# Computation of the Splitting Field of a Dihedral Polynomial

Guénaël Renault

# Computation of the Splitting Field of a Dihedral Polynomial*

Guénaël Renault
LIP6 - Université Pierre et Marie Curie
4, place Jussieu
75005 Paris
France
Guenael.Renault@calfor.lip6.fr

## ABSTRACT

Let $g$ be a univariate separable polynomial of degree $n$ with coefficients in a computable field $\mathbb{K}$ and let $(\alpha_1, \ldots, \alpha_n)$ be an $n$-tuple of its roots in an algebraic closure $\bar{\mathbb{K}}$ of $\mathbb{K}$. Obtaining an algebraic representation of the splitting field $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$ of $g$ is a question of first importance in effective Galois theory. For instance, it allows to manipulate symbolically the roots of $g$. In this paper, we focus on the computation of the splitting field of $g$ when its Galois group is a dihedral group. We provide an algorithm for this task which returns a triangular set encoding the relations ideal of $g$ which has a degree $2n$ since the Galois group of $g$ is dihedral. Our algorithm starts from a factorization of $g$ in $\mathbb{K}[X]/\langle g \rangle$ and constructs the searched triangular set by performing $n^2$ computations of normal forms modulo an ideal of degree $2n$.

## Categories and Subject Descriptors

I.1 [**Computing Methodologies**]: Symbolic and algebraic manipulations

## General Terms

Algorithm, Theory

## Keywords

Galois theory, triangular set, splitting field, dihedral group

## 1. INTRODUCTION

The computation of the splitting field of a polynomial plays an important role in Galois theory and more generally in algebra. It is the smallest field where all the roots of the polynomial lie. Computing a suitable representation of this field allows us to manipulate all the roots of the polynomial. Let $g$ be a polynomial of degree $n$ with coefficients in a computable field $\mathbb{K}$ and whose Galois group is dihedral, which implies that it is irreducible and separable. We are interested here with the computation of the splitting field of $g$ and the representation of the action of the Galois group over the roots of $g$. Our aim is to exploit the knowledge on the Galois group of $g$.

The splitting field of $g$ can be represented as a simple extension of the base field but, since here we want to compute with all the roots of $g$ it is better to considerate another representation. The natural representation for this task is the following quotient algebra

$$\mathbb{K}(\alpha_1, \ldots, \alpha_n) \simeq \mathbb{K}[x_1, \ldots, x_n]/I$$

where $I$ is the kernel of the surjective morphism from $\mathbb{K}[x_1, \ldots, x_n]$ to $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$ which maps $x_i$ to $\alpha_i$. The ideal $I$ is called a *relations ideal* of $g$. Remark that $I$ is zero-dimensional and maximal. A Gröbner basis of $I$ allows computations in this quotient algebra by means of linear algebra operations (see e.g. [7, 5]) and then to make symbolic operations with the roots of $g$.

When $n = 5$ and $\mathbb{K} = \mathbb{Q}$, Spearman and Williams give in [21] a first solution to this problem: they provide closed formulæ which express all the roots of $g$ as rational functions of any two roots $\alpha_1$, $\alpha_2$. Thus, if we have a radical representation of $\alpha_1$ and $\alpha_2$, we have the ones for all the other roots. But, when $n \geqslant 6$, the result of Spearman an Williams is not generalized. Moreover, the radical representation of the roots is not suitable for symbolic computation (see [15, Section 9]) when $n \geqslant 6$. Thus, we focus on the computation of the representation of the splitting field of $g$ with the above representation.

It is well known that the ideal $I$ has a *triangular* reduced Gröbner basis for a lexicographical order (see e.g. [22, 14, 2, 24, 4]). This Gröbner basis can be obtained from the polynomial $g$ by computing successive factorizations in algebraic extensions of $\mathbb{K}$ (see e.g. [2]). Another method for this task is based on computations and factorizations of resolvents (see e.g. [24, 10]). When such a triangular basis is known, we can compute the symmetric representation of the action of the Galois of $g$ over $\alpha_1, \ldots, \alpha_n$ (see [2, 1]). None of the aforementioned methods take advantage of the fact that the Galois group of the studied polynomial is dihedral.

In this paper, we focus on the computation of this triangular Gröbner basis. In our specific case, this triangular set

*

$\{f_1, f_2, f_3, \ldots, f_n\}$ verifies a theorem of Galois which states that polynomials $f_3, \ldots, f_n$ are linear in their principal variable. Thus, as soon as we know an irreducible factor $g_2$ of $g$ over its stem field (an extension of $\mathbb{K}$ generated by one of its roots) we can take $f_1 = f$ and $f_2 = g_2$, then it rests to compute the polynomials $f_3, \ldots, f_n$. If we know the action of the Galois group of $g$ over approximations (complex or $p$-adic) of its roots we can compute these relations by interpolation (see [16, 25, 20]). Here, we do not assume the knowledge of the explicit action of the Galois over approximations (we only know the name of the group) so we cannot use these methods.

An other framework for the computation of such a basis is presented in [17]: the main idea is to begin the process by a factorization of $g$ over its stem field and to end the algorithm by computations using the algorithm `GaloisIdeal` (see [24]) with a tricky use of the galoisian informations obtained from the factorization in order to avoid some computations. This framework describes a method for the construction of a table-based algorithm for the computation of relations ideal of polynomial with a fixed degree.

The algorithm we provide here starts also from a factorization of $g$ over its stem field but, it does not depend neither on the degree of $g$ and nor on the field of its coefficients. We prove that the knowledge on the fact that the Galois group of $g$ is dihedral allows to reduce the end of the process to computations of normal forms modulo an ideal of degree $2n$ obtained from the pre-process of factorization. We also prove that the number of normal forms computed by our algorithm is dominated by $n^2$, and that they are computed modulo a zero-dimensional ideal of degree bounded by $2n$.

In the particular case of degree $n = 5$, we prove that this basis can be given from the factorization of $g$ over its stem field without any other computation of normal forms. This can be viewed as an improvement of the result of [21].

The paper is organized as follows. In section 2, we present results about Galois ideals relating them to triangular sets. These results are used in Section 3 which is devoted to the proof of the principal results leading to the algorithm and its complexity study. Section 4 presents two examples of use of this algorithm.

