Dynamic Galois Theory

G.M. Diaz–Toca*, Dpto. de Matemática Aplicada,
Universidad de Murcia, Spain.
H. Lombardi, Laboratoire de Mathématiques, UMR CNRS 6623,
Université de Franche-Comté, France.

April 23, 2010

Abstract

Given a separable polynomial over a field, every maximal idempotent of its splitting algebra defines a representation of its splitting field. Nevertheless such an idempotent is not computable when dealing with a computable field if this field has no factorization algorithm for separable polynomials. Moreover, even when such an algorithm does exist, it is often too heavy. So we suggest to address the problem with the philosophy of lazy evaluation: make only computations needed for precise results, without trying to obtain a priori a complete information about the situation. In our setting, even if the splitting field is not computable as a static object, it is always computable as a dynamic one. The Galois group has a very important role in order to understand the unavoidable ambiguity of the splitting field, and this is even more important when dealing with the splitting field as a dynamic object. So it is not astonishing that successive approximations to the Galois group (which is again a dynamic object) are a good tool for improving our computations. Our work can be seen as a Galois version of the Computer Algebra software D5 [7].

Introduction

This work is a continuation and improvement of [8]. Given a separable polynomial $f(T)$ over a discrete field $\mathbb{K}$, we want to run computations in the splitting field in an exact way with the minimum effort. We propose to address the problem with the philosophy of lazy evaluation: make only computations needed for an asked result, without trying to compute a priori a representation of the splitting field.

Our goal here is to introduce lazy algorithms for computations in a splitting field of $f(T)$, some of them with no factorization assumptions for the given computable field. In what follows, $\mathbf{A}_{\mathbb{K},f}$ will denote the splitting algebra associated to $f(T)$. A splitting field can be defined by an ideal generated by a maximal idempotent e of $\mathbf{A}_{\mathbb{K},f}$ (the quotient $\mathbf{A}_{\mathbb{K},f}/\langle e\rangle$ is a splitting field). In some important particular cases, computational methods for the construction of this ideal are known (see for example [15] and for implementations, [3]). However these methods work only for polynomials over the rationals or over number fields. In fact there is no algorithm to compute such an idempotent in the general situation. E.g., computing a splitting field for $T^2 - a$ in characteristic $\neq 2$ requires to know if a is a square in the base field. And there is clearly no general algorithm testing the squares in a computable field. In a similar way, even when $T^3 + pT + q$ is known to be irreducible, the computation of a splitting field in characteristic $\neq 2, 3$ requires to know if the discriminant is a square.

Instead we propose the following idea: consider the splitting algebra as a lazy approximation to the splitting field and start computing. If when calculating, we find an element z indicating that the splitting algebra is not really a field, then we will react by applying our algorithms to construct a new algebra where z will behave in a correct way. Thus, we will consider this new algebra as our new splitting field, go on computing and proceed in the same way if we find another element indicating that this new algebra is not a field. Moreover, each time we improve our knowledge of the splitting field, we are able to improve also our knowledge of the Galois group. For this reason, the splitting field and Galois group are "dynamic objects".

In fact, all the successive algebras appearing as lazy splitting fields of $f(T)$ are Galois quotients of the splitting algebra. These quotients are defined by Galois ideals whose stabilizers define our "dynamic Galois groups".

*This work is partially supported by the MICINN project MTM2008-04699-C03-03

We would like to emphasize that this manner of proceeding, based on the D5 philosophy (see [7]), is important from a theoretical point of view, since when no factorization algorithm is available for separable polynomials, the splitting field cannot exist as a computable static object. It is also important for a practical point of view. Indeed even when a factorization algorithm does exist, it is often too heavy.

The D5 philosophy allows us to give a clear computational content for the splitting field and the Galois group: even when they are not computable static objects, they are always computable dynamic objects. This also gives for example a clear status to the separable closure of a discrete field in constructive mathematics. This separable closure is in fact a dynamic computable object.

Another "dynamic" approach is introduced in [18, 19], where a scheme is presented for constructing algebraic extensions of $\mathbb{Q}$ as needed during a computation. The techniques described in these articles provide a dynamic algebraic closure of $\mathbb{Q}$. However they are different from ours because on the one hand, the Galois structure of $\mathbf{A}_{\mathbb{K},f}$ is not used and on the other hand, they are based on modular evaluations techniques and require factorization algorithms. These smart techniques cannot be generalized to an arbitrary computable field.

The paper is organized as follows. Section 1 recalls basic facts about the splitting algebra of a polynomial. Section 2 introduces the definition and properties of Galois quotients. In Section 3, we present the algorithms and emphasize the dynamic aspect of our methodology with examples.

1 Splitting Algebras

Let $\mathbb{K}$ be a computable field. Let $f(T) \in \mathbb{K}[T]$ be a separable monic polynomial, given by

$$f = T^n + \sum_{k=1}^{n} (-1)^k a_k T^{n-k}.$$

Given the polynomial ring $\mathbb{K}[X_1, \ldots, X_n]$ and the ideal $\mathcal{J}(f)$ generated by the symmetric functions on the roots of $f(T)$,

$$\mathcal{J}(f) = \left\langle a_1 - \sum_{i=1}^{n} X_i,\ a_2 - \sum_{1 \le i < j \le n} X_i X_j, \ldots,\ a_n - \prod_{i=1}^{n} X_i \right\rangle,$$

the *splitting algebra of* $f(T)$, denoted by $\mathbf{A}_{\mathbb{K},f}$, is defined as the following quotient ring

$$\mathbf{A}_{\mathbb{K},f} = \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f) = \mathbb{K}[x_1, \ldots, x_n].$$

In this algebra the polynomial $f(T)$ totally splits

$$\overline{f}(T) = \prod_{i=1}^{n} (T - x_i).$$

This factorization of $f(T)$ is known as the universal decomposition of $f(T)$. Moreover the Cauchy Modules polynomials associated to $f(T)$ define a triangular Gröbner basis for the ideal $\mathcal{J}(f)$ (see [20] for more details).

Let S_n be the symmetric group of degree n. It is well known that if we make S_n to act on $\mathbb{K}[X_1, \ldots, X_n]$, then we have that

$$\forall\, \sigma \in \mathrm{S}_n,\ \forall\, P \in \mathcal{J}(f),\ \sigma(P) \in \mathcal{J}(f).$$

Consequently, S_n acts on $\mathbf{A}_{\mathbb{K},f}$ and actually, can be seen as a first approximation to the Galois group of f (the group of $\mathbb{K}$-automorphisms of the splitting field of $f(T)$).

In order to recall the main properties of $\mathbf{A}_{\mathbb{K},f}$, we first introduce some definitions. If G denotes a group acting on a $\mathbb{K}$-finite dimensional algebra $\mathbf{B}$ and $a \in \mathbf{B}$, then

- the *stabilizer of* a under the action of G is a subgroup of G defined by

$$\mathrm{Stab}_G(a) = \{g \in G \,\text{such that}\, g(a) = a\}\,;$$

- if $G_1 \subseteq G$, then the subalgebra of the elements fixed by G_1 is given by

$$\mathrm{Fix}_{\mathbf{B}}(G_1) = \{a \in \mathbf{B} \,\text{such that}\, g(a) = a,\ \forall g \in G_1\};$$

- for $a \in \mathbf{B}$, $G.a$ denotes *the orbit of* a under the action of G;
- for $a \in \mathbf{B}$, $\mathrm{Min}_a(T)$ denotes its minimal polynomial over $\mathbb{K}$;
- given $G.a = \{a_1, \ldots, a_k\}$ (without repetition), and assuming that $\mathrm{Fix}_{\mathbf{B}}(G) = \mathbb{K}$, *the resolvent of* a is a polynomial in $\mathbb{K}[T]$ given by

$$\mathrm{Rv}_{G,a}(T) = \prod_{i=1}^{k}(T - a_i).$$

Recall that if e is an idempotent in a ring $\mathbf{R}$ then the ideal $e\mathbf{R}$ can be considered as a ring with e as unit and then the canonical map $e\mathbf{R} \to \mathbf{R}/\langle 1 - e\rangle$ is an isomorpism.

