^3 + x_2^2\, x_1 + x_2\, x_1^2 + x_1^3, \\ & x_3^2 + x_3\, x_2 + x_3\, x_1 + x_2^2 + x_2\, x_1 + x_1^2, \\ & x_4 + x_3 + x_2 + x_1,\ x_5^4 + x_1^4 + 1,\ x_6^3 + x_6^2\, x_5 + x_6\, x_5^2 + x_5^3, \\ & x_7^2 + x_7\, x_6 + x_7\, x_5 + x_6^2 + x_6\, x_5 + x_5^2,\ x_8 + x_7 + x_6 + x_5\rangle. \end{aligned}$$

Now, it is possible to compute the L-relative resolvent by Θ_1 using the algorithm $\mathsf{Resolvent}(L, \mathcal{T}_L, H, \Theta_1)$. As explained in Remark 7.6, its computation is performed modulo the ideal I_Ω^L as follows:

- Let $R_0(X, x_1, \ldots, x_8) = X - \Theta_1$. We denote by $\mathsf{div}(a, b, x)$ the Euclidean division of a by b with respect to the variable x. The reduction of R_0 modulo the ideal I_Ω^L, given by $\mathsf{div}(\ldots, \mathsf{div}(\mathsf{div}(R_0, f_8, x_8), f_7, x7), \ldots, f_1, x_1)$, eliminates the variables x_8

and x_7. The result of this reduction is

$$W_0(X, x_1, \dots, x_6) = x_6^2 + 2x_5x_6 + x_5^2 + x_2^2 + 2x_1x_2 + x_1^2 - X.$$

- We set $R_1(X, x_1, \dots, x_5) = \mathrm{Res}_{x_6}(f_6, W_0)$. The reduction of R_1 modulo the ideal I_Ω^L eliminates the variables x_3 and x_4 and produces a polynomial $W_1(X, x_1, x_2)$.
- The elimination of the variable x_2 is given by $R_2(X, x_1) = \mathrm{Res}_{x_2}(f_2, W_1)$ which has degree 16 in x_1. The reduction of R_2 modulo the ideal I_Ω^L produces a univariate polynomial of degree 9 in X. No extraneous power appears in this computation since the T_{47}-relative resolvent of Ω by Θ_1 has degree $9 = [L : H]$. Hence the function nthRoot has not been used during this process. The obtained result is the resolvent and its factorization is the following:

$$\mathcal{L}_{\Theta_1, I_\Omega^{T_{47}}} = X\,(X^8 - 12\,X^6 - 48\,X^4 + 192\,X^2 - 3584).$$

This computation is performed within 0.1 s.

Example 7.13. Denote by Θ_2 the following T_{35}-primitive T_{26}-invariant:

$$\begin{aligned}\Theta_2 = {} & x_2\,x_6\,x_4^2\,x_8^2 + x_4\,x_8\,x_2^2\,x_6^2 + x_2\,x_7\,x_4^2\,x_6^2 + x_4\,x_6\,x_2^2\,x_7^2 + x_2\,x_8\,x_4^2\,x_5^2 + x_4\,x_5\,x_2^2\,x_8^2 \\ & + x_2\,x_5\,x_4^2\,x_7^2 + x_4\,x_7\,x_2^2\,x_5^2 + x_2\,x_8\,x_3^2\,x_6^2 + x_3\,x_6\,x_2^2\,x_8^2 + x_2\,x_6\,x_3^2\,x_7^2 + x_3\,x_7\,x_2^2\,x_6^2 \\ & + x_2\,x_5\,x_3^2\,x_8^2 + x_3\,x_8\,x_2^2\,x_5^2 + x_2\,x_7\,x_3^2\,x_5^2 + x_3\,x_5\,x_2^2\,x_7^2 + x_1\,x_8\,x_4^2\,x_6^2 + x_4\,x_6\,x_1^2\,x_8^2 \\ & + x_1\,x_6\,x_4^2\,x_7^2 + x_4\,x_7\,x_1^2\,x_6^2 + x_1\,x_5\,x_4^2\,x_8^2 + x_4\,x_8\,x_1^2\,x_5^2 + x_1\,x_7\,x_4^2\,x_5^2 + x_4\,x_5\,x_1^2\,x_7^2 \\ & + x_1\,x_6\,x_3^2\,x_8^2 + x_3\,x_8\,x_1^2\,x_6^2 + x_1\,x_7\,x_3^2\,x_6^2 + x_3\,x_6\,x_1^2\,x_7^2 + x_1\,x_8\,x_3^2\,x_5^2 + x_3\,x_5\,x_1^2\,x_8^2 \\ & + x_1\,x_5\,x_3^2\,x_7^2 + x_3\,x_7\,x_1^2\,x_5^2.\end{aligned}$$

