Dynamic Construction of the Splitting Field of a polynomial

Gema Mª Díaz-Toca
Universidad de Murcia
gemadiaz@um.es

We provide a “Dynamic Algorithm” to “dynamically” obtain both an approach of the splitting field and the Galois group of a given separable polynomial from its universal decomposition algebra. In fact, we try to answer

FIRST QUESTION: HOW TO APPROXIMATE THE SPLITTING FIELD SUCCESSFULLY ?

Let’s examine what the classical theory says about the splitting field of a separable polynomial f.

$$f(T) = T^n - a_1\,T^{n-1} + \ldots + (-1)^n a_n, \quad a_i \in \mathbb{K}$$

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

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

$$\mathcal{R} = \text{an ideal of relations of } f: \text{ maximal ideal containing } \mathcal{J}(f)$$

Then we get $(\mathbb{K}, \mathrm{Uda}_{\mathbb{K},f}, \mathrm{S}_n)$ is a Galois Algebra, $|\mathrm{S}_n| = \dim_{\mathbb{K}}(\mathrm{Uda}_{\mathbb{K},f})$,

$(\mathrm{Uda}_{\mathbb{K},f}/\mathcal{R}, \mathrm{Stab}(\mathcal{R}))$ is a realization of $(\mathrm{Split}(f), \mathrm{Gal}(f))$

Some definitions

1. A family of nonzero idempotent elements $\{r_1,\ldots,r_m\} \subset \mathrm{Uda}_{\mathbb{K},f}$ is said a **Basic System of Orthogonal Idempotents** if $\sum r_i = 1,\ r_i\,r_j = 0,\ i \neq j$.
2. An idempotent in $\mathrm{Uda}_{\mathbb{K},f}$ is said a **Galois’ idempotent** when its orbit is a Basic System of Orthogonal Idempotents.
3. An ideal $\mathcal{I} \subset \mathrm{Uda}_{\mathbb{K},f}$ is said a **Galois’ ideal** if $\mathcal{I} = \langle 1-e\rangle$, with e Galois’ idempotent.
   Hence, $\mathrm{Uda}_{\mathbb{K},f}/\mathcal{I}$ is said a **Galois’ quotient**.

Some properties

- $e \in \mathrm{Uda}_{\mathbb{K},f}$ is Galois’ idempotent $\iff$ $\exists g$ minimal idempotent, such that
  $\mathrm{Gal}(f) = \mathrm{Stab}_{\mathrm{S}_n}(g) \subseteq \mathrm{Stab}_{\mathrm{S}_n}(e),\ e = \displaystyle\sum_{\sigma \in \mathrm{Stab}_{\mathrm{S}_n}(e)/\mathrm{Stab}_{\mathrm{S}_n}(g)} \sigma\, g,$
  $\iff$ $\dim(\mathrm{Uda}_{\mathbb{K},f}/\langle 1-e\rangle) = |\mathrm{Stab}_{\mathrm{S}_n}(e)|$
- $(\mathbb{K}, \mathrm{Uda}_{\mathbb{K},f}/\mathcal{I}, \mathrm{Stab}_{\mathrm{S}_n}(e))$ is a Galois Algebra, closer to $(\mathbb{K}, \mathrm{Split}(f), \mathrm{Gal}(f))$.

ANSWER: BY GALOIS QUOTIENTS

MAP 2006, *Mathematics, Algorithms, Proofs*, Castro Urdiales, Spain

SECOND QUESTION: HOW TO GET GALOIS' IDEALS ?

Some properties

Let $(\mathbf{B}, G)$ be a Galois Algebra. Given an idempotent $e \in \mathbf{B}$, $\mathrm{Orb}_G(e) = \{e, \sigma_2(e), \ldots, \sigma_k(e)\}$. Then

$$e \text{ Galois' idempotent} \iff e\,\sigma_i(e) = \begin{cases} 0 \\ e \end{cases}$$

Idea!

Thus from $\mathrm{Orb}_G(e)$, we compute the longest non-zero product

$$e' = e \cdot \sigma_{i_2}(e) \cdots \sigma_{i_t}(e)$$

such that

$$e' \cdot \sigma_t(e) = 0 \text{ for all } t \neq i_j$$

and then e' is a Galois' idempotent.