### Notations

In this paper, the following notations are used:

- $\mathbb{K}$ is a computable field and $\bar{\mathbb{K}}$ is an algebraic closure of $\mathbb{K}$.
- For $i \in [\![1, n]\!]$, the multivariate polynomials ring $\mathbb{K}[x_1, \ldots, x_i]$ is denoted by $\mathbb{K}[\underline{X}_i]$.
- For $i \in [\![2, n]\!]$, $\mathbb{K}[\underline{X}_i]$ is equipped with the lexicographical monomial order $x_1 < x_2 < \ldots < x_i$. For $f \in \mathbb{K}[\underline{X}_i]$, we denote by $\mathrm{HM}(f)$ the greatest monomial of $f$.
- Given an ideal $I$ of $\mathbb{K}[\underline{X}_n]$, the set of zeroes of $I$ in $\bar{\mathbb{K}}^n$ is denoted by $\mathcal{Z}(I)$. For $i \in [\![1, n-1]\!]$, we denote by $\mathcal{Z}(I)_i$ the projection of $\mathcal{Z}(I)$ on the first $i$ coordinates.
- Given $V$ a finite subset of $\bar{\mathbb{K}}^n$, the unique radical ideal of $\mathbb{K}[\underline{X}_n]$ vanishing on $V$ is denoted by $\mathcal{I}(V)$.
- The natural actions of the symmetric group $\mathfrak{S}_n$ over elements of $\bar{\mathbb{K}}^n$ and $\mathbb{K}[x_1, \ldots, x_n]$ are defined by

$$\begin{array}{rcl} \mathfrak{S}_n \times \bar{\mathbb{K}}^n & \longrightarrow & \bar{\mathbb{K}}^n \\ (\sigma, \underline{\alpha}) & \longrightarrow & \sigma.\underline{\alpha} = (\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) \end{array}$$

$$\begin{array}{rcl} \mathfrak{S}_n \times \mathbb{K}[\underline{X}_n] & \longrightarrow & \mathbb{K}[\underline{X}_n] \\ (\sigma, f) & \longrightarrow & \sigma.f = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \end{array}$$

- $D_n$ denotes the symmetric representation of the dihedral subgroup of degree $n$ of $\mathfrak{S}_n$. In the case where $n$ is odd, it is generated by the product of transpositions

$$\tau = (2, 3) \ldots (n-1, n)$$

and the cycle

$$\sigma = (1, 2, 4 \ldots, 2k, \ldots, n-1, n, \ldots, 2k-1, \ldots, 5, 3).$$

When $n$ is even,

$$\tau = (2, 3) \ldots (n-2, n-1)$$

and

$$\sigma = (1, 2, 4 \ldots, 2k, \ldots, n, n-1, \ldots, 2k-1, \ldots, 5, 3).$$

For example, when $n = 5$ (resp. $n = 8$) we have $\tau = (2,3)(4,5)$ (resp. $\tau = (2,3)(4,5)(6,7)$) and $\sigma = (1,2,4,5,3)$ (resp. $\sigma = (1,2,4,6,8,7,5,3)$).

## 2. GALOIS IDEALS

In this section, we recall the definition and give some results about Galois ideals (see [24, 4]).
In the whole section, $g$ is a separable polynomial of degree $n$ with coefficients in $\mathbb{K}$ and $\underline{\alpha} = \{\alpha_1, \ldots, \alpha_n\}$ an $n$-tuple of its roots in $\bar{\mathbb{K}}$.

*Definition 1.* An ideal $I$ of $\mathbb{K}[\underline{X}_n]$ is a *Galois $\underline{\alpha}$-ideal* if there exists a subset $L$ of the symmetric group $\mathfrak{S}_n$ containing the identity such that:

$$I = \mathcal{I}(L.\underline{\alpha}).$$

More generally an ideal $I$ of $\mathbb{K}[\underline{X}_n]$ is said to be a *Galois ideal* if there exists a tuple $\underline{\beta}$ of roots of a separable polynomial of degree $n$ such that $I$ is a Galois $\underline{\beta}$-ideal.

Example 2. *The Galois ideal $I(\{\underline{\alpha}\})$ is called a relations ideal and is denoted by $I(\underline{\alpha})$. Since $\mathbb{K}[\underline{X}_n]/I(\underline{\alpha})$ is isomorphic to the splitting field of $g$, $I(\underline{\alpha})$ is maximal [24, 2]. In fact, it is the unique maximal Galois $\underline{\alpha}$-ideal. More generally, all maximal ideals of $\mathbb{K}[\underline{X}_n]$ which contain a Galois ideal are relations ideals (see [24]).*

We have the following obvious characterization of a Galois $\underline{\alpha}$-ideal:

LEMMA 2.1. *[4] An ideal $I$ of $\mathbb{K}[\underline{X}_n]$ is a Galois $\underline{\alpha}$-ideal if and only if $I$ is radical and its associated algebraic variety $\mathcal{Z}(I)$ satisfies*

$$\{\underline{\alpha}\} \subset \mathcal{Z}(I) \subset \mathfrak{S}_n.\underline{\alpha}\,.$$

The Galois group of $g$, for a fixed numbering of its roots, is now defined from a Galois ideal.

PROPOSITION-DEFINITION 3. *[24, Définition 1.12] There exists a subgroup $G$ of $\mathfrak{S}_n$ such that the algebraic variety $V = \mathcal{Z}(I(\underline{\alpha}))$ verifies $V = G.\underline{\alpha}$. A symmetric representation of the Galois group of $g$ is such a maximal subgroup $G$ (for the inclusion) of $\mathfrak{S}_n$. It is denoted by $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha})$ in the sequel.*

REMARK 4. *As soon as a Gröbner basis of $I(\underline{\alpha})$ and the generators of $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha})$ are known, we can represent the action of the Galois group of $g$ over a symbolic representation of its roots. In fact, the group $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha})$ is the stabilizer of $I(\underline{\alpha})$ (see [1]), thus it represents the $\mathbb{K}$-automorphisms of the algebra $\mathbb{K}[\underline{X}_n]/I(\underline{\alpha})$. Hence, the objects that we want to compute are exactly a Gröbner basis of $I(\underline{\alpha})$ and its stabiliser $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha})$.*

Lemma 2.1 shows that any Galois $\underline{\alpha}$-ideal is included in $I(\underline{\alpha})$. More generally, we have the following result:

LEMMA 2.2. *Let $\sigma$ be a permutation of $\mathrm{Gal}_{\mathbb{Q}}(\underline{\alpha})$. For any Galois $\underline{\alpha}$-ideal $I$, we have:*

$$\forall R \in I,\ I + \sigma.R \subset I(\underline{\alpha})\,.$$

PROOF. We have $I \subset I(\underline{\alpha})$, thus $R \in I(\underline{\alpha})$. Since $\sigma.\underline{\alpha} \in \mathcal{Z}(I(\underline{\alpha}))$ (see Proposition-Definition 3), we have $(\sigma.R)(\underline{\alpha}) = R(\sigma.\underline{\alpha}) = 0$, which implies that $\sigma.R \in I(\underline{\alpha})$ since $I(\underline{\alpha})$ is radical. □

When $\mathbb{K}$ is perfect, a Galois $\underline{\alpha}$-ideal $I \subset \mathbb{K}[\underline{X}_n]$ for which there exists a subgroup $G$ of $\mathfrak{S}_n$ such that $\mathcal{Z}(I) = G.\underline{\alpha}$ is generated by a *separable triangular* set (see [4]). Following the proof of [4], we provide further a more general result.

