Galois theory, splitting fields and computer algebra

Gema M. Diaz-Toca*

Departamento de Matemática Aplicada, Universidad de Murcia, Campus de Espinardo, 30071 Espinardo, Murcia, Spain

Received 26 November 2004; accepted 1 February 2005
Available online 7 September 2006

Abstract

We provide some algorithms for dynamically obtaining both a possible representation of the splitting field and the Galois group of a given separable polynomial from its universal decomposition algebra.

© 2006 Elsevier Ltd. All rights reserved.

Keywords: Universal decomposition algebra; Galois idempotents; Lazy computations; Effective Galois theory

1. Introduction

Given a polynomial, one of the main problems of Galois theory is how to obtain its Galois group and its splitting field. The research on symbolic computation (computer algebra) has yielded a large amount of programming tools which have made it possible to speak about “computationally effective Galois theory” (see for example Aubry and Valibouze (2000), Colin (1995), Ducos (1997) and Arnaudiès and Valibouze (1997)).

This article is devoted to presenting some algorithms which allow one, on the one hand, to dynamically approach the splitting field and Galois group of a polynomial from its universal decomposition algebra and, on the other hand, to compute without errors in quotient algebras of the universal decomposition algebra of the given polynomial.

Given a separable polynomial $f$ and an element $z$ in a Galois algebra intermediate between the universal decomposition algebra of $f$ and the splitting field, our goal is to obtain as much information as possible from this data. By now, we know how to compute idempotent elements as long as either the minimal polynomial of $z$ does not equal its resolvent or a factorization of the
minimal polynomial is known. It is important to emphasize that the factorization of polynomials is not necessary for applying our algorithms. Once we have found an idempotent element, we can define a new intermediate Galois algebra closer to the splitting field.

**Dynamic evaluation** was introduced in Duval (1994) for performing computations with algebraic numbers without factoring polynomials over algebraic extensions or computing primitive elements. In our setting, the splitting process in D5 is replaced by the consideration of distinct $S_n$-conjugates of $z$ inside the same Galois algebra.

In the literature, there are other algorithms which consider idempotent elements in order to approach the splitting field. For example, in Ducos (1997) we find an algorithm for building an intermediate Galois algebra but such an algorithm requires the computation and factorization of resolvent polynomials. In Aubry and Valibouze (2000), the authors study Galois ideals and resolvents and they do not consider the idempotents which generate Galois ideals.

Recall that the universal decomposition algebra of a polynomial $f$ is defined as a quotient of the polynomial ring in $n$ variables by an ideal defined by the symmetric functions in the roots of $f$. Therefore, our computing involves the use of the Gröbner basis.

The paper is organized as follows. Section 2 introduces the universal decomposition algebra. Section 3 shows the importance of Galois idempotents in such an algebra. In Section 4, the algorithms are described. Finally, the paper finishes with an example in Section 5.

### 2. Universal decomposition algebra over $\mathbb{K}$

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

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

Recall that a polynomial is separable if it has no multiple zeros in a splitting field.

Given the polynomial ring $\mathbb{K}[X_1, \ldots, X_n]$ and the ideal $\mathcal{J}(f)$ defined by

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

the universal decomposition algebra of $f(T)$, denoted by $\text{Uda}_{\mathbb{K},f}$, is defined as the following $\mathbb{K}$-algebra:

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

In this section, we present the main characteristics of this algebra. For more details see Chapter IV, pages 72–75, of Bourbaki (1990), Chapter II of Ducos (1997) and Valibouze (1995).

#### 2.1. Finite dimensional case

Observe that if $x_i$ is the residue class of $X_i \mod \mathcal{J}(f)$, then $f(T)$ totally splits over $\text{Uda}_{\mathbb{K},f}$, that is,

$$f(T) = \prod_{i=1}^{n} (T - x_i)$$
in \( \text{Uda}_{K,f} \), because of the relations between the elementary symmetric functions in the roots of \( f(T) \) and its coefficients.

If we consider the lexicographic order, with \( X_n > \cdots > X_1 \), then a Gröbner basis for \( \text{Uda}_{K,f} \) is given by the Cauchy module polynomials, defined by

\[
\begin{align*}
\hat{f}_1(X_1) &= f(X_1) \\
\hat{f}_2(X_1, X_2) &= \frac{f_1(X_1) - f_1(X_2)}{X_1 - X_2} \\
&\quad \vdots \\
\hat{f}_{k+1}(X_1, \ldots, X_{k+1}) &= \frac{f_k(X_1, \ldots, X_{k-1}, X_k) - f_k(X_1, \ldots, X_{k-1}, X_{k+1})}{X_k - X_{k+1}} \\
&\quad \vdots \\
\hat{f}_n(X_1, \ldots, X_n) &= X_n + \cdots + X_1 - a_1.
\end{align*}
\]