A nonzero idempotent e in a ring is said to be *minimal* (or *indecomposable*) when for any other idempotent e' one has $ee' = 0$ or $ee' = e$ (in other words e is minimal among the nonzero idempotents).

Following the previous notations, the splitting algebra verifies the following well known properties.

Theorem 1

1. $\mathbf{A}_{\mathbb{K},f}$ *is a* $\mathbb{K}$*–vector space of dimension* $n!$
2. *A basis is given by the monomials* $x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}$, $d_k \leq n - k$.
3. *When* S_n *acting on* $\mathbf{A}_{\mathbb{K},f}$, $\mathcal{J}(f)$ *is fixed by* S_n *and* $\mathrm{Fix}(\mathrm{S}_n) = \mathbb{K}$.
4. $\mathbf{A}_{\mathbb{K},f}$ *is separable (and so, etale) over* $\mathbb{K}$*, which implies reduced.*
5. *Given* $a \in \mathbf{A}_{\mathbb{K},f}$*, its minimal polynomial* $\mathrm{Min}_a(T)$ *is the squarefree part of the resolvent* $\mathrm{Rv}_{\mathrm{S}_n,a}(T)$.
6. *Every ideal is generated by an idempotent. Moreover we can compute the idempotent if we have a finite generator system of the ideal.*
7. *If* g *is a minimal idempotent,*
   - $\mathbf{A}_{\mathbb{K},f}/\langle 1 - g\rangle =: \mathbb{L}$ *splitting field of* f,
   - $G = \mathrm{Stab}_{\mathrm{S}_n}(g)$ *acts on* $\mathbb{L}$ *as Galois group of* f,
   - $\mathbf{A}_{\mathbb{K},f} = \bigoplus_{\sigma \in \mathrm{S}_n/G} \sigma(g)\mathbf{A}_{\mathbb{K},f} \simeq \mathbb{L}^m$ *where* $m = (\mathrm{S}_n : G)$.

For more detail see [4, Chapter IV, Section 5], [10, Chapter II] and [14, Chapter 2].

Remark that all these results do have an algorithmic content when the arithmetic operations in $\mathbb{K}$ are computable and there is an explicit test of whether an element is zero. When these hypothesis are satisfied, we will say that $\mathbb{K}$ is a discrete field. Hereafter, we suppose that $\mathbb{K}$ is discrete.

2 Galois Quotients

Next we introduce the definition of Galois idempotents and Galois quotients.

Definition 2

- *A family of nonzero idempotent elements* $\{r_1, \ldots, r_m\}$ *in a commutative ring* $\mathbf{R}$ *is a* Basic System of Orthogonal Idempotents *if* $\sum_{i=1}^{m} r_i = 1$ *and* $r_i r_j = 0$ *for* $1 \leq i < j \leq m$. *This means that* $\mathbf{R} = \bigoplus_{i=1}^{m} r_i\mathbf{R}$.
- *An idempotent in* $\mathbf{A}_{\mathbb{K},f}$ *is said to be* a Galois idempotent of $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$ *when its orbit is a basic system of orthogonal idempotents. More generally if* H *is a group acting on the ring* $\mathbf{R}$, a Galois idempotent of $(\mathbf{R}, H)$ *is an idempotent* e *whose orbit is a basic system of orthogonal idempotents. This means that* $\mathbf{R}$ *is the direct sum* $\bigoplus_{e' \in H.e} e'\mathbf{R}$.
- *A* Galois ideal *of* $(\mathbf{R}, H)$ *is an ideal* $(1 - e)\mathbf{R}$*, where* e *is a Galois idempotent.*
- *A* Galois quotient *of* $(\mathbf{R}, H)$ *is given by the pair* $(\mathbf{B}, G)$*, where*

$$\mathbf{B} := \mathbf{R}/\langle 1 - e\rangle, \quad G := \mathrm{Stab}_H(e), \quad e \text{ a Galois idempotent of } (\mathbf{R}, H)$$

Observe that if e is a Galois idempotent of $(\mathbf{R}, H)$, then, for every $\sigma \in H$, we have either $e\sigma(e) = e$, which means that $\sigma(e) = e$, or $e\sigma(e) = 0$.

A minimal idempotent in $\mathbf{A}_{\mathbb{K},f}$ is an example of Galois idempotent and the corresponding Galois quotient provides a representation of the splitting field and the Galois group of $f(T)$.

2.1 Properties of Galois Idempotents

The following theorem states some useful equivalences for an idempotent written as sum of conjugates of a Galois idempotent.

Theorem 3 *Let g be a Galois idempotent of $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$ and an idempotent e such that $e = g + \sigma_2(g) + \cdots + \sigma_r(g)$ with $g, \sigma_2(g), \ldots, \sigma_r(g)$ pairwise distinct. Let $\sigma_1 = \mathrm{Id} \in \mathrm{S}_n$, $G = \mathrm{Stab}_{\mathrm{S}_n}(g)$ and $E = \mathrm{Stab}_{\mathrm{S}_n}(e)$. The following assertions are equivalent.*

1. *$e \in \mathbf{A}_{\mathbb{K},f}$ is a Galois idempotent.*
2. *$G \subseteq E$ and $e = \sum_{\sigma \in E/G} \sigma(g)$.*
3. *$|E| = r \cdot |G|$.*
4. *$\dim(e\mathbf{A}_{\mathbb{K},f}) = |E|$*

Proof.
Let $\sigma_1, \ldots, \sigma_m$ be a system of representants for S_n/G, $G_i = \sigma_i G$ and $g_i = \sigma_i(g)$. So $\mathrm{S}_n.g = \{g_1, \ldots, g_m\}$ and S_n acts on $\mathrm{S}_n.g$ in the same way as on $\{G_1, \ldots, G_m\}$.
Since $\mathbf{A}_{\mathbb{K},f} = \bigoplus_{i=1}^{m} g_i \mathbf{A}_{\mathbb{K},f}$ we have

$$\dim(g_i \mathbf{A}_{\mathbb{K},f}) = \frac{n!}{m} = \frac{|\mathrm{S}_n|}{(\mathrm{S}_n : G)} = |G|.$$

The Boolean algebra generated by $\mathrm{S}_n.g$ is made of the idempotents $g_I = \sum_{i \in I} g_i$ for all subsets I of $\{1, \ldots, m\}$, and it is isomorphic to the Boolean algebra of subsets of $\{1, \ldots, m\}$ (or if one prefers the subsets of $\mathrm{S}_n.g$). Moreover $g_I \mathbf{A}_{\mathbb{K},f} = \bigoplus_{i \in I} g_i \mathbf{A}_{\mathbb{K},f}$, so

$$\dim(g_I \mathbf{A}_{\mathbb{K},f}) = |I| \dim(g\mathbf{A}_{\mathbb{K},f}) = |I| \cdot |G|.$$

Let us denote $J = \{1, \ldots, r\}$, we get $e = g_J$ and $\dim(e\mathbf{A}_{\mathbb{K},f}) = r \cdot |G|$.
This shows that *3.* $\Leftrightarrow$ *4.*
For $\sigma \in \mathrm{S}_n$ we have $\sigma(g)\mathbf{A}_{\mathbb{K},f} \subseteq \sigma(e)\mathbf{A}_{\mathbb{K},f}$, so

$$\mathbf{A}_{\mathbb{K},f} = \sum_{\sigma \in \mathrm{S}_n} \sigma(g)\mathbf{A}_{\mathbb{K},f} = \sum_{\sigma \in \mathrm{S}_n} \sigma(e)\mathbf{A}_{\mathbb{K},f} = \sum_{\sigma \in \mathrm{S}_n/E} \sigma(e)\mathbf{A}_{\mathbb{K},f} = \sum_{h \in \mathrm{S}_n.e} h\mathbf{A}_{\mathbb{K},f}.$$

