Dynamic Construction of the Splitting Field of a polynomial

G. Díaz-Toca - Universidad de Murcia (España)

Constructive approach to the splitting field of a separable polynomial

Consider the following situation

- $\mathbb{K}$ is a discrete field,
- $f(T) \in \mathbb{K}[T]$ is monic and separable.

Our goal

Approach dynamically a representation of the splitting field factoring as less as possible.

How

Considering the Splitting Algebra and then its Galois quotients. Using all the oddities that appear when doing dynamical computations.

Outline

Outline

The Splitting Algebra (Universal Decomposition Algebra)

Given

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

and

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

the Splitting Algebra is defined as

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

where

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

Basic properties of $\mathbf{A}_{\mathbb{K},f} = \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f)$

1. $\mathbf{A}_{\mathbb{K},f}$ is a $\mathbb{K}$–vector space of dimension n!

Basic properties of $\mathbf{A}_{\mathbb{K},f} = \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f)$

1. $\mathbf{A}_{\mathbb{K},f}$ is a $\mathbb{K}$–vector space of dimension n!
2. A basis is given by the monomials $x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}$, $d_k \leq n - k$.

Basic properties of $\mathbf{A}_{\mathbb{K},f} = \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f)$

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 $\mathrm{Fix}(\mathrm{S}_n) = \mathbb{K}$.

Basic properties of $\mathbf{A}_{\mathbb{K},f} = \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f)$

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, which implies reduced.

Basic properties of $\mathbf{A}_{\mathbb{K},f} = \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f)$

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, which implies reduced.
5. Every f.g. ideal is generated by an idempotent.

Basic properties of $\mathbf{A}_{\mathbb{K},f} = \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f)$

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, which implies reduced.
5. Every f.g. ideal is generated by an idempotent.
6. If g is an indecomposable idempotent,
   - $\mathbf{A}_{\mathbb{K},f}/(1-g) =: \mathbb{L}$ splitting field of f,
   - $\mathrm{Stabs}_{\mathrm{S}_n}(g)$ acts on $\mathbb{L}$ as Galois group of $f(T)$,
   - $\mathbf{A}_{\mathbb{K},f} = \bigoplus_{\sigma \in \mathrm{S}_n/\mathrm{Stabs}_{\mathrm{S}_n}(g)} \langle \sigma(g) \rangle \simeq \mathbb{L}^r$

Definitions - Galois Idempotents of $\mathbf{A}_{\mathbb{K},f}$

- **BSOI**.
  A Basic System of Orthogonal Idempotents (in a commutative ring R):

$$(r_i)_{1\leq i\leq n}, \quad r_i r_j = 0, \quad \sum_{i=1}^{n} r_i = 1$$

- **Galois Idempotent of $\mathbf{A}_{\mathbb{K},f}$**.
  An idempotent whose orbit is a BSOI.
- **Galois Ideal of $\mathbf{A}_{\mathbb{K},f}$**.

$$\langle 1-e\rangle = (1-e)\mathbf{A}_{\mathbb{K},f}, e \text{ Galois idempotent } .$$

- **Galois Quotient of $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$**: $(\mathbf{B}_1, G)$, where

$$\mathbf{B}_1 := \mathbf{A}_{\mathbb{K},f}/\langle 1-e\rangle, G := \mathrm{Stab}_{\mathrm{S}_n}(e), e \text{ a Galois idempotent.}$$

Definitions - Galois Idempotents of $\mathbf{A}_{\mathbb{K},f}$

- **BSOI**.
  A Basic System of Orthogonal Idempotents (in a commutative ring R):

$$(r_i)_{1\leq i\leq n}, \quad r_i r_j = 0, \quad \sum_{i=1}^{n} r_i = 1$$

- **Galois Idempotent of $\mathbf{A}_{\mathbb{K},f}$**.
  An idempotent whose orbit is a BSOI.
- **Galois Ideal of $\mathbf{A}_{\mathbb{K},f}$**.