For example, for \( f(t) = t^6 \):

\[
\begin{align*}
\hat{f}_2(X_2, X_1) &= X_2^5 + X_2^4X_1 + X_2^3X_1^2 + X_2^2X_1^3 + X_2X_1^4 + X_1^5, \\
\hat{f}_3(X_3, X_2, X_1) &= (X_3^4 + X_2^4 + X_1^4) + (X_3^2X_2^2 + X_3^2X_1^2 + X_2^2X_1^2) \\
&\quad + (X_3X_2^3 + X_3X_1^3 + X_2X_1^3 + X_1X_3^3 + X_1X_2^3) \\
&\quad + (X_3X_2X_1^2 + X_3X_1X_2^2 + X_2X_1X_3^2), \\
\hat{f}_4(X_4, X_3, X_2, X_1) &= (X_4^4 + X_3^4 + X_2^4 + X_1^4) + (X_4X_3X_2X_1 + X_3X_2X_4X_1) \\
&\quad + X_4X_3X_1 + X_3X_2X_1 + (X_4^2X_3 + X_2 + X_1) \\
&\quad + X_3^2(X_4 + X_2 + X_1) + X_2^2(X_4 + X_3 + X_1) \\
&\quad + X_1^2(X_4 + X_3 + X_2)), \\
\hat{f}_5(X_5, X_4, X_3, X_2, X_1) &= (X_5^4 + X_4^4 + X_3^4 + X_2^4 + X_1^4) + (X_5X_4X_3X_2X_1 + X_4X_3X_2X_5 + X_5X_1X_4) \\
&\quad + X_5X_3 + X_1X_2 + X_4X_5 + X_3X_5 + X_3X_4 \\
&\quad + X_2X_5 + X_2X_4 + X_2X_3), \\
\hat{f}_6(X_6, X_5, X_4, X_3, X_2, X_1) &= X_6 + X_5 + X_4 + X_3 + X_2 + X_1.
\end{align*}
\]

Observe that the polynomial \( \hat{f}_{k+1} \) could be described as a linear combination of complete symmetric functions in \( X_1, \ldots, X_{k+1} \) whose factors are coefficients of \( f(T) \). Moreover, it is a symmetric polynomial in \( X_1, \ldots, X_{k+1} \), with leading term \( X_{n-k} \).

So, we can conclude that the algebra \( \text{Uda}_{K,f} \) is a \( \mathbb{K} \)-vector space of dimension \( n! \). In particular, a basis is given by the set of monomials \( x_1^{d_1} \cdots x_{n-1}^{d_{n-1}} \), such that \( d_k \leq n - k \) for \( k = 1, \ldots, n-1 \).
2.2. $S_n$ acting on $\text{Uda}_{\mathbb{K}, f}$

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

$$\forall P \in \mathcal{J}(f), \quad \sigma(P) \in \mathcal{J}(f), \quad \forall \sigma \in S_n.$$ 

Consequently, $S_n$ can act on $\text{Uda}_{\mathbb{K}, f}$ and actually, represents the group of the $\mathbb{K}$-automorphism of the splitting field of $f(T)$.

Moreover, under these hypotheses the following property holds in $\text{Uda}_{\mathbb{K}, f}$:

$$\sigma(a) = a, \quad \forall \sigma \in S_n \iff a \in \mathbb{K}.$$ 

2.3. Some general definitions

Let $B$ be a finite dimensional commutative algebra with identity over $\mathbb{K}$.

- The element $a$ is called separable over $\mathbb{K}$ if its minimal polynomial, denoted by $\text{Min}_a(T)$, is separable.
- The algebra $B$ is called etale if all of its elements are separable.

Recall that if $B$ is etale, then:

- Every ideal is generated by an idempotent.
- An idempotent $e$ is indecomposable if the ideal $eB$ is a minimal nonzero ideal.
- Every regular element is invertible.
- If $e$ is an indecomposable idempotent then $B/(1 - e)$ is a separable extension of $\mathbb{K}$.
- Let $A$ be the set of indecomposable idempotents of $B$. Then the canonical map from $B$ to $\prod_{e \in A} B/(1 - e)$ is an isomorphism.

(For more details about etale algebras, see Chapter V, Section 6, of Bourbaki (1990).)

Let $G$ be a group acting on $B$ and $a \in B$. Then:

- The stabilizer of $a$ is a subgroup of $G$ defined by

$$\text{St}_G(a) = \{g \in G \text{ such that } g(a) = a\}.$$ 

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

$$\text{Fix}_B(G_1) = \{a \in B \text{ such that } g(a) = a \quad \forall \ g \in G_1\}.$$ 

- If $\{a_1, \ldots, a_k\}$ is the orbit of $a$ under $G$, then the resolvent of $a$ is a polynomial in $\mathbb{K}[T]$ given by

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

Recall that if $B$ is etale then $\text{Min}_a(T)$ is the square-free part of $\text{Rv}_{G,a}(T)$. 