*Definition 5.* A subset $\mathcal{T} = \{f_1, \ldots, f_n\}$ of $\mathbb{K}[\underline{X}_n]$ is said to be *triangular* if there exist $n$ positive integers $k_1, \ldots, k_n$ such that:

$$\forall i \in [\![1, n]\!],\ \mathrm{HM}(f_i) = {x_i}^{k_i}\,.$$

A triangular set $\mathcal{T} = \{f_1, \ldots, f_n\}$ is said to be *separable* if for all $i \in [\![1, n]\!]$, and for all $\underline{\beta} \in \mathcal{Z}(\langle\mathcal{T}\rangle)_{i-1}$, $f_i(\beta, x_i)$, seen as a univariate polynomial in $x_i$, is separable.

REMARK 6. *Note that in our definition, we only consider triangular sets whom initials are equal to* 1*, so that the ideal generated by the considered triangular set is the saturated ideal of the triangular set (see [3]). In particular, from [3], the saturated ideal of a* separable *triangular set is radical. In our case, this means that the ideals generated by the separable triangular sets we consider are radical.*

We show now how to generalize the result of [4] about triangular sets and Galois ideals. The first result we need is about *equiprojectable varieties* (see [4, 8] for a definition).

LEMMA 2.3. *An algebraic variety $V$ of $(\bar{\mathbb{K}}^{\mathrm{sep}})^n$ (where $\bar{\mathbb{K}}^{\mathrm{sep}}$ is the separable closure of $\mathbb{K}$) is equiprojectable if and only if the ideal $\mathcal{I}(V)$ can be represented by a separable triangular set.*

PROOF. A proof is given in [4] for the case where $\mathbb{K}$ is perfect but this result does not depend on the perfectness of the base field as soon as we suppose the field $\mathbb{K}[V]$ separable which is the case here (for example, see [9] where this result is used). □

From this lemma we obtain the following generalization of [4].

PROPOSITION 2.4. *Let $I \subset \mathbb{K}[\underline{X}_n]$ be a Galois ideal. If there exists a subgroup $G$ of $\mathfrak{S}_n$ and an element $\underline{\alpha}$ of the algebraic variety $V = \mathcal{Z}(I)$ such that $V = G.\underline{\alpha}$ then there exists a separable triangular set generating $I$.*

PROOF. Let $G$ be a subgroup of $\mathfrak{S}_n$. An algebraic variety $V \subset \bar{\mathbb{K}}^n$ such that $V = G.\underline{\alpha}$, where $\underline{\alpha}$ is an $n$-tuple of roots of a separable degree $n$ polynomial, is equiprojectable (see [4]). Moreover, since $\mathbb{K}(\underline{\alpha})$ is separable so is $\mathbb{K}[V]$ and the result follows from Lemma 2.3. □

REMARK 7. *A Galois ideal whose associated algebraic variety satisfies the conditions of Proposition 2.4 is said to be* pure*. There exist Galois ideals which are not pure and triangular thus Proposition 2.4 is not an equivalence. Moreover, there exist Galois ideals which are not triangular (see [19]).*

Separable triangular sets have many other properties (see [3]), we use the following one in the sequel.

LEMMA 2.5. *Let $\mathcal{T} = \{f_1, \ldots, f_n\}$ be a separable triangular set of $\mathbb{K}[\underline{X}_n]$ and $R$ be a polynomial of $\mathbb{K}[\underline{X}_n]$ such that $\mathrm{HM}(R) = x_j$ with $j \geqslant 2$. Suppose that the ideal $\langle\mathcal{T}, R\rangle \neq \mathbb{K}[\underline{X}_n]$) and $\langle f_1, \ldots, f_{j-1}\rangle$ is a maximal ideal of $\mathbb{K}[\underline{X}_{j-1}]$.*

*Then, the ideal $\langle\mathcal{T}, R\rangle$ is generated by the triangular set*

$$\mathcal{T}' = \{f_1, \ldots, f_{j-1}, R, f_{j+1}, \ldots, f_n\}$$

*which is separable.*

PROOF. Denote by $\mathcal{T}_{j-1}$ the set $\{f_1, \ldots, f_{j-1}\}$. Since $\langle\mathcal{T}_{j-1}\rangle$ is maximal, the quotient ring $A = \mathbb{K}[\underline{X}_j]/\langle\mathcal{T}_{j-1}\rangle$ is a field. This implies that $A[x_j]$ is a principal ideal domain. For $p \in \mathbb{K}[\underline{X}_j]$, we denote by $\hat{p}$ its image in $A[x_j]$. Let $F$ be a representative of the gcd $\hat{F}$ of $\hat{f}_j$ and $\hat{R}$ in $A[x_j]$. Since $F$ can be rewritten as an algebraic combination of $R$ and $f_j$ and $f_1, \ldots, f_{j-1}$, one has $\langle f_1, \ldots, f_{j-1}, F\rangle \subset \langle f_1, \ldots, f_{j-1}, f_j, R\rangle$. Consider now an element $p$ of $\langle f_1, \ldots,$

$f_{j-1}, f_j, R\rangle$ and let $\hat{p}$ its image in $A[x_j]$. Thus, $\hat{p}$ is a multiple of $\hat{F}$ which implies that $p$ can be written as an algebraic combination of $f_1, \ldots, f_{j-1}, F$. Thus, $\langle f_1, \ldots, f_{j-1}, F\rangle = \langle f_1, \ldots, f_{j-1}, f_j, R\rangle$. This implies that $\langle f_1, \ldots, f_{j-1}, F, \ldots, f_n\rangle = \langle f_1, \ldots, f_{j-1}, f_j, R, \ldots, f_n\rangle$. By assumption $\mathrm{HM}(R) = x_j$ which implies that either $\hat{F}$ is the unit in $A$, or $\hat{R} = \hat{F}$. Since $\langle \mathcal{T}, R\rangle \neq \mathbb{K}[\underline{X}_n]$, one has $\hat{F} = \hat{R}$.