ANSWER: BY ORBITS OF IDEMPOTENT ELEMENTS

The following algorithm provides both Galois' idempotent and its stabilizer from an idempotent.

Input: $\mathbf{B}$: Galois' quotient, $e \in \mathbf{B}$: nonzero idempotent; G: finite group; $S = \mathrm{Stab}(e)$
Output: e_1: Galois' idempotent ; H: $\mathrm{Stab}(e_1)$ s.t. $\mathbf{B}/\langle 1 - e_1 \rangle$ is a better Galois' quotient.
Local variables : $h \in \mathbf{B}$; $\sigma \in G$; $L \subseteq G$.
Start $e_1 \leftarrow e$; $L \leftarrow [\,]$;
  for σ **in** G/S **do**
# G/S denotes a list of left cosets gS for g in G.
    $h \leftarrow e_1\sigma(e)$;
    if $h \neq 0$ **then** $e_1 \leftarrow h$; $L \leftarrow L \bullet [\sigma]$ **end if**;
  end for
  $H \leftarrow$ subgroup of G defined by all α's such that: $\forall \sigma \in L$, $\alpha\sigma \in \bigcup_{\tau \in L} \tau S$.
End.

Algorithm 1: *Algorithm fo computation of a Galois Idempotent and its Stabilizer.*

THIRD QUESTION: HOW TO GET IDEMPOTENT ELEMENTS ?

Odd Elements An element $z \in \mathrm{B}$ is said "odd" if it verifies at least one of these properties:

- its minimal polynomial $\neq$ its resolvent,
- its resolvent factorizes,
- its minimal polynomial factorizes,
- it is a zero divisor.

Then, we know how to get an idempotent element from each of these "oddities".

ANSWER: BY ODDITIES

DYNAMIC ALGORITHM

Now we can say that we have a method to deal with our problem.

Given $f(T) \in \mathbb{K}[T]$, the first step is to find an"odd" element $z \in \mathrm{Uda}_{\mathbb{K},f}$.

Another point of view is the following: oddities may appear when you try to perform safe computations inside the unknown splitting field of f. When an "oddity appears", we know how to take advantage of it by improving the Galois' quotient where the "oddity" is eliminated.

When we have on oddity, we compute a Galois idempotent e', define a new Galois Algebra and see what happens here.

Thus we are able to gradually compute Galois' idempotents in order to best approximate the splitting field.

The $z's$ elements are the interactive input in our algorithm.

Undynamic Input: $f(T) \in \mathbb{K}[T],\ \mathcal{J}(f),\ \mathrm{S}_n$
Dynamic Output: $(\mathbf{B}, G)$ Galois Algebra: approximation to splitting field and Galois group.
Local variables : $e, e', \mathcal{I}, G, \mathbf{B}$
Start
$\mathbf{B} := \mathrm{Uda}_{\mathbb{K},f};\ G := \mathrm{S}_n, \mathcal{I} := \mathcal{J}.$
while we find odd elements in $\mathbf{B}$ **do**
Interactive Input: $z \in \mathbf{B}$,
if $\mathrm{odd}(z)$ **then**
$e := idempotent(z);$
$e' := galois - idempotent(e);$
$\mathcal{I} := \mathcal{I} + \langle 1 - e' \rangle;$
$G := \mathrm{Stab}_G(e');$
$\mathbf{B} := \mathbf{B}/\mathcal{I};$
end if
end while

Algorithm 2: *Dynamic Algorithm for approaching ideal of relations.*

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.

DISCUSSION

The computing of an ideal of relations of a separable polynomial is a big deal in computer algebra. Here we show how to get closer to it.

You must realize that we don't fix any numeration of roots at the beginning of the process. While the algorithm is being executed, we are getting some precision about a possible numeration of the roots (is we know a field where the roots live).

Finally, we must say that the computing in quotients of polynomial rings requires Groebner basis computations, another big task, not easy, in computer algebra.