$$\langle 1-e\rangle = (1-e)\mathbf{A}_{\mathbb{K},f}, e \text{ Galois idempotent } .$$

- **Galois Quotient of** $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$: $(\mathbf{B}_1, G)$, where

$$\mathbf{B}_1 := \mathbf{A}_{\mathbb{K},f}/\langle 1-e\rangle, G := \mathrm{Stab}_{\mathrm{S}_n}(e), e \text{ a Galois idempotent.}$$

Definitions - Galois Idempotents of $\mathbf{A}_{\mathbb{K},f}$

- **BSOI**.
  A Basic System of Orthogonal Idempotents (in a commutative ring R):

$$(r_i)_{1\leq i\leq n}, \quad r_i r_j = 0, \quad \sum_{i=1}^{n} r_i = 1$$

- **Galois Idempotent of $\mathbf{A}_{\mathbb{K},f}$**.
  An idempotent whose orbit is a BSOI.
- **Galois Ideal of $\mathbf{A}_{\mathbb{K},f}$**.

$$\langle 1-e\rangle = (1-e)\mathbf{A}_{\mathbb{K},f}, e \text{ Galois idempotent } .$$

- **Galois Quotient of $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$**: $(\mathbf{B}_1, G)$, where

$$\mathbf{B}_1 := \mathbf{A}_{\mathbb{K},f}/\langle 1-e\rangle, G := \mathrm{Stab}_{\mathrm{S}_n}(e), e \text{ a Galois idempotent.}$$

Definitions - Galois Idempotents of $\mathbf{A}_{\mathbb{K},f}$

- **BSOI**.
  A Basic System of Orthogonal Idempotents (in a commutative ring R):

$$(r_i)_{1\leq i\leq n}, \quad r_i r_j = 0, \quad \sum_{i=1}^{n} r_i = 1$$

- **Galois Idempotent of $\mathbf{A}_{\mathbb{K},f}$**.
  An idempotent whose orbit is a BSOI.
- **Galois Ideal of $\mathbf{A}_{\mathbb{K},f}$**.

$$\langle 1-e\rangle = (1-e)\mathbf{A}_{\mathbb{K},f}, e \text{ Galois idempotent .}$$

- **Galois Quotient of** $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$: $(\mathbf{B}_1, G)$, where

$$\mathbf{B}_1 := \mathbf{A}_{\mathbb{K},f}/\langle 1-e\rangle, G := \mathrm{Stab}_{\mathrm{S}_n}(e), e \text{ a Galois idempotent.}$$

Definitions - Galois Idempotents of $\mathbf{A}_{\mathbb{K},f}$

- **BSOI**.
  A Basic System of Orthogonal Idempotents (in a commutative ring R):

$$(r_i)_{1\leq i\leq n}, \quad r_i r_j = 0, \quad \sum_{i=1}^{n} r_i = 1$$

- **Galois Idempotent of $\mathbf{A}_{\mathbb{K},f}$**.
  An idempotent whose orbit is a BSOI.
- **Galois Ideal of $\mathbf{A}_{\mathbb{K},f}$**.

$$\langle 1-e\rangle = (1-e)\mathbf{A}_{\mathbb{K},f}, e \text{ Galois idempotent } .$$

- **Galois Quotient of $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$: $(\mathbf{B}_1, G)$**, where

$$\mathbf{B}_1 := \mathbf{A}_{\mathbb{K},f}/\langle 1-e\rangle, G := \mathrm{Stabs}_{\mathrm{S}_n}(e), e \text{ a Galois idempotent.}$$

Properties - Galois Idempotents

- $e \in \mathbf{A}_{\mathbb{K},f}$ is Galois Idempotent $\Leftrightarrow$ $\exists\, g$ indecomposable idempotent,

$$\mathrm{Gal}(f) = \mathrm{Stab}_{\mathrm{S}_n}(g) \subseteq \mathrm{Stab}_{\mathrm{S}_n}(e),$$

$$e = \sum_{\sigma \in \mathrm{Stab}_{\mathrm{S}_n}(e)/\mathrm{Stab}_{\mathrm{S}_n}(g)} \sigma\, g,$$