It remains to prove that $\mathcal{T}' = \langle f_1, \ldots, f_{j-1}, R, \ldots, f_n\rangle$ is separable. Note that by assumption, $\mathcal{T}_{j-1}$ is separable. Since $R$ is linear in $x_j$, $\hat{R}$ is separable in $A[x_j]$. Consider now for $j+1 \leqslant i \leqslant n$, the image of $f_i$ in $\mathbb{K}[\underline{X}_{i-1}]/\langle f_1, \ldots, f_{j-1}, R, \ldots, f_{i-1}\rangle$. Remark that if it is not separable, then $\mathcal{T}$ can not be separable since $\mathcal{Z}(\mathcal{T}') \subset \mathcal{Z}(\mathcal{T})$. □

## 3. MAIN RESULTS

In this section, we fix $g \in \mathbb{K}[x]$ a polynomial of degree $n \geqslant 5$ with $D_n$ as a symmetric representation of its Galois group (thus this polynomial is irreducible and separable). Such a polynomial is said to be a *dihedral polynomial* of degree $n$. We present an algorithm for the computation of a relations ideal of $g$ from its factorization over its stem field. Here we only know the name of the Galois group of $g$. We show how to fix the representation of this group by numbering the factors of $g$ over its stem field (which is equivalent to fix the order of roots orbits of $g$). Then, from this particular representation of the Galois group we deduce a process in order to construct a triangular set of a relations ideal of $g$ by group action (same sorts of group actions are used in [20, 17] in order to avoid computations).

PROPOSITION 3.1. *Let $\alpha_1$ be a root of $g$.*
*The factorization of $g$ over its stem field $\mathbb{K}(\alpha_1)$ is given by:*

$$\begin{array}{ll} (x-\alpha_1)g_2(\alpha_1,x)\ldots g_{\frac{n+1}{2}}(\alpha_1,x) & n \text{ odd} \\ (x-\alpha_1)g_2(\alpha_1,x)\ldots g_{\frac{n}{2}}(\alpha_1,x)(x-b_{\frac{n}{2}+1}(\alpha_1)) & n \text{ even} \end{array}$$

*where $g_i(t,x) = x^2 + b_i(t)x + a_i(t)$ and $a_i$, $b_i$ are univariate polynomials of degree at most $n-1$.*

PROOF. A symmetric representation of the Galois group of $g$ over the field $\mathbb{K}(\alpha_1)$ is

$$\mathrm{Stab}_{D_n}(\{1\}) = \{s \in D_n \mid s(1) = 1\}.$$

This group is explicitly given by:

$$\mathrm{Stab}_{D_n}(\{1\}) = \begin{cases} \langle (2,3)\ldots(n-1,n)\rangle & n \text{ odd} \\ \langle (2,3)\ldots(n-2,n-1)\rangle & n \text{ even} \end{cases}$$

The orbits of the action of $\mathrm{Stab}_{D_n}(\{1\})$ over $\{1, \ldots, n\}$ are:

$$\begin{array}{ll} \{1\}, \{2,3\}, \ldots, \{n-1,n\} & n \text{ odd} \\ \{1\}, \{2,3\}, \ldots, \{n-2,n-1\}, \{n\} & n \text{ even.} \end{array}$$

There is a one-to-one correspondence between the orbits of the canonical action of the Galois group of a polynomial over its roots and the set of roots of its irreducible factors, so the result follows. □

Let $g_i$ be the factors of $g$ over its stem field with a fixed numbering as in Proposition 3.1. We consider the ideal of $\mathbb{K}[\underline{X}_n]$ generated by the following separable triangular set $\mathcal{T}_1$:

n odd:

$$\begin{cases} f_1 = g(x_1) \\ f_2 = g_2(x_1, x_2) \\ f_3 = x_3 + x_2 + b_2 \\ \quad\vdots \\ f_{2i} = g_{i+1}(x_1, x_{2i}) \\ f_{2i+1} = x_{2i+1} + x_{2i} + b_{i+1} \\ \quad\vdots \\ f_{n-1} = g_{(n+1)/2}(x_1, x_{n-1}) \\ f_n = x_n + x_{n-1} + b_{(n+1)/2} \end{cases}$$

n even:

$$\begin{cases} f_1 = g(x_1) \\ f_2 = g_2(x_1, x_2) \\ f_3 = x_3 + x_2 + b_2 \\ \quad\vdots \\ f_{2i} = g_{i+1}(x_1, x_{2i}) \\ f_{2i+1} = x_{2i+1} + x_{2i} + b_{i+1} \\ \quad\vdots \\ f_{n-2} = g_{n/2}(x_1, x_{n-2}) \\ f_{n-1} = x_{n-1} + x_{n-2} + b_{n/2} \\ f_n = x_n + b_{n/2+1} \end{cases}$$

where the polynomials $b_i$ are univariate in $x_1$.

Remark that the set $\mathcal{T}_1$ depends on the numbering of the factors of $g$ in its stem field. Thus, there exist several different sets constructed as $\mathcal{T}_1$. Actually, if $\Omega$ denotes the set of permutations of $\mathrm{Stab}_{\mathfrak{S}_n}(\{1\})$ defined by

$n$ odd :

$$\begin{array}{cccccccc} 2 & 3 & 4 & 5 & \ldots & n-1 & & n \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \ldots & \updownarrow & & \updownarrow \\ 2k_1 & 2k_1+1 & 2k_2 & 2k_2+1 & \ldots & 2k_{(n+1)/2} & & 2k_{(n+1)/2}+1 \end{array}$$

$n$ even :

$$\begin{array}{ccccccc} 2 & 3 & 4 & 5 & \ldots & n-2 & n-1 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \ldots & \updownarrow & \updownarrow \\ 2k_1 & 2k_1+1 & 2k_2 & 2k_2+1 & \ldots & 2k_{n/2} & 2k_{n/2}+1 \end{array}$$

where $k_i \in [\![1, \lfloor \frac{n+1}{2} \rfloor]\!]$, then the set

$$\mathcal{S} = \{\{\omega.f \,:\, f \in \mathcal{T}_1\} \,:\, \omega \in \Omega\}$$

represents all possible triangular sets with the same form as $\mathcal{T}_1$ and constructed with the factors $g_i$ (a permutation of $\Omega$ corresponds to a numbering of these factors).