EXAMPLE-DEGREE 7

$f(T) = T^7 - 2T^6 + 2T^5 + T^3 - 3T^2 + T - 1;$
$\mathbf{B} := \mathrm{Uda}_{\mathbb{Q},f} = \mathbb{Q}[x_1, x_2, x_3, x_4, x_5, x_6, x_7],\ G := \mathrm{S}_7,\ \mathcal{I} := \mathcal{J}(f).$

Interactive Input

$z := x_6 + x_7;$

$$\begin{aligned}\min - \mathrm{pol}(z) \ = \ & (T^7 - 4T^6 + 5T^5 - T^4 - 3T^3 + 2T^2 - 1)\cdot \\ & (T^7 - 4T^6 + 6T^5 - 5T^4 + 15T^3 - 11T^2 + 6T - 1)\cdot \\ & (T^7 - 4T^6 + 11T^5 - 14T^4 + 4T^3 + 29T^2 - 63T + 49)\end{aligned}$$

Oddities:

- Minimal polynomial factorizes.

e := idempotent(z) =

$1/11x_6^5x_7^5 - 139/781x_6^5x_7^4 - 139/781x_6^4x_7^5 + 109/781x_6^5x_7^3 + 307/781x_6^4x_7^4 + 109/781x_6^3x_7^5 - 12/781x_6^5x_7^2 - 344/781x_6^4x_7^3 - 344/781x_6^3x_7^4 - 12/781x_6^2x_7^5 + 92/781x_6^5x_7 + 81/781x_6^4x_7^2 + 383/781x_6^3x_7^3 + 81/781x_6^2x_7^4 + 92\ /781x_6x_7^5 - 182/781x_6^5 - 145/781x_6^4x_7 - 101/781x_6^3x_7^2 - 101/781x_6^2x_7^3 - 145/781x_6x_7^4 - 182/781x_7^5 + 271/781x_6^4 - 36\ /781x_6^3x_7 - 164/781x_6^2x_7^2 - 36/781x_6x_7^3 + 271/781x_7^4 - 111/781x_6^3 + 442/781x_6^2x_7 + 442/781x_6x_7^2 - 111/781x_7^3 - 314/7\ 81x_6^2 - 317/781x_6x_7 - 314/781x_7^2 - 129/781x_6 - 129/781x_7 + 644/781;$

$$G := \mathrm{Stab}_G(e') \ = \ \mathrm{Group}([(1,3,5,7,6,4,2),\ (2,3)(4,5)(6,7)]) = \mathrm{Gal}(f)$$

7T2: Transitive Group of order 14=7.2

$$\begin{aligned}\mathcal{I} + \langle \mathbf{1 - e'} \rangle \ = \ & \langle \mathbf{x_7^7 - 2x_7^6 + 2x_7^5 + x_7^3 - 3x_7^2 + x_7 - 1} \\ & \mathbf{11x_6^2 - x_6x_7^6 - 5x_6x_7^5 + 7x_6x_7^4 - 6x_6x_7^3 - 10x_6x_7^2 - x_6x_7 + 3x_6 -} \\ & \mathbf{x_7^6 + 6x_7^5 - 4x_7^4 + 5x_7^3 + x_7^2 + 10x_7 + 3,} \\ & \mathbf{11x_5 + 11x_6 - x_7^6 - 5x_7^5 + 7x_7^4 - 6x_7^3 - 10x_7^2 - x_7 + 3,} \\ & \mathbf{11x_4 - 5x_6x_7^6 + 7x_6x_7^5 - 2x_6x_7^4 - 8x_6x_7^3 - x_6x_7^2 + 13x_6x_7 + 7x_6 - 6x_7^6 +} \\ & \mathbf{10x_7^5 - 7x_7^4 - 3x_7^3 - 7x_7^2 + 22x_7 - 3,} \\ & \mathbf{11x_3 + 5x_6x_7^6 - 7x_6x_7^5 + 2x_6x_7^4 + 8x_6x_7^3 + x_6x_7^2 - 13x_6x_7 - 7x_6 - 2x_7^6 +} \\ & \mathbf{5x_7^5 - 3x_7^4 - x_7^3 + 4x_7^2 + 14x_7 - 6,} \\ & \mathbf{11x_2 + x_6x_7^6 - 3x_6x_7^5 + 5x_6x_7^4 - 5x_6x_7^3 + 6x_6x_7^2 - 9x_6x_7 + 10x_6 + 5x_7^6 -} \\ & \mathbf{7x_7^5 + 2x_7^4 + 8x_7^3 + x_7^2 - 13x_7 - 7,} \\ & \mathbf{11x_1 - x_6x_7^6 + 3x_6x_7^5 - 5x_6x_7^4 + 5x_6x_7^3 - 6x_6x_7^2 + 9x_6x_7 - 10x_6 + 4x_7^6 -} \\ & \mathbf{3x_7^5 + x_7^4 + 2x_7^3 + 12x_7^2 - 11x_7 - 9\rangle,} \\ = \ & \mathcal{R}\end{aligned}$$