Properties - Galois Idempotents

- $e \in \mathbf{A}_{\mathbb{K},f}$ is Galois Idempotent $\Leftrightarrow$ $\exists\, g$ indecomposable idempotent,

  $$\mathrm{Gal}(f) = \mathrm{Stab}_{\mathrm{S}_n}(g) \subseteq \mathrm{Stab}_{\mathrm{S}_n}(e),$$

  $$e = \sum_{\sigma \in \mathrm{Stab}_{\mathrm{S}_n}(e)/\mathrm{Stab}_{\mathrm{S}_n}(g)} \sigma\, g,$$

- $e \in \mathbf{A}_{\mathbb{K},f}$ is Galois Idempotent $\Leftrightarrow$ $\dim(\mathbf{A}_{\mathbb{K},f} / \langle 1 - e \rangle) = |\mathrm{Stab}_{\mathrm{S}_n}(e)|$

Structure Theorem for Galois quotient $(\mathbf{B}_1, G)$ in $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$

Same properties as the universal decomposition algebra.

Structure Theorem for Galois quotient $(\mathbf{B}_1, G)$ in $(\mathbf{A}_{\mathbb{K},f}, \mathrm{S}_n)$

Same properties as the universal decomposition algebra.

1. A good $\mathbb{K}$-vector space basis (a triangular Gröbner basis)
2. $\mathbf{B}_1$ is separable, which implies reduced.
3. Every f.g. ideal is generated by an idempotent.
4. $\mathbf{B}_1$ closer to Splitting Field; G closer to Galois group.
5. If h is a Galois idempotent in $\mathbf{B}_1$, let $\mathbf{B}_2 := \mathbf{B}_1/(1-h)$, $H := \mathrm{St}(h)$, then $(\mathbf{B}_2, H)$ is a better Galois Quotient, with fixed field $\mathbb{K}$.
6. If e' is an indecomposable idempotent,
   - $\mathbf{B}_1/(1-e') =: \mathbb{L}$ splitting field of f,
   - $\mathrm{St}_G(e')$ acts on $\mathbb{L}$ as Galois group of $f(T)$,
   - $\mathbf{B}_1 = \bigoplus_{\sigma \in G/\mathrm{St}(e')} \langle \sigma(e') \rangle \simeq \mathbb{L}^m$

Outline

Dynamic constructive Galois theory – Idea

$\mathbf{A}_{\mathbb{K},f} := \mathbf{A}_{\mathbb{K},f} := \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f)$ splitting algebra;

Dynamic constructive Galois theory – Idea

$\mathbf{A}_{\mathbb{K},f} := \mathbf{A}_{\mathbb{K},f} := \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f)$ splitting algebra;

If we get a indecomposable idempotent g and compute the Groebner Basis of $\mathcal{J}(f) + < 1 - g > \Rightarrow$ well done !

Dynamic constructive Galois theory – Idea

$\mathbf{A}_{\mathbb{K},f} := \mathbf{A}_{\mathbb{K},f} := \mathbb{K}[X_1,\ldots,X_n]/\mathcal{J}(f)$ splitting algebra;

If we get a indecomposable idempotent g and compute the Groebner Basis of $\mathcal{J}(f) + < 1 - g > \Rightarrow$ well done !

:(we do not know how to compute indecomposable idempotents.

Dynamic constructive Galois theory – Idea

$\mathbf{A}_{\mathbb{K},f} := \mathbf{A}_{\mathbb{K},f} := \mathbb{K}[X_1,\ldots,X_n]/\mathcal{J}(f)$ splitting algebra;

If we get a indecomposable idempotent g and compute the Groebner Basis of $\mathcal{J}(f)+<1-g> \Rightarrow$ well done !