Hence the sum $\sum_{h \in \mathrm{S}_n.e} h\mathbf{A}_{\mathbb{K},f}$ is a direct sum iff $|\mathrm{S}_n.e| \cdot \dim(e\mathbf{A}_{\mathbb{K},f}) = |\mathrm{S}_n|$, which is the same thing as $\dim(e\mathbf{A}_{\mathbb{K},f}) = |E|$. Moreover the sum is direct iff e is a Galois idempotent.
This shows that *1.* $\Leftrightarrow$ *4.*
We have $\sigma \in E$ iff $\sigma(\{g_1, \ldots, g_r\}) = \{g_1, \ldots, g_r\}$. Thus let us consider E as acting on $\{g_1, \ldots, g_r\}$. We have

$$r \geq |E.g| = (E : E \cap G) = \frac{|E|}{|E \cap G|}.$$

So the equality $|E| = r \cdot |G|$ is equivalent to $|E \cap G| = |G|$ (which means $G \subseteq E$) and $r = |E.g|$ (which means, when $G \subseteq E$, $e = \sum_{\sigma \in E/G} \sigma(g)$).
This shows that *2.* $\Leftrightarrow$ *3.* □

Note that for a given idempotent e of $\mathbf{A}_{\mathbb{K},f}$, any minimal idempotent g verifies the hypothesis of Theorem 3.

Observe also that if you have an idempotent e and a Gröbner Basis for the ideal $\langle 1 - e \rangle$, then the point *4* provides a method to check if an idempotent is Galois or not, even if we do not know any minimal idempotent g.

As far as Galois quotients are concerned, we can deduce from Theorem 1 and Theorem 3 these properties.

Corollary 1 *Let e be a Galois idempotent of $\mathbf{A}_{\mathbb{K},f}$, $\mathbf{B} = \mathbf{A}_{\mathbb{K},f}/\langle 1 - e \rangle$, $E = \mathrm{Stab}_{\mathrm{S}_n}(e)$ and $r = |\mathrm{S}_n.e|$. Then*

1. *The Galois quotient $\mathbf{B}$ is a $\mathbb{K}$-vector space of dimension $|E|$.*

2. $\mathbf{A}_{\mathbb{K},f} \simeq \mathbf{B}^r$.

3. *The group* E *acts on* $\mathbf{B} \simeq e\mathbf{A}_{\mathbb{K},f}$ *and* $\mathrm{Fix}_{\mathbf{B}}(E) = \mathbb{K}$.

4. *Let* g *be a minimal idempotent such that* $G = \mathrm{Stab}_{\mathrm{S}_n}(g) \subseteq E$ *and* $e = \sum_{\sigma \in E/G} \sigma(g)$. *Let* $k = (E : G)$. *Then*

$$\mathbf{B} \simeq e\mathbf{A}_{\mathbb{K},f} \simeq \bigoplus_{\sigma \in E/G} \sigma(g)\mathbf{A}_{\mathbb{K},f} \simeq \mathbb{L}^k.$$

Thus, knowing a Galois idempotent e involves to get closer to the splitting field and Galois group of the given polynomial. Furthermore, we have the following result.

Proposition 4 *Let* e *be a Galois idempotent of* $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$, $\mathbf{B} = \mathbf{A}_{\mathbb{K},f}/\langle 1 - e\rangle$ *and* $E = \mathrm{Stab}_{\mathrm{S}_n}(e)$. *Let* e' *be a Galois idempotent of* $(\mathbf{B}, E)$. *Let* $x \in \mathbf{A}_{\mathbb{K},f}$, $\overline{x} = e'$ *in* $\mathbf{B}$. *Then*

1. ex *is a Galois idempotent of* $\mathbf{A}_{\mathbb{K},f}$.

2. $\mathbf{B}/\langle 1 - e'\rangle = \mathbf{A}_{\mathbb{K},f}/\langle 1 - e, 1 - x\rangle = \mathbf{A}_{\mathbb{K},f}/\langle 1 - ex\rangle$.

3. $\mathrm{Stab}_{\mathrm{S}_n}(ex) = \mathrm{Stab}_E(e')$.

4. *If* $g' \in \mathbf{B}$ *is a minimal idempotent,* $G' = \mathrm{Stab}_E(g')$ *and* $m = (E : G')$, *then*

   (a) $\mathbf{B}/\langle 1 - g'\rangle =: \mathbb{L}$ *splitting field of* f,

   (b) G' *acts on* $\mathbb{L}$ *as Galois group of* f,

   (c) $\mathbf{B} = \bigoplus_{\sigma \in E/G'} \sigma(g')\mathbf{B} \simeq \mathbb{L}^m$.

Proof.
1. Since x is an element of $\mathbf{A}_{\mathbb{K},f}$ such that $x = e'$ in $\mathbf{B}$, we have $x^2 = x$ in $\mathbf{B}$, that is $ex^2 = ex$ in $\mathbf{A}_{\mathbb{K},f}$. Thus,

$$ex\,ex = e\,e\,x^2 = e\,e\,x = e\,x \text{ in } \mathbf{A}_{\mathbb{K},f}$$

and so ex is an idempotent of $\mathbf{A}_{\mathbb{K},f}$.
The fact that e and e' are Galois idempotents of $\mathbf{A}_{\mathbb{K},f}$ and $\mathbf{B}$ respectively implies that ex is also a Galois idempotent in $\mathbf{A}_{\mathbb{K},f}$.
2. We have $\mathbf{B}/\langle 1 - e'\rangle = \mathbf{A}_{\mathbb{K},f}/\langle 1 - e, 1 - x\rangle$ by definition. $\mathbf{A}_{\mathbb{K},f}/\langle 1 - e, 1 - x\rangle = \mathbf{A}_{\mathbb{K},f}/\langle 1 - ex\rangle$ because

$$\langle 1 - e, 1 - x\rangle = \langle 1 - e, 1 - x, x - xe\rangle = \langle 1 - xe, 1 - e, x - xe\rangle = \langle 1 - xe, 1 - e\rangle$$

and

$$\langle 1 - xe, 1 - e\rangle = \langle 1 - xe^2\rangle = \langle 1 - xe\rangle$$

3. Let $\sigma \in \mathrm{Stab}_{\mathrm{S}_n}(ex)$. If $\sigma(e) \neq e$ in $\mathbf{A}_{\mathbb{K},f}$, since e is Galois idempotent, $\sigma(e)\,e = 0$,

$$ex = \sigma(ex) \text{ and } ex = e^2x = e\sigma(e)\sigma(x) = 0 \Rightarrow x = e' = 0 \text{ in } \mathbf{B},$$

which yields a contradiction. Then $\sigma(e) = e$. Furthermore

$$\sigma(ex) = ex = \sigma(e)\sigma(x) = e\sigma(x) \Rightarrow e' = x = \sigma(x) = \sigma(e') \text{ in } \mathbf{B}.$$

So $\sigma \in \mathrm{Stab}_E(e')$.
Let $\sigma \in \mathrm{Stab}_E(e')$, then $\sigma(e) = e$ and so

$$\sigma(ex) = ex \text{ in } \mathbf{B} \Rightarrow e\sigma(ex) = e^2x \Rightarrow \sigma(ex) = ex.$$

So $\sigma \in \mathrm{Stab}_{\mathrm{S}_n}(ex)$.
4. Since g' is a minimal idempotent in $\mathbf{B}$, the idempotent eg' is a minimal idempotent in $\mathbf{A}_{\mathbb{K},f}$. The result follows from Property 7 of Theorem 1. □

We have shown that Galois quotients have the same good properties as the splitting algebra. Furthermore, the new Galois quotient $(\mathbf{B}/\langle 1 - e'\rangle, \mathrm{Stab}_E(e'))$ is closer to the splitting field and Galois group than $(\mathbf{B}, E)$ $(E = \mathrm{Stab}_{\mathrm{S}_n}(e))$.