PROPOSITION 3.2. *There exists a triangular set $\mathcal{T}$ in $\mathcal{S}$ such that the ideal $\langle \mathcal{T}\rangle$ is an $\underline{\alpha}$-Galois ideal where $\underline{\alpha}$ is an $n$-tuple of the roots of $g$ satisfying* $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = D_n$.

PROOF. Let $\underline{\alpha}$ be an $n$-tuple of different roots of $g$ verifying $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = D_n$. In the proof of Proposition 3.1, we have seen that for all integer $i$ in $[\![1, \lfloor \frac{n+1}{2} \rfloor]\!]$, the set $R_i = \{\alpha_{2i}, \alpha_{2i+1}\}$ corresponds to the roots of a quadratic factor of $g$ in $\mathbb{K}(\alpha_1)[x]$. If we number these factors so that $Roots(g_i) = R_i$ for each $i$ in $[\![1, \lfloor \frac{n+1}{2} \rfloor]\!]$, then we can construct a triangular set $\mathcal{T}$ contained in $\mathcal{S}$ so that $\underline{\alpha}$ is a zero of $I = \langle \mathcal{T}\rangle$ and $\mathcal{Z}(I) \subset \mathfrak{S}_n.\underline{\alpha}$. As $\mathcal{T}$ is clearly triangular and separable (since $\mathcal{T}_1$ is) , we have the result by Lemma 2.1 and Remark 6. □

In particular, we have the following result:

COROLLARY 3.3. *With the same notations as in Proposition 3.2, if the degree $n$ of $g$ is equal to 5, then all the ideals generated by the triangular sets of $\mathcal{S}$ are $\underline{\alpha}$-Galois ideals with* $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = D_5$.

PROOF. When $n = 5$, by Proposition 3.1 we have two non linear factors, so two possible numberings and thus two

triangular sets in $\mathcal{S}$. Let $\langle \mathcal{T}_1 \rangle$ and $\langle \mathcal{T}_2 \rangle$ be the two possible ideals corresponding to these two possible numbering. By Proposition 3.2, at least one of these ideals is an $\underline{\alpha}$-Galois ideal with $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = D_5$, let $\langle \mathcal{T}_1 \rangle$ be this ideal. We have

$$\mathcal{T}_2 = \{\omega.f \mid f \in \mathcal{T}_1\}$$

where $\omega = (5,\ 3)(2,\ 4)$, thus $\langle \mathcal{T}_2 \rangle$ is an $(\omega^{-1}.\underline{\alpha})$-Galois ideal with

$$\mathrm{Gal}_{\mathbb{K}}(\omega^{-1}.\underline{\alpha}) = \omega^{-1}.\,\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}).\omega\,.$$

Since $\omega^{-1}\,\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha})\omega = \omega^{-1}D_5\omega = D_5$ we obtain the result. □

Remark 8. *Corollary 3.3 can be seen as a symbolic reformulation of the result of Spearman and Williams [21].*

If the ideal $\langle \mathcal{T} \rangle$ of Proposition 3.2 is known, the following proposition shows how to construct a Gröbner basis of the relations ideal $I(\underline{\alpha})$ with $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = D_n$ by only applying the action of a permutation on the variables of the polynomials of $\mathcal{T}$. Actually, a triangular set of $\mathcal{S}$ which generates an $\underline{\alpha}$-Galois ideal with $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = D_n$ fixes an order on the roots of $g$, thus we can apply a particular group action on this set.

Proposition 3.4. *Consider a triangular set $\mathcal{T} = \{f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)\}$ of $\mathcal{S}$ such that $\langle \mathcal{T} \rangle$ is an $\underline{\alpha}$-Galois ideal with $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = D_n$ and*

$$\mu = \begin{cases} (1\ 2)(3\ 4)\ldots(n-2\ n-1) & n \text{ odd} \\ (1\ 2)(3\ 4)\ldots(n-1\ n) & n \text{ even} \end{cases}$$

*be a permutation of $\mathfrak{S}_n$. Then, the set $\mathcal{T}'$ containing the 3 polynomials $f_1, f_2, f_n$, all the $f_i$ with even integer $1 < i < n$ and $\mu.f_i$ with odd integer $1 < i < n-1$, is a Gröbner basis of the ideal $I(\underline{\alpha})$.*

Proof. We can suppose w.l.o.g. that $\mathcal{T} = \mathcal{T}_1$ (as we have seen above, it depends only on the numbering of the factors $g_i$). Since for all odd integer $k = 2i-1$ with $i \in [\![2, \lfloor \frac{n-1}{2} \rfloor]\!]$, we have:

$$\mu.f_k = \mu.(x_k + x_{k-1} + b_{i+1}(x_1)) = x_{k+1} + x_{k-2} + b_{i+1}(x_2)\,,$$

the set $\mathcal{T}'$ is given by

$n$ odd :

$$\begin{cases} f_1 \\ f_2 \\ f_3 \\ x_4 + x_1 + b_2(x_2) \\ \quad\vdots \\ x_{2i} + x_{2i-3} + b_i(x_2) \\ f_{2i+1} \\ \quad\vdots \\ x_{n-1} + x_1 + b_{(n+1)/2}(x_2) \\ f_n \end{cases}$$

$n$ even :

$$\begin{cases} f_1 \\ f_2 \\ f_3 \\ x_4 + x_1 + b_2(x_2) \\ \quad\vdots \\ x_{2i} + x_{2i-3} + b_i(x_2) \\ f_{2i+1} \\ \quad\vdots \\ x_{n-2} + x_1 + b_{(n-2)/2}(x_2) \\ f_{n-1} \\ f_n \end{cases}$$

By construction, the set $\mathcal{T}'$ is triangular, so it is a Gröbner basis (see [7]) and we just have to prove that this set generates the relations $\underline{\alpha}$-ideal. For this, we first prove that the ideal generated by $\mathcal{T}'$ is maximal and then that it is contained in $I(\underline{\alpha})$.

