Dynamical Galois Theory and Splitting Fields

G. Díaz-Toca - Universidad de Murcia (España)
joint work with Henri Lombardi

Constructive approach to the splitting field of a separable polynomial

In this talk we consider only the following simple situation

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

Our goal

Give a constructive substitute for the "classical" splitting field, which doesn't work when there is no factorization algorithm.

Literature

Literature

- Classical
  - Tartaglia, Cardan, Lagrange, Galois, Kronecker, Artin, etc

Literature

- Classical
  - Tartaglia, Cardan, Lagrange, Galois, Kronecker, Artin, etc
- Effective Galois Theory
  - A. Valibouze, L. Ducos, Y. Eichenlaub, A. Hulpke, R. Stauduhar, etc

Literature

- Classical
  - Tartaglia, Cardan, Lagrange, Galois, Kronecker, Artin, etc
- Effective Galois Theory
  - A. Valibouze, L. Ducos, Y. Eichenlaub, A. Hulpke, R. Stauduhar, etc
- Constructive Galois Theory
  - Mines-Richman-Ruitenburg

    A course in constructive algebra

    a constructive Galois theory is developed for the case of a separably closed field $\mathbb{K}$, i.e., a field with a factorization algorithm for separable polynomials.

Literature

- Classical
  - Tartaglia, Cardan, Lagrange, Galois, Kronecker, Artin, etc
- Effective Galois Theory
  - A. Valibouze, L. Ducos, Y. Eichenlaub, A. Hulpke, R. Stauduhar, etc
- Constructive Galois Theory
  - Mines-Richman-Ruitenburg

    A course in constructive algebra

    a constructive Galois theory is developed for the case of a separably closed field $\mathbb{K}$, i.e., a field with a factorization algorithm for separable polynomials.
- Constructive and dynamic approach to the algebraic closure
  - Computer Algebra System D5

Literature

- Classical
  - Tartaglia, Cardan, Lagrange, Galois, Kronecker, Artin, etc
- Effective Galois Theory
  - A. Valibouze, L. Ducos, Y. Eichenlaub, A. Hulpke, R. Stauduhar, etc
- Constructive Galois Theory
  - Mines-Richman-Ruitenburg

    A course in constructive algebra

    a constructive Galois theory is developed for the case of a separably closed field $\mathbb{K}$, i.e., a field with a factorization algorithm for separable polynomials.
- Constructive and dynamic approach to the algebraic closure
  - Computer Algebra System D5
- The NEXT

Literature

- Classical
  - Tartaglia, Cardan, Lagrange, Galois, Kronecker, Artin, etc
- Effective Galois Theory
  - A. Valibouze, L. Ducos, Y. Eichenlaub, A. Hulpke, R. Stauduhar, etc
- Constructive Galois Theory
  - Mines-Richman-Ruitenburg

    A course in constructive algebra

    a constructive Galois theory is developed for the case of a separably closed field $\mathbb{K}$, i.e., a field with a factorization algorithm for separable polynomials.
- Constructive and dynamic approach to the algebraic closure
  - Computer Algebra System D5
- The NEXT maybe

Literature

- Classical
  - Tartaglia, Cardan, Lagrange, Galois, Kronecker, Artin, etc
- Effective Galois Theory
  - A. Valibouze, L. Ducos, Y. Eichenlaub, A. Hulpke, R. Stauduhar, etc
- Constructive Galois Theory
  - Mines-Richman-Ruitenburg

    A course in constructive algebra

    a constructive Galois theory is developed for the case of a separably closed field $\mathbb{K}$, i.e., a field with a factorization algorithm for separable polynomials.
- Constructive and dynamic approach to the algebraic closure
  - Computer Algebra System D5
- The NEXT maybe Diaz & Lombardi

Dynamic constructive Galois theory

We're trying to do something more (Galois, Galois, Galois)

- At the same time a dynamic approach of the splitting field and Galois Theory.
  - Using the symmetries of the problem.
  - Not always requiring factorization algorithm.
- Starting by considering the Universal Decomposition Algebra and then its quotients,
  - Using all the oddities that appear when doing dynamical computations (not only zero-divisors).

Main Tool: the Universal Decomposition Algebra
and its Galois quotients
(often called: the splitting algebra)

The universal decomposition algebra

Given

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

the universal decomposition algebra is defined as

$$\begin{aligned} \mathcal{J}(f) &:= \left\langle a_1 - \sum_{i=1}^n X_i, a_2 - \sum_{1\le i<j\le n} X_i X_j, \ldots, a_n - \prod_{i=1}^n X_i \right\rangle \\ \mathrm{Uda}_{\mathbb{K},f} &:= \mathbb{K}[X_1, \ldots, X_n]/\mathcal{J}(f) = \mathbb{K}[x_1, \ldots, x_n], \end{aligned}$$

where

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

A canonical basis of $\mathrm{Uda}_{\mathbb{K},f}$

- A basis is given by the monomials $x_1^{d_1} \cdots x_{n-1}^{d_{n-1}}$, $d_k \leq n-k$.
- In fact a Gröbner basis with respect to the lexicographic order, $X_1 < X_2 < \cdots < X_n$, is given by