1. EXAMPLE-DEGREE 8

$f(T) = T^8 - 8T^7 + 16T^6 + 16T^5 - 90T^4 + 104T^3 - 24T^2 - 32T + 16$;
$\mathbf{B} := \mathrm{Uda}_{\mathbb{Q},f} = \mathbb{Q}[x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8]$, $G := \mathrm{S}_8$, $\mathcal{I} := \mathcal{J}(f)$.

Interactive Input

$z := x_7 + x_8$;

$$\begin{aligned}\min - \mathrm{pol}(z) \;=\; & (T-2)\cdot(T^2-4T-8)\cdot(T^2-4T-4)\cdot(T^4-8T^3+20T^2-16T+8)\cdot\\ & (T^8-16T^7+88T^6-176T^5-36T^4+416T^3+112T^2-800T+100)\cdot\\ & (T^8-16T^7+88T^6-144T^5-356T^4+1696T^3-2448T^2+1440T-284)\end{aligned}$$

Oddities:

- Minimal polynomial factorizes.
- Resolvent is not equal to minimal polynomial.

e := idempotent(z) =
$-791/50784x_7^6x_8^6 + 791/8464x_7^6x_8^5 + 791/8464x_7^5x_8^6 - 1409/25392x_7^6x_8^4 - 599/1058x_7^5x_8^5 - 1409/25392x_7^4x_8^6 - 1273/3174x_7^6x_8^3 + 381/1058x_7^5x_8^4 + 381/1058x_7^4x_8^5 - 1273/3174x_7^3x_8^6 + 4713/8464x_7^6x_8^2 + 1250/529x_7^5x_8^3 - 610/1587x_7^4x_8^4 + 1250/529x_7^3x_8^5 + 4713/8464x_7^2x_8^6 - 791/12696x_7^6x_8 - 14047/4232x_7^5x_8^2 - 1600/1587x_7^4x_8^3 - 1600/1587x_7^3x_8^4 - 14047/4232x_7^2x_8^5 - 791/12696x_7x_8^6 - 2233/12696x_7^6 + 407/1058x_7^5x_8 + 7075/4232x_7^4x_8^2 - 18232/1587x_7^3x_8^3 + 7075/4232x_7^2x_8^4 + 407/1058x_7x_8^5 - 2233/12696x_8^6 + 1105/1058x_7^5 - 877/3174x_7^4x_8 + 8107/529x_7^3x_8^2 + 8107/529x_7^2x_8^3 - 877/3174x_7x_8^4 + 1105/1058x_8^5 - 790/1587x_7^4 - 2408/1587x_7^3x_8 - 88053/4232x_7^2x_8^2 - 2408/1587x_7x_8^3 - 790/1587x_8^4 - 7798/1587x_7^3 + 4621/2116x_7^2x_8 + 4621/2116x_7x_8^2 - 7798/1587x_8^3 + 14027/2116x_7^2 - 430/1587x_7x_8 + 14027/2116x_8^2 - 1082/1587x_7 - 1082/1587x_8 - 2566/1587$;

$G := \mathrm{Stab}_G(e') = \mathrm{Group}([(1,2),\ (7,8),\ (5,6),\ (4,5),\ (3,4),\ (1,7,2,8)])$; $\quad |G| = 192 = 4.4.3.2.2$

$$\begin{aligned}\mathcal{I} := \mathcal{I} + \langle 1 - e' \rangle \;=\; & \langle x_8^{\mathbf{4}} - 4x_8^3 - 4x_8^2 + 16x_8 - 8,\ x_7 + x_8^3 - 3x_8^2 - 7x_8 + 8,\\ & x_6^{\mathbf{4}} - 4x_6^3 + 4x_6^2 - 2,\\ & x_5^{\mathbf{3}} + x_5^2x_6 + x_5x_6^2 + x_6^3 - 4x_5^2 - 4x_5x_6 - 4x_6^2 + 4x_5 + 4x_6,\\ & x_4^{\mathbf{2}} + x_4x_5 + x_4x_6 + x_5^2 + x_5x_6 + x_6^2 - 4x_4 - 4x_5 - 4x_6 + 4,\\ & x_3 + x_4 + x_5 + x_6 - 4,\\ & x_2^{\mathbf{2}} - x_2x_8^3 + 3x_2x_8^2 + x_8^3 + 8x_2x_8 - 3x_8^2 - 12x_2 - 8x_8 + 12,\\ & x_1 + x_2 - x_8^3 + 3x_8^2 + 8x_8 - 12\rangle\end{aligned}$$