We compute below the T_{35}-relative resolvent of f by Θ_2 which has degree $2 = [T_{35} : T_{26}]$.

We remark that the factorization of $\mathcal{L}_{\Theta_1, I_\Omega^L}$, given in Example 7.12, provides a simple linear factor over $\mathbb{Q}$. This implies that T_{35} contains actually the Galois group G_Ω.

The first step consists in computing the Galois ideal $I_\Omega^{T_{35}}$. It can be efficiently performed with the algorithm TriangSet$(T_{35}, T_L, \mathcal{T}_L)$ instead of using Σ_8 and the Cauchy moduli of f.

We only need to compute a Gröbner basis if the resolvent in Example 7.12 and its factorization are used. The ideal fixed by T_{35} is given by

$$I_\Omega^{T_{35}} = I_\Omega^L + \mathbf{Id}(\Theta_1 - 0),$$

where 0 is the value given by the simple linear factor over $\mathbb{Q}$ of the resolvent $\mathcal{L}_{\Theta_1, I_\Omega^L}$.

In the same way as for the ideal fixed by L, we compute in 0.1 s, from Θ_1 and the polynomials of $\mathcal{T}_L$, the following triangular Gröbner basis of the Galois ideal $I_\Omega^{T_{35}}$:

$$\begin{aligned}I_\Omega^{T_{35}} = \langle & x_1^8 + x_1^4 + 2, x_2 + x_1, x_3^2 + x_1^2, x_4 + x_3, \\ & x_5^4 + x_1^4 + 1, x_6 + x_5, x_7^2 + x_5^2, x_8 + x_7\rangle.\end{aligned}$$

We then perform the computation of Resolvent$(T_{35}, T_{26}, \mathcal{T}_{T_{35}}, \Theta_2)$ modulo the ideal $I_\Omega^{T_{35}}$. The reduction of Θ_2 modulo the ideal $I_\Omega^{T_{35}}$ produces the value 0. Therefore the result of our computation is the polynomial X. But the degree of the T_{26}-relative resolvent is 2, the index of T_{26} in T_{35}. We are in the degenerate case mentioned in Remark 7.6, where the resolvent is a power of the result of the computation. Thus we obtain immediately

$$\mathcal{L}_{\Theta_2, I_\Omega^{T_{35}}}(X) = X^2.$$

8. Conclusion

We have given some information on the algebraic structure of the ideals of relations invariant under a subgroup of Σ_n. The algorithm for computing relative resolvents presented in Section 7 avoids the first step of hard generic computations needed in the method of Colin (1995). It is not as efficient as modular techniques based on approximations of the roots (Yokoyama, 1996; Geissler and Klüners, 2000) involved in the computation of the Galois group of rational polynomials, but it is independent of the coefficient ring and some ill-conditions which may appear in p-adic approach.

Acknowledgements

We would like to thank the referees for their many helpful suggestions.

References

Abdeljaouad, I. (1999). Calcul d'invariants primitifs de groupes finis. *RAIRO—Inform. Théor. Programm.*, **33**, 59–77.

Arnaudiès, J., Valibouze, A. (1996). Lagrange resolvents. In Cohen, A., Roy, M. eds, *Special Issue of MEGA'96*, *J. Pure Appl. Algebra*, **117 & 118**, 23–40.

Aubry, P. (1999). Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Ph.D. Thesis, Université Paris 6.