Cauchy Modules

$$\begin{aligned}
f_1(X_1) &= f(X_1) = X_1^n + \dots \\
f_2(X_1, X_2) &= \tfrac{f_1(X_1) - f_1(X_2)}{X_1 - X_2} = X_2^{n-1} + \dots \\
&\vdots \\
f_{k+1}(X_1, \dots, X_{k+1}) &= \tfrac{f_k(X_1, \dots, X_{k-1}, X_k) - f_k(X_1, \dots, X_{k-1}, X_{k+1})}{X_k - X_{k+1}} = \\
&= X_{k+1}^{n-k} + \dots \\
&\vdots \\
f_n(X_1, \dots, X_n) &= X_n + \dots + X_1 - a_1
\end{aligned}$$

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

1. When S_n acting on $\mathbf{B}$, $\mathcal{J}(f)$ is fixed by S_n and $\mathrm{Fix}(\mathrm{S}_n) = \mathbb{K}$.

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

1. When S_n acting on $\mathbf{B}$, $\mathcal{J}(f)$ is fixed by S_n and $\mathrm{Fix}(\mathrm{S}_n) = \mathbb{K}$.
2. $\mathbf{B}$ is separable, which implies reduced.

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

1. When S_n acting on **B**, $\mathcal{J}(f)$ is fixed by S_n and $\mathrm{Fix}(\mathrm{S}_n) = \mathbb{K}$.
2. **B** is separable, which implies reduced.
3. Every f.g. ideal is generated by an idempotent.

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

1. When S_n acting on $\mathbf{B}$, $\mathcal{J}(f)$ is fixed by S_n and $\mathrm{Fix}(\mathrm{S}_n) = \mathbb{K}$.
2. $\mathbf{B}$ is separable, which implies reduced.
3. Every f.g. ideal is generated by an idempotent.
4. If g is an indecomposable idempotent,
   - $\mathbf{B}/(1-g) =: \mathbb{L}$ splitting field of f,
   - $\mathrm{Stab}_{\mathrm{S}_n}(g)$ acts on $\mathbb{L}$ as Galois group of $f(T)$,
   - $\mathbf{B} = \bigoplus_{\sigma \in \mathrm{S}_n/\mathrm{Stab}_{\mathrm{S}_n}(g)} \langle \sigma(g) \rangle \simeq \mathbb{L}^r$

Definitions - Galois quotient of $\mathbf{B} = \mathrm{Uda}_{\mathbb{K},f}$

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

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

- **Galois idempotent of B**.
  An idempotent whose orbit is a BSOI.
- **Galois ideal of B**.

$$\langle 1 - e \rangle = (1 - e)\mathbf{B}, e \text{ Galois idempotent } .$$

- **Galois quotient of** $(\mathbf{B}, \mathrm{S}_n)$: $(\mathbf{B}_1, G)$, where

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

Definitions - Galois quotient of $\mathbf{B} = \mathrm{Uda}_{\mathbb{K},f}$

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

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

- **Galois idempotent of B**.
  An idempotent whose orbit is a BSOI.
- **Galois ideal of B**.

$$\langle 1 - e \rangle = (1 - e)\mathbf{B}, e \text{ Galois idempotent }.$$

- **Galois quotient of** $(\mathbf{B}, \mathrm{S}_n)$: $(\mathbf{B}_1, G)$, where

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

Definitions - Galois quotient of $\mathbf{B} = \mathrm{Uda}_{\mathbb{K},f}$

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

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

- **Galois idempotent of B**.
  An idempotent whose orbit is a BSOI.
- **Galois ideal of B**.

$$\langle 1 - e \rangle = (1 - e)\mathbf{B}, e \text{ Galois idempotent } .$$

- **Galois quotient of** $(\mathbf{B}, \mathrm{S}_n)$: $(\mathbf{B}_1, G)$, where

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

Definitions - Galois quotient of $\mathbf{B} = \mathrm{Uda}_{\mathbb{K},f}$

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

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

- **Galois idempotent of B**.
  An idempotent whose orbit is a BSOI.
- **Galois ideal of B**.

$$\langle 1 - e \rangle = (1 - e)\mathbf{B}, e \text{ Galois idempotent }.$$

- **Galois quotient of $(\mathbf{B}, \mathrm{S}_n)$**: $(\mathbf{B}_1, G)$, where

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

Definitions - Galois quotient of $\mathbf{B} = \mathrm{Uda}_{\mathbb{K},f}$

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

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

- **Galois idempotent of B**.
  An idempotent whose orbit is a BSOI.
- **Galois ideal of B**.

$$\langle 1 - e \rangle = (1 - e)\mathbf{B}, e \text{ Galois idempotent }.$$

- **Galois quotient of $(\mathbf{B}, \mathrm{S}_n)$**: $(\mathbf{B}_1, G)$, where