2.4. Separability of $\text{Uda}_{\mathbb{K}, f}$

Given a $\mathbb{K}$-algebra of finite degree, the set of its separable elements forms a $\mathbb{K}$-algebra. Thus, since $f(T)$ is separable and $\text{Uda}_{\mathbb{K}, f}$ is generated by $\{x_1, \ldots, x_n\}$, we can conclude that $\text{Uda}_{\mathbb{K}, f}$ is an etale algebra.

Moreover we have the following result.

**Proposition 2.1.** If $e \in \text{Uda}_{\mathbb{K}, f}$ is an indecomposable idempotent, then:

1. $\text{Uda}_{\mathbb{K}, f}/(1 - e) = \mathbb{L}$ is a splitting field of $f(T)$.
2. $\text{St}(e)$ acts on $\mathbb{L}$ and it is the Galois group of $f(T)$.
3. $\text{Uda}_{\mathbb{K}, f} = \bigoplus_{\sigma \in S_n/\text{St}(e)} \langle \sigma(e) \rangle \simeq \mathbb{L}^{r_{12}}$.

Thus, if we knew how to directly obtain an indecomposable idempotent, our problem would have a neat solution. Unfortunately, that is not the case. However, we have found out the way to go down by successive steps to the splitting field from the universal decomposition algebra.

3. Galois idempotents

Next we introduce the definition of a Galois idempotent.

**Definition 3.1.** A family of nonzero idempotent elements $\{r_1, \ldots, r_m\}$ in a commutative ring is a **basic system of orthogonal idempotents** if $\sum_{i=1}^{m} r_i = 1$ and $r_i r_j = 0$ for $1 \leq i < j \leq m$.

An idempotent in $\text{Uda}_{\mathbb{K}, f}$ is said to be a **Galois idempotent** when its orbit is a basic system of orthogonal idempotents.

Since the characteristic of $\mathbb{K}$ is zero, an idempotent element in $\text{Uda}_{\mathbb{K}, f}$ is a Galois idempotent if and only if the sum of its orbit equals one.

3.1. Structure theorem

An extension $E$ of $\mathbb{K}$ is said to be Galois if it is algebraic and for every $a$ in $E$ the minimal polynomial of $a$ over $\mathbb{K}$ splits in $E[T]$ into a product of distinct polynomials of degree 1. Our goal is to obtain a Galois extension from $\text{Uda}_{\mathbb{K}, f}$. The next theorem shows how to use Galois idempotents for such a purpose.

**Theorem 3.1 (Structure Theorem).** Let $e_1$ be a Galois idempotent of $\text{Uda}_{\mathbb{K}, f}$ and $G = \text{St}_{S_n}(e_1)$. Let $\{e_1, \ldots, e_k\}$ be the orbit of $e_1$ and $B_i = \text{Uda}_{\mathbb{K}, f}/(1 - e_i)$. Then

1. The idempotent $e_1$ is indecomposable if and only if $B_1$ is a field. In this case, $B_1$ is a Galois extension with $\text{Gal}(B_1/\mathbb{K}) \simeq G$.
2. The algebra $B_1$ is a $\mathbb{K}$-vector space of dimension $|G|$.
3. The algebras $B_i$ are isomorphic and $\text{Uda}_{\mathbb{K}, f} \simeq B_1^k$.
4. The group $G$ acts on $B_1$ and $\text{Fix}_{B_1}(G) = \mathbb{K}$.
5. Given $z \in B_1$, the polynomial $R_{G, z}(T)$ is in $\mathbb{K}[T]$.

Hence, given a Galois idempotent $e_1$, $(B_1/\mathbb{K}, G)$ can be understood as a better approximation of the true Galois extension ($\mathbb{L}/\mathbb{K}, \text{Gal}(f)$). If we prove that $B_1$ is a field (that means that $e_1$ is indecomposable), we will achieve our goal; otherwise, we search another Galois idempotent in $B_1$.

Recall that every quotient of an etale algebra is also etale, so $B_1$ is etale. Actually, both pairs $(\text{Uda}_{\mathbb{K}, f}/\mathbb{K}, S_n)$ and $(B_1/\mathbb{K}, \text{St}_{S_n}(e_1))$ are Galois algebras.
Definition 3.2. Let $A \subseteq B$ be two commutative rings and $G$ a finite group of automorphisms of $B$. The pair $(B/A, G)$ is said to be a Galois algebra if $\text{Fix}_B(G) = A$ and for every $\alpha \neq \text{Id}$ in $G$, 1 is in the ideal generated by the image of $\alpha - \text{Id}$.