2.2 Galois Quotients in literature

The concept of splitting algebra is already mentioned in [6], [13] and [23] and there is a large literature on it, see for example [2], [4, Chapter IV, Section 5], [9], [10, Chapter II], [12] and [14]. As far as Galois quotients are concerned, we are not the first to introduce them. In [11], Galois quotients are introduced as Galois algebras over a field.

Definition 5 ([5]) *Let $A \subseteq B$ be two commutative rings and G a finite group of automorphisms of B. The pair (B, G) is said a* Galois algebra over A of group G *if* $\mathrm{Fix}_B(G) = A$ *and for every $\alpha \neq Id$ in G, 1 is in the ideal generated by the image of $\alpha - Id$.*

The $\mathbb{K}$-algebra $\mathbf{A}_{\mathbb{K},f}$ is an example of Galois algebra over a field $\mathbb{K}$ of group S_n. Recall that $f(T)$ is supposed to be separable through the paper.

Definition 6 ([11]) *Let B be a Galois algebra over a field $\mathbb{K}$ of group G. A proper ideal of B, denoted by I, is a* Galois ideal *if the residual quotient B/I is a Galois algebra over $\mathbb{K}$ of group* $\mathrm{Stab}_G(I)$.

Moreover, in [11] there is a proposition asserting that an ideal is a Galois ideal if and only if for every $\sigma \in G$, either $I = \sigma(I)$ or $I + \sigma(I) = B$. This result shows the equivalence between our Galois ideals and Galois ideals as Definition 6.

Another very different point of view is presented in [21], where the following definitions can be found.

Definition 7 *A proper ideal of $\mathbb{K}[X_1, \ldots, X_n]$ is a* Galois ideal *if it contains the ideal $\mathcal{J}(f)$. A Galois ideal $I \subset \mathbb{K}[X_1, \ldots, X_n]$ is said* pure *if its injector in the relations ideal is a group.*

For details of this definition, see publications of A. Valibouze from 1999.

In [21] one can also find that a Galois ideal I is pure if and only if $|\mathrm{Stab}_{\mathrm{S}_n}(I)| = \dim(\mathbb{K}[\underline{X}]/I)$, which shows that their pure Galois ideals are our Galois ideals. However, their methodology is quite different from ours.

In [14, Chapter 2, section 6, p. 148] Galois idempotents appear in Proposition 10.18 which describes a method for determining the Galois group.

Let us finish the section mentioning that one of the most important properties of Galois (pure) ideals is that their Gröbner basis are triangular. This property independently appears in both [2] and [11]. A generalization of this property appears in [9].

3 Dynamic Computation

Our goal is to be able to do computations into the splitting field of $f(T)$. By computations we mean addition, subtraction, multiplication and computation of inverses. We first consider $\mathbf{A}_{\mathbb{K},f}$ and pretend it to be a splitting field. Thus, $\mathbf{A}_{\mathbb{K},f}$ and S_n will be our first dynamic splitting field and Galois group respectively denoted by $\mathcal{C}_d = \mathbf{A}_{\mathbb{K},f}, \mathcal{G}_d = \mathrm{S}_n$.

If when computing, we find out an element $z \in \mathcal{C}_d$ indicating that $\mathcal{C}_d$ is not a field, we get a new dynamic splitting field and Galois group, defined by a Galois ideal and its stabilizer, where z behaves correctly, and go on computing.

These elements z are said *odd* elements and must verify at least one of these properties,

i) they are neither null nor invertible (T divides $\mathrm{Min}_z(T)$).

ii) $\mathrm{degree}(\mathrm{Min}_z(T)) < \mathrm{degree}(\mathrm{Rv}_{\mathcal{G}_d,z}(T))$,

iii) $\mathrm{Min}_z(T) = R_1(T)\, R_2(T)$, with $\deg(R_1) \geq 1$ and $\deg(R_2) \geq 1$.

In the process, we are gradually obtaining a family of successive Galois quotients. However, since our goal is not to obtain an exact representation of the splitting field but to compute into it, we only reduce our dynamic splitting field if it is necessary.

The boolean algebra defined by idempotents in the splitting algebra contains a finite number of paths which lead to splitting field and Galois group of the given polynomial. The successive vertices of such paths are descending chains of Galois idempotents (in other words, ascending chains of Galois ideals). Every time we get a Galois ideal, we are choosing a vertex, getting closer to the splitting field. Hence,

we dynamically approach the splitting field of the given polynomial by making disappear all oddities we find in the successive detected Galois quotients.

Note that when doing usual computations in (successive approximations of) the splitting field, only computations of inverses lead to finding odd elements. Nevertheless, if one wants to compute better approximations of the splitting field, a possibility is to compute systematically the minimal polynomial of each new element appearing in the computations, in order to find possible oddities. Indeed minimal polynomials lead to oddities not only by ii) but also by iii) and possible factors of a minimal polynomial can be found either through the squarefree decomposition (if the field is perfect) or through gcd computations (e.g., computing the gcd of distinct minimal polynomials). No sophisticated factorization algorithm of polynomials over the base field is needed for this job, gcd computations are sufficient.

Next we are to describe the algorithms to obtain a Galois Quotient from an odd element. Such algorithms have been implemented in Magma (see [3]).

3.1 How to get Galois Quotients

Let $(\mathcal{C}_d, \mathcal{G}_d)$ be a dynamic splitting field. Let $z \in \mathcal{C}_d$ be an odd element.

- If z verifies either property i) or iii), obviously there exist polynomials $P(T)$ and $K(T)$, $\text{degree}(P(T)) \geq 1, \text{degree}(K(T)) \geq 1$, such that $\text{Min}_z(T) = P(T)K(T)$.
- If z verifies property ii), there exists a conjugate of z under the action of $\mathcal{G}_d$, $\sigma(z)$, such that $z - \sigma(z)$ is a zero divisor (for proof, see [8]) and verifies i). Substitute $z - \sigma(z)$ for z in what follows.

Then, let $P(T)$ and $K(T)$ such that $\text{Min}_z(T) = P(T)K(T)$.

3.1.1 From idempotents

By Bezout's Identity, there are $U(T)$ and $V(T)$ verifying $P(T)U(T) + K(T)V(T) = 1$. Consider the element e defined by $e := P(z)U(z)$. Observe that e is idempotent and we compute its orbit $\mathcal{G}_d.e = \{\sigma_1(e) = e, \ldots, \sigma_k(e)\}$. It is possible to compute an element $e_1 \neq 0$ written as a product

$$e_1 := e\sigma_{j_1}(e) \cdots \sigma_{j_t}(e),$$

such that for $1 \leq \ell \leq k$, either $e_1\sigma_\ell(e) = 0$ or $e_1\sigma_\ell(e) = e_1$.

Proposition 8 *The element e_1 is a Galois idempotent. Moreover e is a sum of conjugates of e_1.*

Thus we have the following algorithm presented in [8] to compute Galois quotients,

1. compute e_1,
2. compute $\text{Stab}_{\mathcal{G}_d}(e_1)$,
3. compute the Gröbner basis of $\langle 1 - e_1 \rangle$.

However, from a practical point of view, this is not the most efficient way to obtain a Galois quotient because it requires first the computation of Galois idempotent, second the computation of the stabilizer and finally the Gröbner Basis. Furthermore, the experience tells us that Galois idempotents are usually very large.