Aubry, P., Moreno Maza, M (1999). Triangular sets for solving polynomial systems: a comparative implementation of four methods. *J. Symb. Comput.*, **28**, 125–154.

Becker, T., Weispfenning, V. (1993). *Gröbner Bases,* volume 141 of Graduate Texts in Mathematics. New York, Springer-Verlag.

Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. Thesis, Universität Innsbruck.

Butler, G., McKay, J. (1983). The transitive groups of degree up to 11. *Commun. Algebra*, **11**, 863–911.

Casperson, D., McKay, J. (1994). Symmetric functions, m-sets, and Galois groups. *Math. Comput.*, **63**, 749–757.

Colin, A. (1989). Formal computation of Galois groups with relative resolvents. In Cohen, G., Giusti, M., Mora, T. eds, *Proceedings of AAECC'11, Paris, July 1995*, LNCS **948**, pp. 169–182. Berlin, Springer-Verlag.

Darmon, H., Ford, D. (1989). Computational verification of M_{11} and M_{12} as Galois groups over $\mathbb{Q}$. *Commun. Algebra*, **17**, 2941–2943.

Eichenlaub, Y. (1996). Problèmes effectifs de théorie de Galois en degrés 8 à 11. Ph.D. Thesis, Université de Bordeaux 1.

Faugère, J. (1999). A new efficient algorithm for computing Gröbner bases (F4). *J. Pure Appl. Algebra*, **139**, 61–88.

Geissler, K., Klüners, J. (2000). Galois group computation for rational polynomials. *J. Symb. Comput*, **30**, 653–674, doi:10.1006/jsco.2000.0377.

Henrici, P. (1956). Automatic computations with power series. *J. Assoc. Comput. Mach.*, **3**, 10–15.

Lagrange, J. (1770). Réflexions sur la résolution algébrique des équations. Mémoires de l'Académie de Berlin.

Lazard, D. (1991). Systems of algebraic equations (algorithms and complexity). In Eisenbud, D., Robbiano, L. eds, *Cortona Proceedings.* Cambridge, Cambridge University Press.

Lazard, D. (1992). Solving zero-dimensional algebraic systems. *J. Symb. Comput.*, **15**, 117–132.

Lehobey, F. (1997). Resolvent computations by resultants without extraneous powers. In Küchlin, W. ed., *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, pp. 85–92. New York, ACM Press.

Rennert, N., Valibouze, A. (1999). Calcul de résolvantes avec les modules de Cauchy. *Exp. Math.*, **8**, 351–366.

Soicher, L. (1981). The computations of Galois groups. Ph.D. Thesis, Concordia University, Montreal.

Soicher, L., McKay, J. (1985). Computing Galois groups over the rationals. *J. Number Theory*, **20**, 273–281.

Stauduhar, R. (1973). The determination of Galois groups. *Math. Comput.*, **27**, 981–996.

Valibouze, A. (1989a). Résolvantes et fonctions symétriques. In *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation*, pp. 390–399. New York, ACM Press.

Valibouze, A. (1989b). Sym, symbolic computation with symmetric polynomials: an extension to macsyma. In Kalthofen, E., Watt, S. M. eds, *Proceedings of Computers and Mathematics (Cambridge, Massachussetts, 1989)*, New York, Springer-Verlag.

Valibouze, A. (1995). Computation of the Galois group of the resolvent factors for the direct and inverse Galois problems. In Cohen, G., Giusti, M., Mora, T. eds, *Proceedings of AAECC'11, Paris, July 1995*, LNCS **948**, pp. 456–468. Berlin, Springer-Verlag.

Valibouze, A. (1999). Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bull. Belgian Math. Soc. Simon Stevin*, **6**, 507–535.

Yokoyama, K. (1996). A modular method for computing the Galois groups of polynomials. In Cohen, A., Roy, M. eds, *Special Issue of MEGA'96*, *J. Pure Appl. Algebra*, **117 & 118**, 617–636

Zariski, O., Samuel, P. (1967). *Commutative Algebra*, volume I. van Nostrand.

Originally Received 1 October 1999
Accepted 17 April 2000