Given a Galois algebra $(B/A, G)$, if $A$ is a field then $B$ is an etale algebra and a vector space over $A$ of dimension $|G|$.

If we extend the definitions of the basic system of orthogonal idempotents and the Galois idempotent to a Galois algebra over a field, there is a more general structure theorem.

Theorem 3.1 (bis (Structure Theorem)). Let $(B/\mathbb{F}, G)$ be a Galois algebra. Let $e_1 \in B$ be a Galois idempotent. Let $\{e_1, \ldots, e_k\}$ be the orbit of $e_1$, $C_i = B/(1 - e_i)$ and $S_i = \text{St}_G(e_i)$. Then

1. The idempotent $e_1$ is indecomposable if and only if $C_1$ is a field. In this case, $C_1$ is a Galois extension with $\text{Gal}(C_1/\mathbb{F}) \simeq S_1$.
2. The algebra $C_i$ is a $\mathbb{F}$-vector space of dimension $|S_i|$.
3. The algebras $C_i$ are isomorphic.
4. The group $S_i$ acts on $C_i$ and $\text{Fix}_{C_i}(S_i) = \mathbb{F}$.
5. Given $z \in C_i$, the polynomial $R_{V_{S_i,z}}(T)$ is in $\mathbb{F}[T]$.
6. The pair $(C_i/\mathbb{F}, S_i)$ is a Galois algebra.

Consequently, the successive computations of Galois idempotents in successive Galois algebras will allow us to approach the splitting field and Galois group in several steps.

3.2. The computation

This section introduces how to compute a Galois idempotent. In the process, we first compute an idempotent and second, a Galois idempotent.

The next theorem presents the way to compute an idempotent from a “no good” element $z$. By “no good” we mean an element in a Galois algebra $(B/\mathbb{F}, G)$ which attests that $B$ is not a field: either because $\text{Min}_z(T) \neq R_{V_{G,z}}(T)$ or because we can factorize $\text{Min}_z(T)$.

Theorem 3.2. Let $(B/\mathbb{F}, G)$ be a Galois algebra and $z \neq 0 \in B$. Then

1. $z$ is a zero divisor if and only if $\text{Min}_z(T) = TP(T)$.
2. If $\text{Min}_z(T) = P(T)K(T)$ with $P(T), K(T) \in \mathbb{F}[T]$ then $\text{gcd}(P, K) = 1$ and it is possible to compute an idempotent $\neq 0, 1$ in $B$.
3. If $\delta = \deg(\text{Min}_z(T)) < d = \deg(R_{V_{G,z}}(T))$, then it is possible to compute an idempotent $\neq 0, 1$ in $B$.

Proof.

1. If $\text{Min}_z(T) = TP(T)$ then $z$ is obviously a divisor of zero.

   Let $z$ be a divisor of zero and $\text{Min}_z(T) = TP(T) + \text{Min}_z(0)$. Then $zP(z) = -\text{Min}_z(0)$.

   If $\text{Min}_z(0) \neq 0$ then $z$ is invertible. So $zP(z) = 0$ and $P(z) \neq 0$ because $\deg(P) = \deg(\text{Min}_z) - 1$. Thus $\text{Min}_z(T) = TP(T)$. Observe that $P(0) \neq 0$ because the minimal polynomial is separable.

2. By Bezout’s identity, there are $U(T)$ and $K(T)$ verifying $P(T)U(T) + K(T)V(T) = 1$, $\deg(PU) < \deg(\text{Min}_z)$. Consider $e = P(z)U(z)$ and $f = K(z)V(z)$. Then $e + f = 1$, $e \neq 0$, $f \neq 0$ and $ef = 0$, that is, $e$ is idempotent.

   Observe that if $z$ is a zero divisor, its minimal polynomial verifies the hypothesis of this point.
(3) Let \( \{z_1 = z, \ldots, z_d\} \) be the orbit of \( z \). Let us note that there exists \( z_i \) such that \( z_i - z_i \neq 0 \) is a zero divisor.

Since \( \text{Min}_e(z_1) = 0 \), \( \text{Min}_e(T) = M_1(T)(T - z_1) \).

Since \( \text{Min}_e(z_2) = 0 \), \( \text{Min}_e(z_2) = M_1(z_2)(z_2 - z_1) \).

If \( (z_2 - z_1) \) is a divisor of zero, we are done. Otherwise, \( (z_2 - z_1) \) is invertible and \( M_1(z_2) = 0 \). Thus, \( \text{Min}_e(T) = M_2(T)(T - z_2)(T - z_1) \).