The permutation $\mu$ is in $D_n$, more precisely we have the (right) product $\mu = \sigma\tau$. Since $\mathbb{K}[\underline{X}_2]/\langle f_1, f_2 \rangle$ is isomorphic to a field (since $f_1 = g$ and $f_2$ corresponds to an irreducible factor of $g$ over its stem field), all ideals of the form

$$\langle f_1, f_2, x_3 + h_3(x_1, x_2), \ldots, x_i + h_i(x_1, \ldots, x_{i-1}) \rangle$$

is a maximal ideal of $\mathbb{K}[\underline{X}_i]$. Thus we can recursively use the lemma 2.5 in order to construct a new ideal which is generated by $\mathcal{T}'$:

$$I = \langle \mathcal{T}_1 \rangle + \langle \mu.f_3 \rangle + \langle \mu.f_5 \rangle + \ldots + \langle \mu.f_m \rangle,$$

where $m$ is the greatest odd integer less than $n-1$. Then $I$ is generated by the set $\mathcal{T}'$ and is maximal. By lemma 2.2, we have $I \subset I(\underline{\alpha})$, hence $I$ is the relations $\underline{\alpha}$-ideal. □

Remark 9. *The last relation of the set $\mathcal{T}'$ can be replaced by the classical one $x_n + x_{n-1} + \ldots + x_1 + c$ where $c$ is the coefficient of $x^{n-1}$ in $g$.*

Now, if we want to apply Proposition 3.4 for the computation of a relations ideal of $g$, we need to know an effective method to choose a triangular set in $\mathcal{S}$ which verifies the hypothesis of this proposition.

Proposition 3.5. *Let $\mathcal{T}$ be a triangular set of $\mathcal{S}$ and $\mathcal{T}'$ be the triangular set obtained by action of $\mu$ on $\mathcal{T}$ (as in Proposition 3.4). If we have the following inclusion*

$$\langle \mathcal{T} \rangle \subset \langle \mathcal{T}' \rangle\,,$$

*then $\mathcal{T}$ is an $\underline{\alpha}$-Galois ideal with $\underline{\alpha}$ an $n$-tuple of roots of $g$ and verifying $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = D_n$*

Proof. Assume that $\langle \mathcal{T} \rangle \subset \langle \mathcal{T}' \rangle$. As we have seen in the proof of Proposition 3.4, the ideal $\langle \mathcal{T}' \rangle$ is maximal, thus, if $\underline{\beta}$ denotes one of its zeros, it is a relations $\underline{\beta}$-ideal. Because of the form of $\mathcal{T}'$, one can see that $\mathrm{Gal}_{\mathbb{K}}(\underline{\beta})$, which is a conjugate of $D_n$, contains these two permutations:

$$\mu = \begin{cases} (1\ 2)(3\ 4)\ldots(n-2\ n-1) & n \text{ odd} \\ (1\ 2)(3\ 4)\ldots(n-1\ n) & n \text{ even} \end{cases}$$

$$\tau = \begin{cases} (2\ 3)(4\ 5)\ldots(n-1\ n) & n \text{ odd} \\ (2\ 3)(4\ 5)\ldots(n-2\ n-1) & n \text{ even} \end{cases}$$

Thus $\mathrm{Gal}_{\mathbb{K}}(\underline{\beta})$ contains $\mu\tau = \sigma$ and $\mathrm{Gal}_{\mathbb{K}}(\underline{\beta}) = D_n$. Hence $\langle \mathcal{T} \rangle$ is a $\underline{\beta}$-Galois ideal with $\mathrm{Gal}_{\mathbb{K}}(\underline{\beta}) = D_n$. □

Now, we give the algorithm which computes a triangular basis of a relations ideal of $g$ from its factorization over its stem field $\mathbb{K}[x_1]/\langle g \rangle$. We recall that any quadratic factor $g(t, x)$ of $g$ is of the form $g(t, x) = x^2 + b(t).x + a(t)$.

We first give the scheme of the algorithm. By Corollary 3.3 we can split the process in two parts, the first one for degree 5 where no computations of normal forms is needed, the second for degree at least 6. In the second part, we successively number the factors of $g$ in order to satisfy the condition of

Proposition 3.5 and we apply, at the same time, the action of permutation $\mu$ to construct two linear relations. At the end of the process we obtain a triangular set of a relations ideal of $g$.

**Algorithm:** DihedralRelationsIdeal

**Require:** A dihedral polynomial $g$ of degree $n \geqslant 5$ and the set $F$ of its irreducible quadratic factors over its stem field.

**Ensure:** The set $\mathcal{T} = \{f_1, \ldots, f_n\}$ is a triangular Gröbner basis of a relations ideal $I(\underline{\alpha})$ of $g$ with $\mathrm{Gal}_{\mathbb{K}}(\underline{\alpha}) = D_n$.

$n := Degree(g)$;
$f_1(x_1) := g(x_1)$;

**if** $n = 5$ **then**
  Let $f_2(t,x) = x^2 + b(t).x + a(t)$ and $f_3(t,x) = x^2 + d(t).x + c(t)$ be the two elements of $F$;
  $\mathcal{T} := [f_1(x_1), f_2(x_1, x_2), x_3 + x_2 + b(x_1), x_4 + x_1 + b(x_2), x_5 + x_4 + d(x_4)]$;
  **return** $\mathcal{T}$;
**end if**

Let $f_2(t,x) = x^2 + b(t).x + a(t)$ and $f_3(t,x) = x^2 + d(t).x + c(t)$ be two elements of $F$ such that NormalForm$(f_3(x_1, x_4), [f_1(x_1), f_2(x_1, x_2), x_3 + x_2 + b(x_1), x_4 + x_1 + b(x_2)]) = 0$;
$F := F \setminus \{f_2, f_3\}$;
$\mathcal{T} := [f_1(x_1), f_2(x_1, x_2), x_3 + x_2 + b(x_1), x_4 + x_1 + b(x_2), x_5 + x_4 + d(x_1), x_6 + x_3 + d(x_2)]$;
**if** $n = 6$ **then**
  **return** $\mathcal{T}$;
**end if**

$i := 3$;
**while** $|F| > 1$ **do**
  $i := i + 1$;
  Let $f(t,x) := x^2 + b(t).x + a(t)$ be an element of $F$ such that NormalForm$(f(x_1, x_{2i}), \mathcal{T}) = 0$;
  $F := F \setminus \{f\}$;
  $\mathcal{T} :=$ Concat$(\mathcal{T}, [x_{2i-1} + x_{2i-2} + b(x_1), x_{2i} + x_{2i-3} + b(x_2)])$;
**end while**
$i := i + 1$;
$f(t,x) := x^2 + b(t).x + a(t)$ be the last element of $F$;
$\mathcal{T} :=$ Concat$(\mathcal{T}, [x_{2i+1} + x_{2i} + b(x_1)])$;
**if** $n$ is even **then**
  $c :=$ the coefficient of $x^{n-1}$ in $g$;
  $\mathcal{T} :=$ Concat$(\mathcal{T}, [x_{2i+2} + x_{2i+1} + \ldots + x_1 - c])$;
**end if**
**return** $\mathcal{T}$;