It would be a good idea if the stabilizer and the Galois ideal were got at the same time. In fact, it is not necessary to obtain a Galois idempotent to obtain a Galois ideal since

$$\langle 1 - e_1 \rangle = \langle 1 - e, \ldots, 1 - \sigma_{j_t}(e) \rangle$$

Moreover once obtained $L = \{\text{id}, \sigma_{j_1}, \ldots, \sigma_{j_t}\}$, the stabilizer of e_1 under the action of $\mathcal{G}_d$ is given by the next identity

$$\text{Stab}_{\mathcal{G}_d}(e_1) = \{x \in \mathcal{G}_d \mid \forall i \in L, \exists j \in L \text{ such that } i\, x\, j^{-1} \in \text{Stab}_{\mathcal{G}_d}(e)\}.$$

For proof, see [8].

This reasoning yields Algorithm 3.1.

Algorithm 3.1 (Galois Quotient from idempotents)
Input: Idempotent e, $\mathcal{C}_d, \mathcal{G}_d$;
Output: New Galois quotient $(\mathcal{C}_d, \mathcal{G}_d)$;
Local variables : S, C , Ω;

Start $S := \mathrm{Stab}_{\mathcal{G}_d}(e)$; $C := \mathrm{Cosets}(\mathcal{G}_d/S)$; $\Omega := [\,]$;
  for σ **in** C **do**
    if $\sigma(e) \neq 0$ **then**
      Append(Ω, σ);
      $\mathcal{C}_d := \mathcal{C}_d/\langle 1 - \sigma(e)\rangle$;
    end if;
  end for;
  $\mathcal{G}_d := \{x \in \mathcal{G}_d$ such that $\forall i \in \Omega, \exists j \in \Omega$ with $i\,x\,j^{-1} \in S\}$;
  return $\mathcal{C}_d, \mathcal{G}_d$;
End.

Modular Algorithms The performance of Algorithm 3.1 can be affected by the calculation of several Gröbner bases during the process because the computation of Gröbner bases can be computationally expensive. However, we can use modular algorithms to deal with this problem when $\mathbb{K} = \mathbb{Q}$ in the following way.

Following the notation of Algorithm 3.1, suppose we have a Galois ideal I, its stabilizer G, triangular Gröbner basis Gb of I and an idempotent $e \in \mathbb{Q}[\underline{X}]/I$ with its orbit $O = G.e = \{e, \sigma_2(e), \ldots, \sigma_k(e)\}$ as input.

Let p be a prime such that gcd(p,discriminant(f))=1. If $e_1 := e\sigma_{j_1}(e)\cdots\sigma_{j_t}(e)$ is a maximal nonzero product of conjugates of e modulo p, then $e_1 \neq 0$ in characteristic zero and so

$$I + \langle 1 - e, 1 - \sigma_{j_1}(e), \ldots, 1 - \sigma_{j_t}(e)\rangle \subseteq J$$

where J is the Galois ideal we want to compute.

Hence, once we obtain the list $\{1 - e, 1 - \sigma_{j_1}(e), \ldots, 1 - \sigma_{j_t}(e)\}$, we check if the ideal $I + \langle 1 - e, 1 - \sigma_{j_1}(e), \ldots, 1 - \sigma_{j_t}(e)\rangle$ is a Galois ideal in $\mathbb{K}[\underline{X}]$ by applying point 4) of Theorem 3.

Remark that similar modular algorithms can be designed in more general situations.

3.1.2 From zero divisors

When we find an odd element z in a Galois quotient, we can obtain a zero divisor in an easy way. If $\mathrm{Min}_z(T) = P(T)K(T)$, with $P(T)U(T) + K(T)V(T) = 1$, $P(z)$ and $K(z)$ are both zero divisors.

Indeed, if we apply Algorithm 3.1 with $e := P(z)U(z)$, making e be 1 implies making $K(z)$ be 0 in the next Galois quotient. Moreover if $y := K(z)$, observe that $\langle y\rangle = \langle 1 - e\rangle$ because $y = (1 - e)y$ and $y\,V(z) = 1 - e$. Therefore $\langle\sigma(y)\rangle = \langle 1 - \sigma(e)\rangle$ for all σ in $\mathcal{G}_d$.

Thus the ideal $I = \langle y, \sigma_{i_1}(y), \ldots, \sigma_{i_t}(y)\rangle$ such that $1 \notin \langle y, \sigma_{i_1}(y), \ldots, \sigma_{i_t}(y)\rangle$ and $1 \in \langle y, \sigma_{i_1}(y), \ldots, \sigma_{i_t}(y), \sigma(y)\rangle$ for $\sigma(y) \neq \sigma_{i_j}(y)$, $j \leq t$, defines a Galois ideal. This yields the following algorithm.

Algorithm 3.2 (Galois Quotient from zero divisors)
Input: Zero divisor y, $\mathcal{C}_d, \mathcal{G}_d$;
Output: New Galois quotient $(\mathcal{C}_d, \mathcal{G}_d)$;
Local variables : S, C, Ω;

Start S:=$\mathrm{Stab}_{\mathcal{G}_d}(y)$; C:=$\mathrm{Cosets}(\mathcal{G}_d/S)$;
    $\mathcal{C}_d := \mathcal{C}_d/\langle y\rangle$; Ω:=[ ];
  for σ **in** C **do**
    if not IsUnit($\sigma(y)$) **then**
      Append(Ω, σ);
      $\mathcal{C}_d := \mathcal{C}_d/\langle\sigma(y)\rangle$;
    end if;
  end for;
  $\mathcal{G}_d := \{x : x \in \mathcal{G}_d$ such that $\forall i \in \Omega, \exists j \in \Omega$ with $i\,x\,j^{-1} \in S\}$;
  return $\mathcal{C}_d, \mathcal{G}_d$;
End.

Remark that using zero divisors, we can also use modular algorithms.

We would like to emphasize that we require neither a complete factorization of resolvents or minimal polynomials, nor conditions on the stabilizer of z.

In practice, given $z \in \mathcal{C}_d$, we start computing its minimal polynomial $M_z(T)$. If $M_z(T)$ has a root a in $\mathbb{K}$, we run Algorithm 3.2 on $z - a$. If $M_z(T)$ is not equal to the resolvent, there exists $z_j \in \mathcal{G}_d.z$ such that $z - z_j$ is a divisor of zero (for proof, see [8]) and we run Algorithm 3.2 on $z - z_j$. If $M_z(T) = g_1(T)g_2(T)$, we run either Algorithm 3.2 on $g_1(z)$ or Algorithm 3.1 on the idempotent $1 - g_2(z)p_2(z)$, with $g_1(T)p_1(T) + g_2(T)p_2(T) = 1$. Otherwise, the element z behaves as in the splitting field.

Suppose that z is odd. Observe that this hypothesis implies that any element of $\mathcal{G}_d.z$ is odd too. We compute a new Galois quotient. It may happen that in this new quotient, either z or some of its conjugates do not behave as in a field (in other words, some oddities may appear when examining these elements) and consequently we must run our algorithms again until obtaining a good quotient, our new dynamic field, where all elements of $\mathcal{G}_d.z$ behave as in a field.

Moreover, observe that our methods allow us to partially factorize minimal polynomials and resolvents. If $\mathcal{G}_d.z = \{z, \dots, \alpha_r(z)\}$, then it may happen that the minimal polynomials of $\overline{z}, \dots, \overline{\alpha_r(z)}$ in the new dynamic field provide a new factorization of the minimal polynomial of z in the previous one.

3.2 Explicit Computations

In this section we describe what happens when we reduce the dynamic field. It is well known in Galois Theory that given $z \in \mathbf{A}_{\mathbb{K},f}$, if $\mathrm{Min}_z(T) = \mathrm{Rv}_{S_n,z}(T)$ and $\mathrm{Rv}_{S_n,z}(T)$ has a simple root a in $\mathbb{K}$, then the Galois group of $f(T)$ is contained in a conjugate to $\mathrm{Stab}_{S_n}(z)$. This means that $z - a$ is a zero divisor of $\mathbf{A}_{\mathbb{K},f}$ such that the pair $(\mathbf{A}_{\mathbb{K},f}/\langle z - a\rangle, \mathrm{Stab}_{S_n}(z))$ defines a Galois quotient of the splitting algebra (see for example [17]). The next proposition generalizes this result and explains what happens when we run Algorithm 3.2.