$\mathbf{B} := \mathbf{B}/\mathcal{I}$;

Interactive Input

$z := x_7x_6$;

$$\begin{aligned}\min - \mathrm{pol}(z) \;=\; & (T^8 - 8T^7 - 32T^6 + 32T^5 + 192T^4 - 128T^3 - 512T^2 + 512T + 256)\cdot\\ & (T^8 - 8T^7 + 224T^5 - 832T^4 + 896T^3 - 512T + 256)\end{aligned}$$

Oddities:

- Minimal polynomial factorizes.

e := idempotent(z) = $1/8x_6^2x_8^3 - 3/8x_6^2x_8^2 - 1/4x_6x_8^3 - 3/4x_6^2x_8 + 3/4x_6x_8^2 + x_6^2 + 3/2x_6x_8 - 2x_6 + 1/2$;

$$\begin{aligned}G := \mathrm{Stab}_G(e'') \;&=\; \mathrm{Group}([(1,7)(2,8),\ (4,5),\ (1,2)(3,5)(4,6)(7,8),\ (1,2)(3,4)(5,6)(7,8)])\\ &=\; \mathrm{Gal}(f) : \text{non transitive group of order 16 = 4.2.2}\end{aligned}$$

$$\begin{aligned}\mathcal{I} + \langle \mathbf{1} - \mathbf{e''} \rangle \;&=\; \langle \mathbf{x_8^{\mathbf{4}} - 4x_8^3 - 4x_8^2 + 16x_8 - 8},\ \mathbf{x_7 + x_8^3 - 3x_8^2 - 7x_8 + 8}\\ &\quad\ \mathbf{2x_6^{\mathbf{2}} + -x_8^3 + 3x_8^2 - 4x_6 + 6x_8 - 8},\\ &\quad\ \mathbf{2x_5^{\mathbf{2}} + x_8^3 - 3x_8^2 - 4x_5 - 6x_8 + 8},\\ &\quad\ \mathbf{x_4 + x_5 - 2},\ \mathbf{x_3 + x_6 - 2},\ \mathbf{x_2 - x_8^3 + 3x_8^2 + 7x_8 - 10},\ \mathbf{x_1 + x_8 - 2}\rangle\\ &=\; \mathcal{R}\end{aligned}$$

References

[1] AUBRY P., VALIBOUZE A. *Using Galois Ideals for Computing Relative Resolvents.* J. Symbolic Computation, **30**, 635–651, (2000).

[2] BISHOP E., BRIDGES D. *Constructive Analysis*. Springer-Verlag (1985).

[3] BOURBAKI *Algèbre. Chap 4 à 7*. Masson. Paris (1981).

[4] DELLA DORA J., DICRESCENZO C., 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).

[5] DEMEYER F., INGRAHAM E. *Separable algebras over commutative rings*. Springer Lecture Notes in Mathematics 181 (1971).

[6] DÍAZ TOCA G. *Galois Theory, Splitting fields and Computer Algebra*. To appear Journal of Symbolic Computation (2005).

[7] DÍAZ TOCA G., LOMBARDI H. ET QUITTÉ C. *L'algèbre de décomposition universelle*. Preprint (2005).

[8] DUCOS L. *Thèse doctorale*. Poitiers (2000).

[9] 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).

[10] GAP04-The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4; 2005. (http://www.gap-system.org).

[11] EKEDAHL E., LASKOV D. *Splitting algebras, symmetric functions ans Galois Theory.* Journal of Algebra and its Applications, **4** (1), 59–76, (2005).

[12] MINES R., RICHMAN F., RUITENBURG W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, (1988)., University of Amsterdam, Amsterdam, The Netherlands, 1994.