Theorem 3.6. *The algorithm* DihedralRelationsIdeal *terminates and computes a triangular basis of a relations ideal of $g$. Moreover, the number of normal forms performed during the computation is bounded by*

$$\Psi(n) = \begin{cases} 0 & n = 5 \\ 1 & n = 6 \\ \frac{1}{2}(3m^2 - 7m + 6) & n \geqslant 7 \end{cases}$$

*where $n$ is the degree of the polynomial $g$ and $m := \lfloor \frac{n-1}{2} \rfloor$.*

Proof. By Proposition 3.4 and Proposition 3.5, it is clear that this algorithm terminates and gives the good result. All the normal forms are performed when we have to find the good numbering of the $f_i$, so degree 5 is not affected. Finding $f_2$ and $f_3$ requires at most $\frac{m!}{(m-2)!} = m^2 - m$, so there is exactly one normal form to compute in the cases $n = 6$. All the other normal forms are performed during the while loop. Any such loop performs at most $|F| - 1$ normal form. As $|F| = m-2$ before the while loop, the total number of normal forms computations is bounded by:

$$\sum_{k=2}^{m-2} k - 1 = \frac{1}{2}(m-3)(m-2)$$

which gives the result. □

Remark 10. *Consider an irreducible separable polynomial $g$ of degree $n$ whose their irreducible factors over its stem field have the same degrees than the ones of a dihedral polynomial of the same degree. If the above algorithm, applied to the factors of $g$, terminates then, by Proposition 3.5, the Galois group of $g$ is proved to be $D_n$ and we compute at the same time a relations ideal of this polynomial. Using Theorem 3.6, one can stop the* while *loop if the number of computed normal forms is greater than the bound we provide.*

# 4. EXAMPLES

In this section we give two examples of computations of relations ideals using the results of this paper.

## 4.1 Generic $D_5$ relations ideal

This first example is devoted to the computation of a relations ideal of the $D_5$ generic polynomial $f_{D_5}$ of Brumer (see [11, Theorem 2.3.5]). This polynomial has its coefficients in the function field $\mathbb{Q}(s,t)$. The polynomial $f_{D_5}$ is given by:

$$x^5 + (t-3)x^4 + (s-t+3)x^3 + (t^2 - t - 2s - 1)x^2 + sx + t \quad .$$

Using Trager's algorithm (see [23]) we can compute the factorization of $f_{D_5}$ over its stem field $\mathbb{K}[\alpha_1]$. The two non linear factors computed with Magma ([6]) are given by:

$$x^2 + \frac{1}{t}(-\alpha_1^4 + (-t+2)\alpha_1^3 + (-s-1)\alpha_1^2 + (s - t^2 + 2t)\alpha_1 - t)x - \alpha_1 + 1$$

$$x^2 + \frac{1}{t}(\alpha_1^4 + (t-2)\alpha_1^3 + (s+1)\alpha_1^2 + (-s + t^2 - t)\alpha_1 + t(t-2))x + \frac{1}{t}((t-1)\alpha_1^4 + (t^2 - 4t + 2)\alpha_1^3 + (st - s - t^2 + 3t - 1)\alpha_1^2 + (-2st + s + t^3 - 2t^2)\alpha_1) + s - t + 1$$

Corollary 3.3 gives without any other computation the triangular basis of a *g*eneric $D_5$ relations ideal:

$$x_1^5 + (t-3)x_1^4 + (s-t+3)x_1^3 + (-2s + t^2 - t - 1)x_1^2 + sx_1 + t$$

$$x_2^2 - \frac{1}{t}x_2x_1^4 + \frac{t+2}{t}x_2x_1^3 + \frac{-s-1}{t}x_2x_1^2 + \frac{s - t^2 + 2t}{t}x_2x_1 - x_2 - x_1 + 1$$

$$x_3 + x_2 - \frac{1}{t}x_1^4 + \frac{-t+2}{t}x_1^3 + \frac{-s-1}{t}x_1^2 + \frac{s - t^2 + 2t}{t}x_1 - 1$$

$$x_4 - \frac{1}{t}x_2^4 + \frac{-t+2}{t}x_2^3 + \frac{-s-1}{t}x_2^2 + \frac{s - t^2 + 2t}{t}x_2 + x_1 - 1$$

$$x_5 + x_4 + \frac{1}{t}x_1^4 + \frac{t-2}{t}x_1^3 + \frac{s+1}{t}x_1^2 + \frac{-s + t^2 - t}{t}x_1 + t - 2$$

This ideal can be said *generic* because every irreducible polynomial $f \in \mathbb{Q}[x]$ with $D_5$ as Galois group is Tchirnhaus equivalent to a specialization of $f_{D_5}$. So, the basis of a relations ideal $I$ of $f$ verifying $D_5.I = I$, is Tchirnhaus equivalent to a specialisation of the basis of this generic ideal.

## 4.2 An example in degree 8

Let $g = x^8 - 3x^5 - x^4 + 3x^3 + 1$ be a polynomial given by the *Database for Number Fields* of J. Klüners and G. Malle (see [13]) with rational coefficients and Galois group $D_8$. The factorization of $g$ over its stem field $\mathbb{Q}(\alpha_1)$ can be computed with MAGMA, GP/PARI (see [18]) or KANT/KASH (see [12]). The three quadratic factors are:

$$\begin{aligned}
g_2(\alpha_1, x) &= x^2 + \frac{1}{3}(5\alpha_1^7 - 2\alpha_1^6 + 4\alpha_1^5 - 15\alpha_1^4 + 5\alpha_1^3 \\
&\quad +7\alpha_1^2 - 5\alpha_1 + 3)x - 1 \\
g_3(\alpha_1, x) &= x^2 + \frac{1}{3}(-2\alpha_1^7 + \alpha_1^6 - 3\alpha_1^5 + 7\alpha_1^4 - 2\alpha_1^3 + \alpha_1^2 + 3\alpha_1 - 5)x \\
&\quad +\frac{1}{3}(2\alpha_1^7 - 3\alpha_1^6 + 2\alpha_1^5 - 8\alpha_1^4 + 8\alpha_1^3 - 4\alpha_1 + 4) \\
g_4(\alpha_1, x) &= x^2 + \frac{1}{3}(\alpha_1^6 - \alpha_1^5 - \alpha_1^4 - 6\alpha_1^3 + \alpha_1^2 + 5\alpha_1 + 2)x \\
&\quad +\frac{1}{3}(\alpha_1^7 + 3\alpha_1^6 + \alpha_1^5 - \alpha_1^4 - 8\alpha_1^3 + 4\alpha_1 - 1)
\end{aligned}$$