Proposition 9 *Let $(\mathbf{B}, G)$ be a Galois quotient. Let $y \in \mathbf{B}$, $G.y = \{y_1, \dots, y_r\}$ with $y = y_1$ and $g(T) = \mathrm{Rv}_{G,y}(T)$.*

1. *Let $a \in \mathbb{K}$ be a simple root of $g(T)$ ($g(a) = 0$ and $g'(a) \neq 0$). Then:*
   (a) *$\mathfrak{b} = \langle y - a\rangle_{\mathbf{B}}$ is a Galois ideal.*
   (b) *Let $\beta : \mathbf{B} \to \mathbf{C} = \mathbf{B}/\mathfrak{b}$ be the natural homomorphism and $H = \mathrm{Stab}_G(\mathfrak{b})$. Then $\beta(y_1) = a$ and for $j \neq 1$, Rv_{H,y_j} divides $g(T)/(T - a)$.*
2. *Let $a \in \mathbb{K}$ be a root of $g(T)$ of multiplicity k. Then:*
   (a) *There exist $j_2, \dots, j_k \in [2..r]$ such that $\mathfrak{b} = \langle y_1 - a, y_{j_2} - a, \dots, y_{j_k} - a\rangle$ is a minimal element of the set of Galois ideals containing $y - a$. Let $j_1 = 1$. For $j \neq j_1, \dots, j_k$, $y_j - a$ is invertible modulo $\mathfrak{b}$.*
   (b) *Let $\beta : \mathbf{B} \to \mathbf{C} = \mathbf{B}/\mathfrak{b}$ be the natural homomorphism and $H = \mathrm{Stab}_G(\mathfrak{b})$. Then $\beta(y_{j_1}) = \cdots = \beta(y_{j_k}) = a$ and for $j \neq j_1, \dots, j_k$, the polynomial Rv_{H,y_j} divides $g(T)/(T - a)^k$.*
3. *Let $\mathfrak{b}$ be a Galois ideal of $\mathbf{B}$ such that $\mathrm{Stab}_G(\mathfrak{b}) \subseteq \mathrm{Stab}_G(y)$. Then $g(T)$ has a root in $\mathbb{K}$.*

Proof.
1a. We need to prove $\langle y_1 - a\rangle + \langle y_j - a\rangle = \langle 1\rangle$ for $j = 2, \dots, r$. In the quotient $\mathbf{B}/\langle y_1 - a, y_2 - a\rangle$ the polynomial $(T - a)^2$ divides $g(T) = \prod(T - y_j)$ and then $g'(a) = 0$. However, since $g'(a) \in \mathbb{K}$, it is invertible and we have $0 = 1$ in the quotient.

1b. One easily sees that $H = \mathrm{Stab}_G(y_1)$. Thus H acts on $\{\beta(y_2), \dots, \beta(y_r)\}$. Since $g(T)/(T - y_1) = \prod_{j=2}^{r}(T - y_j)$ in $\mathbf{B}$, $g(T)/(T - a) = \prod_{j=2}^{r}(T - \beta(y_j))$ in $\mathbf{C}$.

2a. The element $y_1 - a$ is a zero divisor of $\mathbf{B}$. We obtain a minimal Galois ideal $\mathfrak{b}$ containing $y_1 - a$ by adding a maximal number of conjugates of $y_1 - a$ on condition that 1 is not in the ideal. Thus a conjugate of $y_1 - a$ is either 0 or invertible in $\mathbf{B}/\langle\mathfrak{b}\rangle$.
It follows that there exits a subset $J \subseteq [1..r]$ such that the ideal $\mathfrak{b}$ is equal to $\langle y_j - a \,|\, j \in J\rangle$. Let's see $|J| = k$. Since $g(T) = \prod_j(T - \beta(y_j))$ and a has multiplicity k, the number of j such that $\beta(y_j) = a$ is equal to k because $g(a) = g'(a) = \cdots = g^{(k-1)}(a) = 0$ and $g^{(k)}(a)$ invertible.

2b. We follow the same reasoning as *1b*.

3. By assumption $(\mathbf{B}/\mathfrak{b}, \mathrm{Stab}_G(\mathfrak{b}))$ is Galois quotient and $\overline{y_1} \in \mathrm{Fix}(\mathrm{Stab}_G(\mathfrak{b}))$. It follows that $\overline{y_1} \in \mathbb{K}$. Thus $g(T) = \prod_j (T - \overline{y_j})$ in $\mathbf{B}/\mathfrak{b}$ with $g(\overline{y_1}) = 0$, $\overline{y_1} \in \mathbb{K}$. □

Thus, if y is a zero divisor, i.e. $\mathrm{Rv}_{G,y} = T^k Q(T)$ with $Q(0) \neq 0$, Proposition 9 asserts that k elements of $G.y$ define a new Galois quotient. However, in practice, the Galois ideal is usually reached by adding up less than k conjugates although there are exactly k conjugates becoming zero (see Example 1 below).

Next we introduce the constructive version of Theorem 4.7 in [11], Proposition 1 in [16] and (the generalization) of Theorem 15 in [1].

Proposition 10 *Let $y \in \mathbf{B}$ and $G.y = \{y_1, \ldots, y_r\}$. Assume that $\mathrm{Rv}_{G,y} = \mathrm{Min}_y$. Let $\mathrm{Min}_y = R_1 \cdots R_\ell$ be the irreducible factorization of Min_y over $\mathbb{K}[T]$ with $\ell > 1$. Then there exists a Galois quotient $(\mathbf{C}, H)$, with $\beta : \mathbf{B} \to \mathbf{C} = \mathbf{B}/\mathfrak{b}$ as the natural homomorphism and $H = \mathrm{Stab}_G(\mathfrak{b})$ ($\mathfrak{b}$ Galois ideal), such that for every $y_i \in G.y$, there exists j with $\mathrm{Min}_{\beta(y_i)} = R_j$. The group H acts on $\{\beta(y_1), \ldots, \beta(y_r)\}$ and the length of the orbits are $d_1 = \deg(R_1), \ldots, d_\ell = \deg(R_\ell)$. Moreover, this result is repeated in every Galois quotient of $(\mathbf{C}, H)$.*

Let us add that another interesting result involving factors of resultants can be found in [22].

Finally when the minimal polynomial is different from the resolvent, we have the following.

Proposition 11 *Let $y \in \mathbf{B}$, $G.y = \{y_1, \ldots, y_r\}$ and let $g(T) = \mathrm{Rv}_{G,y}(T) = R_1^{p_1} \cdots R_\ell^{p_\ell} \neq \mathrm{Min}_y(T) = R_1 \cdots R_\ell$. Then there exists a Galois quotient $(\mathbb{K}, \mathbf{C}, H)$ with $\beta : \mathbf{B} \to \mathbf{C} = \mathbf{B}/\mathfrak{b}$ as the natural homomorphism, such that for every $y_i \in G.y$, there exists j with $\mathrm{Min}_{\beta(y_i)} = R_j$. Moreover, for every $\beta(y_t) \in H.\beta(y_i)$, the length of $\beta^{-1}(\beta(y_t))$ is p_j.*

3.3 Note about the minimal polynomial and Gröbner Basis

In our work the computation of minimal polynomials is crucial. In Magma it is done with the function `MinimalPolynomial`. On the other hand, an efficient algorithm based on the Berlekamp Massey Algorithm can be found in [24].