Moreover, \( e \) is a divisor of zero, we are done. Otherwise, we continue the process. Thus, either we find \( z_i - z_j \) zero divisor, with \( 1 \leq i, j, \leq \delta \), or \( \text{Min}_e(T) = (T - z_\delta) \ldots (T - z_1) \).

In this last case, since \( \text{Min}_e(z_\delta+1) = 0 \), there will be \( z_j \) such that \( z_\delta+1 - z_j \) is a zero divisor.

In both cases, we find \( z_i - z_j \) zero divisor, with \( 1 \leq i, j, \leq \delta + 1 \). Let \( \alpha \in S_n \) with \( \alpha(z_i) = z_1 \); then \( \alpha(z_i - z_j) = z_1 - z_i \) is also a zero divisor.

Now suppose that \( y = z_1 - z_i \) is a zero divisor. By (1), there exists \( a_0 \in \mathbb{K}^* \) such that

\[
\text{Min}_e(T) = T(a_0 - TB(T)) \in \mathbb{K}[T], \quad a_0 \neq 0.
\]

If \( \deg(B(T)) = 0 \) then \( B(T) = -1 \) and \( -y/a_0 \) is idempotent. Otherwise, let \( b = B(y)/a_0 \). Then:

\[
y(1 - yb) = 0 \Rightarrow y = y^2 b \Rightarrow yb = (yb)^2 \Rightarrow yb \text{ is an idempotent.} \quad \square
\]

Observe that the points (2) and (3) could be both proved using not the minimal polynomial but the resolvent. For example, if \( \text{Rv}_{S_n,z_1 - z_2}(T) = T^k(c_0 - TP(T)) \in \mathbb{K}[T] \), then \( (z_1 - z_i)P(z_1 - z_i)/c_0 \) is an idempotent \( \neq 0, 1 \).

In practice, we usually compute the minimal polynomial and the orbit of \( z \), avoiding computing the resolvent. However, suppose that we have both and the resolvent is not just a power of \( \text{Min}_e(T) \). In this case, it is possible to factorize \( \text{Min}_e(T) \) by computing the square-free decomposition of the resolvent (see Mignotte (1992)).

The next result shows how to obtain a Galois idempotent from an idempotent.

**Proposition 3.1.** Given an idempotent \( e \) in \( B \), then a Galois idempotent \( e_1 \) can be computed. Moreover, \( e_1 \) is a product of conjugates of \( e \) and \( e \) is a sum of conjugates of \( e_1 \).

**Proof.** Let

\[
\{\sigma_1(e) = e, \sigma_2(e), \ldots, \sigma_k(e)\}
\]

be the orbit of \( e \) under the action of \( S_n \). We define \( e_1 \) as

\[
e_1 = e \sigma_{1_j}(e) \ldots \sigma_{j_l}(e) \neq 0,
\]

such that for \( 1 \leq \ell \leq k \), either \( e_1 \sigma_{\ell}(e) = 0 \) or \( e_1 \). We are to prove that \( e_1 \) is a Galois idempotent. Let

\[
\mathcal{O} = \{\tau_1(e_1) = e_1, \tau_2(e_1) = e_2, \ldots, \tau_h(e_1) = e_h\}
\]

be the orbit of \( e_1 \) under the action of \( S_n \). If \( e_i e_j \neq 0, i \neq j \), then there exists \( m > 1 \) such that \( e_1 e_m \neq 0 \). However, \( e_1 e_m = 0 \) or \( e_1 \) by definition of \( e_1 \). Since \( e_m \neq e_1, e_1 e_m = 0 \).

Since \( e_{\ell} \)'s in \( \mathcal{O} \) are orthogonal idempotents, the sum

\[
e' = \sum_{\ell=1}^{h} e_{\ell}
\]

is an idempotent fixed by \( S_n \), and so in \( \mathbb{K} \). Since \( e' e_1 = e_1 \neq 0 \), we have \( e' = 1 \).
Moreover, \( ee_\ell = 0 \) or \( e_\ell \) by definition of \( e_1 \). Therefore,

\[
e = e \sum_{i=1}^{h} e_\ell = \sum_{ee_\ell \neq 0} ee_\ell \neq \sum_{ee_\ell \neq 0} e_\ell.
\]

Thus, \( e \) is sum of conjugates of \( e_1 \). \( \square \)

4. Algorithms

Given a separable and monic polynomial \( f(T) \in \mathbb{K}[T] \) and \( z \in \text{Uda}_{sn,f} \), we wonder whether it is possible to approach the splitting field with this data. The first step is to see whether \( z \) is no good and in this case, to compute a Galois idempotent by following the Fundamental Step algorithm described below.