However,

- we dynamically obtain a family of successive Galois Idempotents

$$e_1 > e_2 > \cdots > e_t \Longleftrightarrow \langle 1-e_1\rangle \subset \langle 1-e_2\rangle \subset \ldots \subset \langle 1-e_{t-1}\rangle \subset \langle 1-e_t\rangle$$

- and Galois Quotients such that

$$\begin{array}{ccccccc}
\left(\frac{\mathbf{A}_{\mathbb{K},f}}{\langle 1-e_1\rangle}, \mathrm{St}(e_1)\right) & \rightarrow & \left(\frac{\mathbf{A}_{\mathbb{K},f}}{\langle 1-e_2\rangle}, \mathrm{St}(e_2)\right) & \rightarrow & \cdots & \rightarrow & \left(\frac{\mathbf{A}_{\mathbb{K},f}}{\langle 1-e_t\rangle}, \mathrm{St}(e_t)\right) \\
\wr\| & & \wr\| & & & & \wr\| \\
\mathbb{L}^{r_1} & \xrightarrow{r_1>r_2} & \mathbb{L}^{r_2} & \rightarrow & \cdots & \xrightarrow{r_{t-1}>r_t=1} & \mathbb{L}
\end{array}$$

Outline

How to get Galois Quotients

If

- $\mathrm{Min}_z(T)$: the minimal polynomial of z.
- $\mathrm{Rv}_z(T) = \prod_{i=1}^{k}(T - z_i)$: the resolvent of z,

then

1. Find out an "odd" element z. That is
   - neither null nor invertible (T divides $\mathrm{Min}_z(T)$).
   - $\mathrm{Min}_z(T) = R_1\, R_2$,
   - $\mathrm{Min}_z(T) \neq \mathrm{Rv}(T)$,
2. Compute an idempotent e from z.
3. Compute a Galois Idempotent e' from e.

How to get Galois Quotients

If

- $\mathrm{Min}_z(T)$: the minimal polynomial of z.
- $\mathrm{Rv}_z(T) = \prod_{i=1}^{k}(T - z_i)$: the resolvent of z,

then

1. Find out an "odd" element z. That is
   - neither null nor invertible (T divides $\mathrm{Min}_z(T)$).
   - $\mathrm{Min}_z(T) = R_1\, R_2$,
   - $\mathrm{Min}_z(T) \neq \mathrm{Rv}(T)$,
2. Compute an idempotent e from z.
3. Compute a Galois Idempotent e' from e.

How to get Galois Quotients

If

- $\mathrm{Min}_z(T)$: the minimal polynomial of z.
- $\mathrm{Rv}_z(T) = \prod_{i=1}^{k}(T - z_i)$: the resolvent of z,

then

1. Find out an "odd" element z. That is
   - neither null nor invertible (T divides $\mathrm{Min}_z(T)$).
   - $\mathrm{Min}_z(T) = R_1\, R_2$,
   - $\mathrm{Min}_z(T) \neq \mathrm{Rv}(T)$,
2. Compute an idempotent e from z.
3. Compute a Galois Idempotent e' from e.

How to get Galois Quotients

If

- $\mathrm{Min}_z(T)$: the minimal polynomial of z.
- $\mathrm{Rv}_z(T) = \prod_{i=1}^{k}(T - z_i)$: the resolvent of z,

then

1. Find out an "odd" element z. That is
   - neither null nor invertible (T divides $\mathrm{Min}_z(T)$).
   - $\mathrm{Min}_z(T) = R_1\, R_2$,
   - $\mathrm{Min}_z(T) \neq \mathrm{Rv}(T)$,
2. Compute an idempotent e from z.
3. Compute a Galois Idempotent e' from e.