It is also possible to compute it via Gröbner Basis. Let Z be a new variable. Given $y \in \mathcal{C}_d$ and the Galois ideal which defines $\mathcal{C}_d$, denoted by $\mathfrak{b}$, the Gröbner basis of the elimination ideal $(\mathfrak{b} + \langle Z - y \rangle) \cap \mathbb{K}[Z]$ returns the minimal polynomial of y.

However, we can get more information about $\mathcal{C}_d$ from the Gröbner basis of $\mathfrak{b} + \langle Z - y \rangle$. Let $\mathrm{Gb} = \mathsf{GroebnerBasis}(\mathfrak{b} + \langle Z - y \rangle)$ with $Z < X_n < \cdots < X_1$. If Gb is not triangular, then $\mathcal{C}_d$ is not a field. Suppose that $P(T, X_n, \ldots, X_i)$ is a polynomial in Gb such that its leading coefficient with respect to the variable X_i is another polynomial in $Z, X_n, \ldots, X_{i+1}$. Then such a leading coefficient is a zero divisor of $\mathcal{C}_d$ from which we obtain a new dynamic field where y behaves as in a field.

3.4 Examples

Example 1 This example illustrates Proposition 9. We consider $f(T) = T^6 - 3T^5 + T^4 + 10T^2 - 9T + 3$. We are computing in a Galois quotient of dimension 48. The minimal polynomial of $x_3 + x_4x_6$ factorizes into two coprime factors, $\mathrm{Min}_{x_3+x_4x_6}(T) = g_1(T)g_2(T)$. Let $y = g_1(x_3 + x_4x_6)$ be a zero divisor. So we run Algorithm 3.2 on y in Magma (see [3]) and obtain a new Galois quotient. In this case, this new Galois quotient gives the splitting field and the Galois group.

In this example, the resolvent of y has 0 as root of multiplicity 12, so 12 conjugates generate the new quotient. In practice, however, two conjugates were enough to generate it.

```
> z:=x_3 + x_4 x_6;
> g1:=Factorization(MinimalPolynomial(z))[1][1];
> y:=Evaluate(g1,y);
> Algorithm 3.2(y);

Affine Algebra of rank 6 over Rational Field
Lexicographical Order
Variables: x1, x2, x3, x4, x5, x6
Quotient relations:
[
    x1 + 8/33*x5*x6^5 - 23/33*x5*x6^4 + 1/33*x5*x6^3 - 4/33*x5*x6^2 + 32/11*x5*x6 -
```

```
        9/11*x5 - 7/33*x6^5 + 16/33*x6^4 - 5/33*x6^3 + 20/33*x6^2 - 17/11*x6 + 1/11,
    x2 - 8/33*x5*x6^5 + 23/33*x5*x6^4 - 1/33*x5*x6^3 + 4/33*x5*x6^2 - 32/11*x5*x6 +
        9/11*x5 + 8/33*x6^5 - 23/33*x6^4 + 1/33*x6^3 - 4/33*x6^2 + 32/11*x6 - 20/11,
    x3 + 7/33*x6^5 - 16/33*x6^4 + 5/33*x6^3 - 20/33*x6^2 + 17/11*x6 - 12/11,
    x4 + x5 - 8/33*x6^5 + 23/33*x6^4 - 1/33*x6^3 + 4/33*x6^2 - 21/11*x6 - 2/11,
    x5^2 - 8/33*x5*x6^5 + 23/33*x5*x6^4 - 1/33*x5*x6^3 + 4/33*x5*x6^2 - 21/11*x5*x6 -
        2/11*x5 + 31/33*x6^5 - 85/33*x6^4 + 8/33*x6^3 + 1/33*x6^2 + 102/11*x6 - 61/11,
    x6^6 - 3*x6^5 + x6^4 + 10*x6^2 - 9*x6 + 3
]

Permutation group g3 acting on a set of cardinality 6
Order = 12 = 2^2 * 3
    (1, 2)(4, 5)
    (1, 4)(2, 5)(3, 6)
    (1, 5, 3, 4, 2, 6)
```

Example 2 This example illustrates Proposition 10 and Proposition 11. We consider $f(T) = T^6 - 4T^3 + 7$. We are computing in a dynamic field, defined by a Galois quotient of dimension 72. The resolvent of

$$y = x_1x_2^2 + x_2x_3^2 + x_1^2x_3 + x_4x_5^2 + x_5x_6^2 + x_6x_4^2$$

is the cube of its minimal polynomial and the complete factorization of minimal polynomial is given by three factors,

$$\mathrm{Min}_y = R_1R_2R_3;\ \mathrm{Rv}_{G,y} = (\mathrm{Min}_y)^3,\ |\mathcal{G}_d.y| = 36.$$

We compute a zero divisor given by $y - y_j$, with $y_j \in G.y$,

$$y - y_j = 2x_3x_4x_5 - 2x_3x_4x_6 + 2x_3x_5x_6 - 2x_3x_6^2 + 2x_4x_5^2 - 2x_4x_5x_6.$$

We next run Algorithm 3.2 and obtain a new quotient of dimension 36.

```
> Factorization(MinimalPolynomial(y));
[
    <T^3 - 3*T^2 - 18*T + 48, 1>,
    <T^3 + 15*T^2 + 54*T + 48, 1>,
    <T^6 + 12*T^5 + 180*T^4 - 336*T^3 + 1872*T^2 + 1728*T + 2304, 1>
]

> C,H = Algorithm 3.2(y-y_{j});
Affine Algebra of rank 6 over Rational Field
Lexicographical Order
Variables: x1, x2, x3, x4, x5, x6
Quotient relations:
[
    x1 + 1/7*x4*x5*x6^5 - 4/7*x4*x5*x6^2,
    x2 + x4 + x6,
    x3 - 1/7*x4*x5*x6^5 + 4/7*x4*x5*x6^2 + x5,
    x4^2 + x4*x6 + x6^2,
    x5^3 + x6^3 - 4,
    x6^6 - 4*x6^3 + 7
]

Permutation group G3 acting on a set of cardinality 6
Order = 36 = 2^2 * 3^2
    (1, 4, 3, 2, 5, 6)
    (1, 2, 3, 4, 5, 6)
```

However, in this new quotient denoted by $(\mathbf{C}, H)$, we have

$$\begin{aligned} \mathrm{Rv}_{H,y} \;=\; \mathrm{Min}_{\mathbf{C},y} \;&=\; T^6 + 12T^5 - 9T^4 - 336T^3 - 396T^2 + 1728T + 2304 \\ &=\; (T^3 - 3T^2 - 18T + 48)(T^3 + 15T^2 + 54T + 48). \end{aligned}$$

The new orbit of y has 6 elements derived from 18 elements of $\mathcal{G}_d.y$. The other elements of $\mathcal{C}_d.y$ have as minimal polynomial

$$T^6 + 12T^5 + 180T^4 - 336T^3 + 1872T^2 + 1728T + 2304.$$

Finally we run again Algorithm 3.2 on $y^3-3y^2-18y+48$ and obtain a new Galois quotient that represents the splitting field and Galois group.

```
> Algorithm 3.2 (Evaluate( T^3 - 3*T^2 - 18*T + 48,y),H);

Affine Algebra of rank 6 over Rational Field
Lexicographical Order
Variables: x1, x2, x3, x4, x5, x6
Quotient relations:
[
    x1 - 1/2*x5*x6^3 + 3/2*x5,
    x2 + 1/2*x6^4 - 1/2*x6,
    x3 + 1/2*x5*x6^3 - 1/2*x5,
    x4 - 1/2*x6^4 + 3/2*x6,
    x5^3 + x6^3 - 4,
    x6^6 - 4*x6^3 + 7
]

Permutation group acting on a set of cardinality 6
Order = 18 = 2 * 3^2
    (1, 3, 5)(2, 6, 4)
    (1, 2, 3, 4, 5, 6)
```

Example 3 This example illustrates the idea of Section 3.3. Let $f(T) = T^8 - 5T^5 - 3T^4 - 5T^3 + 1$, $\mathcal{C}_d = \mathbf{A}_{\mathbb{Q},f}$, $\mathcal{G}_d = \mathrm{S}_8$ and $y = x_8x_7x_6 \in \mathcal{C}_d$. The Gröbner Basis of $\langle z - x_8x_7x_6\rangle \mathcal{C}_d$ is not triangular, has 12 polynomials, $\mathrm{Gb} = \{P_1(z, x_8, \ldots, x_1), \ldots, P_{11}(z, x_8), P_{12}(z)\}$ and provides the following information.