Once we obtain a Galois idempotent, \( gi \), we see what happens in the new Galois algebra \( ((\text{Uda}_{sn,f}/(1 - gi))/\mathbb{K}, \text{St}(gi)) \) with the image of \( z \) in \( \text{Uda}_{sn,f}/(1 - gi) \). Actually, we must repeat the Fundamental Step until we find an algebra where the resolvent equals the minimal polynomial of \( z \) and we do not know any factorization.

Suppose that such an algebra is denoted by \( (\mathcal{B}/\mathbb{K}, G) \). Then \( \mathcal{B} \) provides an approximation the splitting field but we can get some more information from \( z \).

For each element in the orbit of \( z \) under \( S_n \), if its image in \( \mathcal{B} \) does not belong to the orbit of \( z \) under \( G \), we see whether it is no good. If that is the case, we obtain a new Galois idempotent in \( \mathcal{B} \) and approach the splitting field a little more. After a finite number of Fundamental Steps, we will get a Galois algebra in which the images of \( z \) and its conjugates do not provide more information.

We want to emphasize that the algorithms described here make it possible to compute without errors in the successive Galois algebras.

**Fundamental Step**

**Input:** \( f(T) \in \mathbb{K}[T], n : \deg(f), (\mathcal{B}/\mathbb{K}, G) \): Galois algebra where \( \mathcal{B} \) is a quotient algebra of \( \text{Uda}_{\mathbb{K},f}, z : \text{element in} \ \mathcal{B} \).

**Output:**

\[
\begin{cases}
(\mathcal{B}, G) & \text{if } \text{Min}_z(T) = \text{Rv}_{G,z}(T) \text{ and we do not know how to factorize } \text{Min}_z(T); \\
(\mathcal{B}/(1 - gi), \text{St}(gi)) & \text{otherwise}.
\end{cases}
\]

**Local variables:** \( e, gi, k, M \):

**Start** \( gi := 1; M := \text{Min}_z(T); \)

\[
\begin{align*}
&\text{if } M = R_1 R_2 \text{ then } e := \text{idemfact}(z, R_1, R_2); gi := \text{galois-idemp}(G, e), \\
&\quad\text{else} \\
&\quad\quad k := \#(\text{orbit}(z)), \\
&\quad\quad\text{if } \deg(M) < k \text{ then} \\
&\quad\quad\quad e := \text{idemdiv}(z, \text{orbit}(z)); \\
&\quad\quad\quad gi := \text{galois-idemp}(G, e), \\
&\quad\quad\text{end if}; \\
&\text{end if}; \\
&\text{return } (\mathcal{B}/(1 - gi), \text{St}(gi))
\end{align*}
\]

**End.**

The Fundamental Step involves the following computational steps:
Minz := procedure for obtaining minimal polynomials.

We propose the modified version of the Berlekamp–Massey algorithm presented in Benatti et al. (2006), here as Algorithm 4.1 described below. This algorithm could return either the minimal polynomial or a factor. In this latter case, we would consider other points in \( \mathbb{K}^n \) and execute again the algorithm with the same \( z \). Thus, if we obtain the minimal polynomial, we can factorize it with the factor obtained before; otherwise, we will have computed factors of the minimal polynomial and so, their least common multiple gives us another factor, closer to the minimal polynomial. That means that we can take advantage of every result obtained with Algorithm 4.1.

idemfact := procedure for obtaining idempotents from a factorization of the minimal polynomial.

The proof of Theorem 3.2, point (2), shows how to obtain an idempotent. The procedure is given by Algorithm 4.2 below.

idemdiv := procedure for obtaining idempotents when \( \text{Min}_{z}(T) \neq \text{Rv}_{G,z}(T) \).

If we do not have a factorization of \( \text{Min}_{z} \) but such a polynomial is known to be different from the resolvent, the proof of Theorem 3.2, point (3), shows how to obtain an idempotent. The procedure is given by Algorithm 4.3 below.

galois-idemp := procedure for obtaining Galois idempotents.

Once we have obtained an idempotent \( e \), the next step is to compute a Galois idempotent from \( e \) with Algorithm 4.4, following Proposition 3.1.

Algorithm 4.1 (Minimal Polynomial by Berlekamp–Massey).

Input: \( z \): element, \( G \): group, \([X_1, X_2, \ldots, X_n] \), \( n \): deg \( (f) \).

Output: \( \text{Min}_{z}(T) \)

Local variables: \( pt, k, V, p \)

Start

\[
k := \text{Length(orb}(G, z)) ; \quad pt := \text{RandomMat}(1,n)[1] ; \# \text{ point in } \mathbb{Q}^n .
\]

for \( i \) from 1 to \( 2k \) do \( V_i := \text{Value}(z^i, [X_1, X_2, \ldots, X_n], pt) \); end for;

\( p := \text{berlekamp-massey}(1, V_1, \ldots, V_{2k}) \);

return \( p \);

End.