Using Algorithm DIHEDRALRELATIONSIDEAL, we obtain two different choices of numbering which give a trivial normal form. Actually, let $f_1(x_1)$ be $g(x_1)$, if we choose $f_2(x_1, x_2)$ to be the polynomial $g_4(x_1, x_2)$ or $g_3(x_1, x_2)$ and $f_3(x_1, x_4)$ to be the polynomial $g_2(x_1, x_4)$ then, in all cases, we obtain:

$$\text{NORMALFORM}(f_3(x_1, x_4), [f_1(x_1), f_2(x_1, x_2), x_3 + x_2 + b(x_1), x_4 + x_1 + b(x_2)]) = 0$$

where $b$ is the coefficient of $x_1$ in the polynomial $f_2(x_1, x_2)$. If we choose the first numbering we obtain the following relations ideal:

$$\begin{aligned}
&x_1^8 - 3x_1^5 - x_1^4 + 3x_1^3 + 1 \\
&x_2^2 + \frac{1}{3}(x_1^6 - x_1^5 - x_1^4 - 6x_1^3 + x_1^2 + 5x_1 + 2)x_2 \\
&\quad +\frac{1}{3}(x_1^7 + 3x_1^6 + x_1^5 - x_1^4 - 8x_1^3 + 4x_1 - 1) \\
&x_3 + x_2 + \frac{1}{3}(x_1^6 - x_1^5 - x_1^4 - 6x_1^3 + x_1^2 + 5x_1 + 2) \\
&x_4 + x_1 + \frac{1}{3}(x_2^6 - x_2^5 - x_2^4 - 6x_2^3 + x_2^2 + 5x_2 + 2) \\
&x_5 + x_4 + \frac{1}{3}(5x_1^7 - 2x_1^6 + 4x_1^5 - 15x_1^4 + 5x_1^3 + 7x_1^2 - 5x_1 + 1) \\
&x_6 + x_3 + \frac{1}{3}(5x_2^7 - 2x_2^6 + 4x_2^5 - 15x_2^4 + 5x_2^3 + 7x_2^2 - 5x_2 + 1) \\
&x_7 + x_6 - \frac{1}{3}(2x_1^7 + x_1^6 - x_1^5 + 7x_1^4 - 2x_1^3 + x_1^2 + x_1 - 5) \\
&x_8 + x_7 + x_6 + x_5 + x_4 + x_3 + x_2 + x_1 - 3
\end{aligned}$$

# 5. CONCLUSION

In this paper, we proposed a method for the computation of the relations ideal of a dihedral polynomial which permits us to avoid factorizations. We also did the complexity analysis of the underlying algorithm. we hope that a better study of the set $\mathcal{S}$ could improve this algorithm, this will be investigated in a future work.

# 6. REFERENCES


[1] I. Abdeljaouad-Tej, S. Orange, G. Renault, and A. Valibouze. Computation of the decomposition group of a triangular ideal. *AAECC*, 15(3-4):279–294, 2004.

[2] H. Anai, M. Noro, and K. Yokoyama. Computation of the splitting fields and the Galois groups of polynomials. In *Algorithms in algebraic geometry and applications (Santander, 1994)*, volume 143 of *Progr. Math.*, pages 29–50. Birkhäuser, Basel, 1996.

[3] Ph. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symbolic Comput.*, 28(1-2):105–124, 1999. Polynomial elimination—algorithms and applications.

[4] Ph. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. Symbolic Comput.*, 30(6):635–651, 2000. Algorithmic methods in Galois theory.

[5] T. Becker and V. Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[6] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[7] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[8] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC '05: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation*, pages 108–115, New York, NY, USA, 2005. ACM Press.

[9] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC '04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, pages 103–110, New York, NY, USA, 2004. ACM Press.

[10] L. Ducos. Construction de corps de décomposition grâce aux facteurs de résolvantes. *Comm. Algebra*, 28(2):903–924, 2000.

[11] C. U. Jensen, A. Ledet, and N. Yui. *Generic polynomials*, volume 45 of *Mathematical Sciences Research Institute Publications*. Cambridge University Press, Cambridge, 2002. Constructive aspects of the inverse Galois problem.

[12] *KANT/KASH3*, 2005. http://www.math.tu-berlin.de/ kant/kash.html.

[13] J. Klüners and G. Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, 4:182–196 (electronic), 2001.

[14] D. Lazard. Solving zero-dimensional algebraic systems. *J. Symbolic Comput.*, 13(2):117–131, 1992.

[15] D. Lazard. Solving quintics by radicals. In *The legacy of Niels Henrik Abel*, pages 207–225. Springer, Berlin, 2004.

[16] J. McKay and R. Stauduhar. Finding relations among the roots of an irreducible polynomial. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 75–77 (electronic), New York, 1997. ACM.

[17] S. Orange, G. Renault, and A. Valibouze. Calcul efficace d'un corps de dcomposition. LIP6 Research Report 005, LIP6, Laboratoire d'Informatique de Paris 6, 2003. http://www.lip6.fr/reports/lip6.2003.005.html.

[18] *PARI/GP, version* `2.2.5`, 2003. http://www.parigp-home.de.

[19] G. Renault. *Calcul efficace de corps de décomposition*. PhD thesis, Université Paris 6, 2005.

[20] G. Renault and K. Yokoyama. A modular algorithm for computing a relations ideal of a polynomial. *In preparation*, 2005.

[21] B. K. Spearman and K. S. Williams. Dihedral quintic polynomials and a theorem of Galois. *Indian J. Pure Appl. Math.*, 30(9):839–845, 1999.

[22] N. Tchebotarev. *Gründzüge des Galois'shen Theorie*. P. Noordhoff, 1950.

[23] B. Trager. Algebraic factoring and rational functiun integration. In *Proceedings of SYMSAC'76*, pages 219–226, 1976.

[24] A. Valibouze. Étude des relations algébriques entre les racines d'un polynôme d'une variable. *Bull. Belg. Math. Soc. Simon Stevin*, 6(4):507–535, 1999.

[25] K. Yokoyama. A modular method for computing the Galois groups of polynomials. *J. Pure Appl. Algebra*, 117/118:617–636, 1997. Algorithms for algebra (Eindhoven, 1996).