1. $P_{12}(z)$ is the minimal polynomial of y,
2. the leading coefficient of $P_{11}(z, x_8)$ is a zero divisor, factor of $P_{12}(z)$,
3. the leading coefficient of $P_8(z, x_8, x_7)$, equal to $x_8 - z$, is another zero divisor.

Example 4 This example shows how dynamic our methodology is. Let $f(T) = T^8 + 12T^6 + 42T^4 + 36T^2 + 4$ and the goal is to correctly compute in the splitting field of $f(T)$. So our first dynamic field is $\mathcal{C}_d = \mathbf{A}_{\mathbb{Q},f}$ joint with $\mathcal{G}_d = \mathrm{S}_8$. We consider the element $z = x_8 + x_7 \in \mathbf{A}_{\mathbb{Q},f}$ and observe that

- $25 = \mathrm{degree}(\mathrm{Min}_z(T)) < \mathrm{degree}(\mathrm{Rv}(T)) = 28$,
- z is a zero divisor.

Thus, there are two ways of proceeding.

1. We compute a zero divisor given by $z - z_j$, with $z_j \in \mathcal{G}_d.z$,

   $$z - z_j = x_8 + x_7 - x_5 - x_6.$$

   Let $y = z - z_j$. We next run Algorithm 3.2 on y and obtain a new quotient of dimension 384. In this new quotient the minimal polynomial of $-x_2 - 2x_4 - x_6$, the image of a conjugate of y, factorizes into two polynomials, so we run again Algorithm 3.2, obtaining a new quotient of dimension 128. In this new quotient, the minimal polynomial of $-x_2+x_4+x_6+x_8$, also the image of another conjugate of y, factorizes into two polynomials, so we run Algorithm 3.2 again getting a representation of the splitting field a Galois group.

2. We run Algorithm 3.2 on z and obtain a new quotient of dimension 384. In this new quotient the minimal polynomial of $-x_2 - x_8$, the image of a conjugate of z, factorizes into two polynomials, so we run again Algorithm 3.2, obtaining a new quotient of dimension 128.

   In this new quotient, z and its conjugates behave as in a field. However, we want to take advantage of all the information provided by z. Thus, we must consider the element y and see if y and its conjugates behave as in a field. The answer is not because the minimal polynomial of $x_6+x_8-x_2+x_4$ factorizes into two polynomials. Then we run Algorithm 3.2 again getting a representation of the splitting field a Galois group.

Conclusion

We conclude this paper by emphasizing the idea we have developed here. Our methodology makes it possible to compute in an exact way in the splitting field of a polynomial dynamically. We are able to take advantage of any signal which shows that our dynamic field is given (at a certain moment of the computation) by an algebra which is not a field. We improve the algebra representing the splitting field only when it is required.

As future work, it should be interesting to study what kind of oddities can happen

- when trying to make explicit the fact that the Galois correspondance has to be bijective (if our approximation is not a field, this can fail),
- when trying to compute a normal basis.

Acknowledgements

We are grateful to the anonymous referees for their careful reading of our work and their very precise suggestions to improve our presentation.

References

[1] Arnaudiés J.M. and Valibouze A., *Lagrange Resolvents.* Journal of Pure and Applied Algebra, **117 & 118**, 23–40, (1997). 10

[2] Aubry P. and Valibouze A., *Using Galois Ideals for Computing Relative Resolvents.* J. Symbolic Computation, **30**, 635–651, (2000). 6

[3] Bosma, W., Cannon, J. and Playoust, C., *The Magma Algebra System I: The User Language.* J. Symbolic Comput **24** no. 3, 235–265. (1997). URL: `magma.maths.usyd.edu.au` 1, 7, 10

[4] Bourbaki N., *Algèbre, Chapitres 4 à 7.* Masson, Paris, (1981). 3, 6

[5] Chase S., Harrison D., Rosenberg A., *Galois theory and Galois cohomology of commutative rings.* Mem. Amer. Math. Soc. **52**, 15–33, (1965). 6

[6] Drach J., *Essai sur la théorie générale de l'itération et sur la classification des transcendantes.* Ann. Sci. Ec. Norm. Sup **3** 15, 243–384, (1898). 6

[7] Della Dora J., Dicrescenzo C. and Duval D., *About a new method for computing in algebraic number fields.* In Caviness B.F. (Ed.) EUROCAL '85. Lecture Notes in Computer Science 204, 289–290, Springer (1985). 1, 2

[8] Diaz-Toca G.M., *Galois Theory, Splitting Fields and Computer Algebra.* Journal of Symbolic Computation **41**, 1174–1186, (2006). 1, 7, 9

[9] Diaz-Toca G.M., Lombardi H. and Quitté C., *Universal Decomposition Algebra.* Proceedings of Transgressive Computing 2006, 169–184, (2006). 6

[10] Ducos L., *Effectivité en théorie de Galois. Sous-résultants.* Université de Poitiers, Thèse doctorale. Poitiers (1997). 3, 6

[11] Ducos L., *Construction de corps de décomposition grâce aux facteurs de résolvantes. (French) [Construction of splitting fields in favour of resolvent factors].* Communications in Algebra **28** no. 2, 903–924, (2000). 6, 10

[12] Ekedahl E. and Laskov D., *Splitting algebras, symmetric functions and Galois Theory.* Journal of Algebra and its Applications, **4** (1), 59–76, (2005). 6

[13] Martens F., *Ein Beweis des Galois'schen Fundamentalsatzes.* Sitzungsber. der Akademie der Wissensch. in Wien, Math.-naturw. Kl. Abt. IIa, Bd. **111**, 17–37, (1902). 6

[14] Pohst M.E. and Zassenhaus H.J., *Algorithmic Algebraic Number Theory.* ISBN 0521596696. Cambridge University Press (1989). 3, 6

[15] Renault G. and Yokoyama K., *A Modular Method for Computing the Splitting Field of a Polynomial.* Lecture Notes In Computer Science **4076**. Proceedings of the 7th International Symposium on Algorithmic Number Theory, 124–140, (2006). 1

[16] Soicher, L. and McKay, J., *Computing Galois groups over the rationals.* J. Number Theory 20, 273–281, (1985). 10

[17] Stauduhar R. *The determination of Galois groups.* Math. Comp. **27**, (1973), 981–996. 9

[18] Steel A., *A New Scheme for Computing with Algebraically Closed Fields.* Lecture Notes In Computer Science **2369**. Proceedings of the 5th International Symposium on Algorithmic Number Theory, 491–505, (2002). 2

[19] Steel A., *Computing with algebraically closed fields.* Journal of Symbolic Computation. **45**, 342–372, (2010). 2

[20] Valibouze, A., *Modules de Cauchy, polynômes caractéristiques et résolvantes* . Rapport LITP, 95–62, (1995). 2

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

[22] Valibouze, A., *Classes doubles, idéaux de Galois et résolvantes.* Rev. Roumaine Math. Pures Appl. **52**, 1, 95–109 (2007). 10

[23] Vessiot E., *Sur la théorie de Galois et ses diverses généralisations.* Ann. Sci. E. N. S. 3ème série **21**, 9–85, (1904). 6

[24] Wiedemann D., *Solving sparse linear systems over finite fields.* IEEE Transactions on Information Theory, IT-32, 54-62, (1986). 10