Algorithm 4.2 (Idempotent-Factors (idemfact)).

Input: \( z \): element, \( r_1, r_2 \): factors of \( \text{Min}_{z}(T) \).

Output: idempotent;

Local variables: \( idem, Bez, f_1, pt \);

Start \( Bez := \text{GcdRepresentation}(r_1, r_2) ; \quad f_1 := Bez[1] ; \)

\( pt := r_1 \cdot f_1 ; \quad idem := \text{Value}(pt, T, z) ; \)

return \( idem \);

End.

Algorithm 4.3 (Idempotent-zero Divisor (idemdiv)).

Input: \( z, O \): orbit of \( z \);

Output: idempotent;

Local variables: \( idem, x, p, y \);

Start

for \( y \) in \( O[2, \ldots, \text{Length}(O)] \) do
\[x := z - y;\]
\[p := \text{Min}_{G,x}(T);\]
\[\text{if } \text{IsZero}(\text{Value}(p, [T], [0])) \text{ then break; end if;}\]
\[\text{end for;}\]
\[idem := \text{idemfact}(x, T, p/T);\]
\[\text{return } idem;\]
\[\text{End.}\]

Algorithm 4.4 (Galois Idempotent).

**Input:** \(G, e, I, [X_1, \ldots, X_n], n : \deg(f);\)

**Output:** Galois idempotent;

**Local variables:** \(O, t, x, gi, y, S, nv;\)

**Start**
\[O := \text{orb}(G,e,I); t := \text{Size}(O); nv := [0, \ldots, 0];\]
\[S := \sum_{x \in O} \text{Value}(x, [X_1, \ldots, X_n], nv);\]
\[gi := e;\]
\[\text{if } \text{IsZero}(S - 1) = \text{false} \text{ then}\]
\[\text{for } x \text{ in } O[2, \ldots, t] \text{ do } y := \text{normalf}(gi \cdot x, I);\]
\[\text{if } \text{IsZero}(y) = \text{false} \text{ then } gi := y; \text{ end if;}\]
\[\text{end for;}\]
\[\text{end if;}\]
\[\text{return } gi;\]
\[\text{End.}\]

All the algorithms described here have been programmed with GAP (Groups, Algorithms and Programming) and Singular. More precisely, we use GAP and its package “singular”, a GAP interface to the computer algebra system Singular for polynomial computations. These algorithms involve computing Gröbner bases in order to properly work in quotients of the polynomial ring.

As far as the complexity is concerned, it is better to consider an element \(z\) with a small number of conjugates as input because the bigger the orbit is, the more the complexity of computing increases.

Finally we state that we have only tried these algorithms with polynomials with rational coefficients, but in a future we expect to try with other fields and to find new methods in order to take advantage of all the information given by the universal decomposition algebra.

5. Example

The following example shows how the Fundamental Step is applied in order to obtain an approximation of the splitting field of \(f = X^6 - 4X^3 + 7 \in \mathbb{Q}[x].\)

\[\text{gap}> \text{Read("programme.txt");}\]
The GAP interface to Singular I Started Singular (version 2004)
\[\text{gap> gaporder} := \text{MonomialLexOrdering([x1,x2,x3,x4,x5,x6])};\]
\[\text{gap> } f := X^6 - 4X^3 + 7;\]
\[\text{gap> 1basis} := \text{modcau}(f,[x1,x2,x3,x4,x5,x6]); \#\# \text{Cauchy modules polynomials} \]
\[ x_1 + x_2 + x_3 + x_4 + x_5 + x_6, x_2^2 + x_2 x_3 + x_3 x_4 + x_5 x_6 + x_2^2 + x_4 x_5 + x_4 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + x_4 + x_5 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + x_4 + x_5 + x_5 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + x_4 + x_5 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + x_4 + x_5 + x_5 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + x_4 + x_5 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + x_4 + x_5 + x_5 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + x_4 + x_5 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + x_4 + x_5 + x_5 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + x_4 + x_5 + x_5 x_6 + x_2 x_5 + x_3 x_4 + x_3 x_5 + x_3 x_6 + \]

\( \text{gap> } 1 \text{grp} := \text{SymmetricGroup}(6);; \)

\( \text{gap> } J := \text{Ideal}(\mathbb{Q}[X_1, \ldots, X_6], 1 \text{base});; \quad \text{## Ideal in GAP} \)

\( \text{gap> } J := \text{Singula} \text{rInterface(“groebner”,J,“ideal”)}; \quad \text{## Ideal in Singular} \)

\( \text{gap> } z := \text{normalf}(x 1 \times 2^2 + x 2 \times 3^2 + x 3 \times 1^2 + x 4 \times 5^2 + x 5 \times 6^2 + x 6 \times 4^2, J);; \)