Dynamic Algorithm for approaching Splitting field

Input: $f(T) \in \mathbb{K}[T],\ \mathcal{J}(f),\ \mathrm{S}_n$
Dynamic Output: $(\mathbf{B}, G)$ Galois Quotient: approximation to splitting field and Galois group.
Local variables: $e, e', \mathcal{I}, G, \mathbf{B}$
Start
$\mathbf{B} := \mathbf{A}_{\mathbb{K},f};\ G := \mathrm{S}_n, \mathcal{I} := \mathcal{J}.$
while we find odd elements in **B do**
    Interactive Input: $z \in \mathbf{B}$,
    if 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;

Example - Degree 7

Galois Group	Order	Polynomial – Relations Ideal
7T1	7	$T^7 - T^6 - 12T^5 + 7T^4 + 28T^3 - 14T^2 - 9T - 1$ 7t1
7T2	14	$T^7 - 2T^6 + 2T^5 + T^3 - 3T^2 + T - 1$ 7t2
7T3	21	$T^7 - 8T^5 - 2T^4 + 16T^3 + 6T^2 - 6T - 2$ 7t3
7T4	42	$T^7 - 3T^6 + 9T^5 - 13T^4 + 17T^3 - 10T^2 + 4T + 1$ 7t4
7T5	168	$T^7 - T^6 - 3T^5 + T^4 + 4T^3 - T^2 - T + 1$ 7t5
7T6	2520	$T^7 - 2T^6 + 4T^4 - 5T^3 + 2T - 1$ 7t6

Reference:
`http://www.mathematik.uni-kassel.de/ klueners/minimum/minimum.html`

Example - Degree 6

$$\textbf{Input} \begin{cases} f(T) = T^6 + 6T^5 + 15T^4 + 16T^3 + 3T^2 - 6T + 4; \\ \mathbf{B} := \mathbf{A}_{\mathbb{Q},f} = \mathbb{Q}[x_1, x_2, x_3, x_4, x_5, x_6],\ G := \mathrm{S}_6,\ \mathcal{I} := \mathcal{J}(f) \end{cases}$$

Example - Degree 6

$$\textbf{Input} \begin{cases} f(T) = T^6 + 6T^5 + 15T^4 + 16T^3 + 3T^2 - 6T + 4; \\ \mathbf{B} := \mathbf{A}_{\mathbb{Q},f} = \mathbb{Q}[x_1, x_2, x_3, x_4, x_5, x_6],\ G := \mathrm{S}_6,\ \mathcal{I} := \mathcal{J}(f) \end{cases}$$

Interactive Input

- $z := x_6\, x_5 + x_6\, x_4,$

Example - Degree 6

$$\textbf{Input} \begin{cases} f(T) = T^6 + 6T^5 + 15T^4 + 16T^3 + 3T^2 - 6T + 4; \\ \mathbf{B} := \mathbf{A}_{\mathbb{Q},f} = \mathbb{Q}[x_1, x_2, x_3, x_4, x_5, x_6],\ G := \mathrm{S}_6,\ \mathcal{I} := \mathcal{J}(f) \end{cases}$$

Interactive Input

- $\mathrm{Orb}(z) = \{z, \sigma_2(z), \ldots, \sigma_{60}(z)\},\ z := x_6\, x_5 + x_6\, x_4,$
- $\mathrm{Min}_z(T) = T^{60} + \ldots = (T^6 + \ldots)(T^{18} + \ldots)(T^{18} + \ldots)(T^{18} + \ldots) = f_1 \cdot f_2 \cdot f_3 \cdot f_4$

Example - Degree 6

$$\textbf{Input} \begin{cases} f(T) = T^6 + 6T^5 + 15T^4 + 16T^3 + 3T^2 - 6T + 4; \\ \mathbf{B} := \mathbf{A}_{\mathbb{Q},f} = \mathbb{Q}[x_1, x_2, x_3, x_4, x_5, x_6],\ G := \mathrm{S}_6,\ \mathcal{I} := \mathcal{J}(f) \end{cases}$$

Interactive Input

- $\mathrm{Orb}(z) = \{z, \sigma_2(z), \ldots, \sigma_{60}(z)\}$, $z := x_6\, x_5 + x_6\, x_4$,
- $\mathrm{Min}_z(T) = T^{60} + \ldots = (T^6 + \ldots)(T^{18} + \ldots)(T^{18} + \ldots)(T^{18} + \ldots) = f_1 \cdot f_2 \cdot f_3 \cdot f_4$

Let's consider z.