\( \text{gap> } \text{orb} := \text{orb}(1 \text{grp}, z, J);; \quad \text{## orb: procedure for obtaining the orbit of } z \)

\( \text{gap> } \text{ta} := \text{Length}(\text{orb});; \)

40

\( \text{gap> } \text{polmin} := \text{berlekamp}(z, 1, \text{grp}, 6); \)

minimal polynomial = \( X^{16} - 48 X^{15} + 1134 X^{14} + 15960 X^{13} + 123489 X^{12} + 320760 X^{11} - 3196368 X^{10} - 25956288 X^9 + 22301568 X^8 - 248838912 X^7 - 967617360 X^6 - 446777856 X^5 + 12714402816 X^4 + 3155189760 X^3 - 30636195840 X^2 - 45291405312 X - 34398535680 \); so \( z \) is a “no good” element

\( \text{gap> } \text{factors} := \text{Factors}(\text{polmin});; \)

\( \text{gap> } R1 := \text{factors}[1] \times \text{factors}[2] \times \text{factors}[3]; \quad \text{R2 := factors[4] factors[5] factors[6]};; \)

\( \text{gap> } e := \text{identfact}(z, R1, R2);; \)

\( \text{gap> } g := \text{galois-idem}(1 \text{grp}, e, J, [x_1, x_2, x_3, x_4, x_5, x_6], 6); \)

once obtained a Galois idempotent, we define a new quotient algebra and search again a new Galois idempotent

\( \text{gap> } 2 \text{grp} := \text{stab}(1 \text{grp}, \text{ig}, J);; \)

\( \text{Group([ (1,2,3,4,5,6), (2,6) ])} \)

\( \text{gap> } 2 \text{basis} := \text{ReducedGrobnerBasis(Add(1basis,1-ig),gaporder)};\)

\( \text{gap> } J := \text{Ideal}(\mathbb{Q}[X_1, \ldots, X_6], 2 \text{basis});; \)

\( \text{gap> } J := \text{SingularInterface(“groebner”,J,“ideal”)}; \)

\( \text{gap> } z := \text{normalf}(z, J);; \)
gap> orb:=orb(2grp,z,Js);;
gap> tai-orb:=Length(orb);
36

gap> polmin:=berlekamp(z,Js,tai-orb,\([x1,x2,x3,x4,x5,x6]\),6);
minimal polynomial = \(X^{12} + 24X^{11} + 315X^{10} + 1380X^9 - 8208X^8 - 36288X^7 + 70848X^6 - 145152X^5 - 1508544X^4 + 1002240X^3 + 6386688X^2 + 7962624X + 5308416\)
gap> e:=idemfact(R1,R2,z,Js);;
gap> gi:=galois-idem(2grp,e,Js,\([x1,x2,x3,x4,x5,x6]\),6);
1/21x3x4x5x6 - 1/42x3x5x6 - 1/42x4x6 + 1/6x3x5 + 1/44x4x6 + 13

Once obtained another Galois idempotent, we define a new quotient algebra and search again a new Galois idempotent

gap> 3grp:=stab(2grp,ig,Js);
Group([ (1,2,3,4,5,6), (1,3,5)(2,6,4) ])

gap> 3basis:=ReducedGroebnerBasis (Add(2basis,1-ig),gaporder);
[x6^6 - 4x6^3 + 7, x5^3 + x^3 - 4, 1/2x6^4 + x^4 - 1/2x6, -1/2x5x6^3 + x^3 + 3/2x5, -1/2x6^4 + x^2 + 3/2x6, 1/2x5x6^3 + x - 1/2x5]

gap> J:=Ideal( \(\mathbb{Q}\)[X1,\ldots,X6],3basis));;

gap> Js:=SingularInterface("groebner",[J],"ideal");;
gap> z:=normalf(z,Js);;
gap> orb:=orb(3grp,z,Js);;
gap> tai-orb:=Length(orb);
3

gap> polmin:=berlekamp(z,Js,tai-orb,\([x1,x2,x3,x4,x5,x6]\),6);
minimal polynomial = X^3 + 15X^2 + 54X + 48

Thus, we have obtained an irreducible polynomial and so our last group, Group([ (1,2,3,4,5,6), (1,3,5)(2,6,4) ]), and algebra are candidates for being the Galois group and splitting field. In fact, we know that we have obtained the right answer.

Acknowledgements

I would like to express my gratitude to the professors H. Lombardi and C. Quitte for their helpful advice. I also thank M. Costantini for his help in using GAP join with the Singular package. This work was partially supported by the Galois Theory and Explicit Methods in Arithmetic Project (HPRN-CT-2000-00114) and by the MEC grant MTM2005-08690-C02-02.
References