1. $e :=$ idempotent$(z) = \frac{1}{12} x_4^3 x_5^3 + \frac{1}{12} x_4^3 x_6^3 + \ldots$
2. $G_1 := \mathrm{Stab}_G(e') = \mathrm{Group}([(1,6),\ (1,4)(2,5)(3,6),\ (5,6)])$, $|G_1| = 72$,
3. $\mathcal{I} := \langle \mathcal{I} + \langle 1 - e' \rangle \rangle$, $\mathbf{B}_1 := \mathbf{B}/\mathcal{I}$ (new) Galois quotient .

Example - Degree 6

New Interactive Input

Example - Degree 6

New Interactive Input

- $z := \sigma_{50}(z)$,
- $\mathrm{Min}_z(T) = T^{36} + \ldots = (T^{18} + \ldots)(T^{18} + \ldots) = f_2 \cdot f_3$

Example - Degree 6

New Interactive Input

- $z := \sigma_{50}(z)$,
- $\mathrm{Min}_z(T) = T^{36} + \ldots = (T^{18} + \ldots)(T^{18} + \ldots) = f_2 \cdot f_3$

1. $e := \text{idempotent}(z) = \frac{2}{21} x_3 x_4^2 x_6^3 + \frac{2}{7} x_3 x_4^2 x_6^2 + \ldots$
2. $$\begin{aligned} G_2 := \mathrm{Stab}_{G_1}(e'') &= \mathrm{Group}([(1,4)(2,5)(3,6),\ (2,4,3),\ (1,6,5)]) \\ &= Gal(f) \end{aligned}$$
   Transitive Group of order 18
3. $\mathbf{B}_2 := \mathbf{B}_1 / \langle \mathcal{I} + \langle 1 - e'' \rangle \rangle$ representation of the splitting field.

Example - Degree 6

And if we start with a conjugate of the initial z?

Example - Degree 6, Bis

Interactive Input

Example - Degree 6, Bis

Interactive Input

- $z := \sigma_{30}(z)$, $\mathrm{Min}_z(T) = T^{60} + \ldots$

Example - Degree 6, Bis

Interactive Input

- $z := \sigma_{30}(z)$, $\mathrm{Min}_z(T) = T^{60} + \ldots$

1. $e :=$ idempotent$(z) = \frac{1}{42}x_2x_3x_4x_5x_6^5 + \frac{1}{42}x_3^2x_4x_5x_6^5 + \ldots$
2. $$\begin{aligned} G_3 := \mathrm{Stab}_G(e') &= \mathrm{Group}([(1,3)(2,6)(4,5),\ (1,4,6),\ (2,3,5)]) \\ &= Gal(f) \end{aligned}$$
   Transitive Group of order 18.
3. $\mathbf{B}_3 := \mathbf{B}/\langle \mathcal{I} + \langle 1 - e' \rangle \rangle$ representation of the splitting field.

Example - Degree 6

Example - Degree 6

We compare the two results:

- Both groups are isomorphic.
  - IsomorphismGroups(G_2 , G_3);

$$[(1,4)(2,5)(3,6),(2,4,3),(1,6,5)] \to [(1,3)(2,6)(4,5),(1,4,6),(2,3,5)]$$

- Different minimal polynomials of z

$$Min_z(T) = f_2 \,\mathbf{in}\, \mathbf{B}_2, \quad Min_z(T) = f_3 \,\mathbf{in}\, \mathbf{B}_3$$

- G.B. of Galois ideal defining $\mathbf{B}_3$ = (1,4,5)(3,2)(G.B. of Galois ideal defining $\mathbf{B}_2$)

THANK YOU !

y ¡FELIZ CUMPLEAÑOS ANDRE!