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

Properties - Galois idempotents

- $$e \in \mathbf{B} \text{ is Galois' idempotent} \quad \Leftrightarrow \quad \begin{array}{l} \exists\, g \text{ indecomposable idempotent,} \\ \mathrm{Gal}(f) = \mathrm{Stab}_{\mathrm{S}_n}(g) \subseteq \mathrm{Stab}_{\mathrm{S}_n}(e), \\ e = \displaystyle\sum_{\sigma \in \mathrm{Stab}_{\mathrm{S}_n}(e)/\mathrm{Stab}_{\mathrm{S}_n}(g)} \sigma\, g, \end{array}$$

Properties - Galois idempotents

- $$e \in \mathbf{B} \text{ is Galois' idempotent} \quad \Leftrightarrow \quad \begin{array}{l} \exists\, g \text{ indecomposable idempotent,} \\ \mathrm{Gal}(f) = \mathrm{Stab}_{\mathrm{S}_n}(g) \subseteq \mathrm{Stab}_{\mathrm{S}_n}(e), \\ e = \displaystyle\sum_{\sigma \in \mathrm{Stab}_{\mathrm{S}_n}(e)/\mathrm{Stab}_{\mathrm{S}_n}(g)} \sigma\, g, \end{array}$$
- $$e \in \mathbf{B} \text{ is Galois' idempotent} \quad \Leftrightarrow \quad \dim(\mathbf{B}/\langle 1 - e \rangle) = |\mathrm{Stab}_{\mathrm{S}_n}(e)|$$

Basic properties of a Galois quotient $(\mathbf{B}_1, G)$

Same properties as the universal decomposition algebra.

1. A good $\mathbb{K}$-vector space basis (a triangular Gröbner basis)

Basic properties of a Galois quotient $(\mathbf{B}_1, G)$

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.

Basic properties of a Galois quotient $(\mathbf{B}_1, G)$

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.

Basic properties of a Galois quotient $(\mathbf{B}_1, G)$

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.

Basic properties of a Galois quotient $(\mathbf{B}_1, G)$

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 e' is an indecomposable idempotent,

Basic properties of a Galois quotient $(\mathbf{B}_1, G)$

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 e' is an indecomposable idempotent,
   - $\mathbf{B}_1/(1 - e') =: \mathbb{L}$ splitting field of f,

Basic properties of a Galois quotient $(\mathbf{B}_1, G)$

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 e' is an indecomposable idempotent,
    - $\mathbf{B}_1/(1 - e') =: \mathbb{L}$ splitting field of f,
    - $\mathrm{St}(e')$ acts on $\mathbb{L}$ as Galois group of $f(T)$,

Basic properties of a Galois quotient $(\mathbf{B}_1, G)$

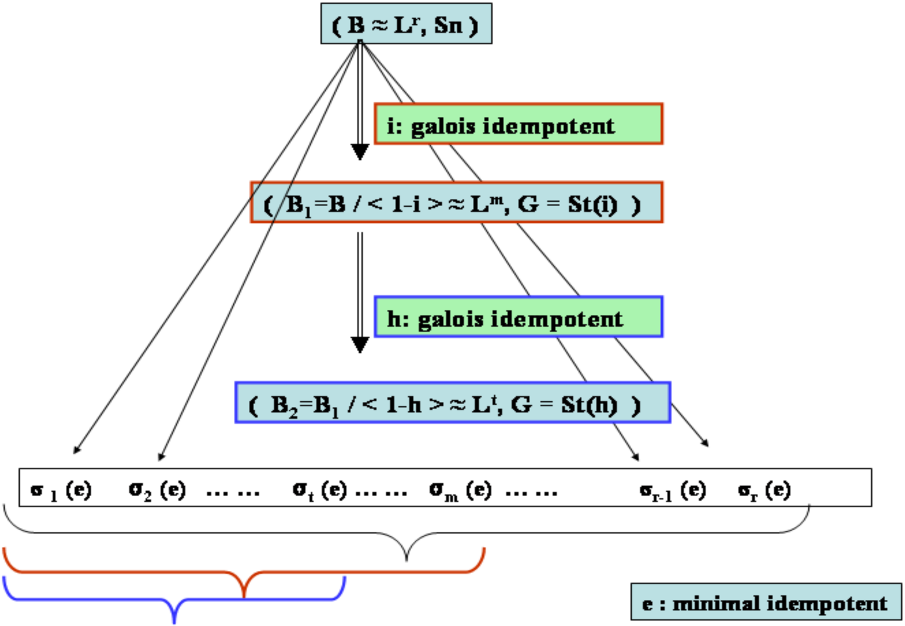
Same properties as the universal decomposition algebra.

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 e' is an indecomposable idempotent,
    - $\mathbf{B}_1/(1-e') =: \mathbb{L}$ splitting field of f,
    - $\mathrm{St}(e')$ acts on $\mathbb{L}$ as Galois group of $f(T)$,
    - $\mathbf{B}_1 = \bigoplus_{\sigma \in G/\mathrm{St}(e)} \langle \sigma(e) \rangle \simeq \mathbb{L}^m$

Basic properties of a Galois quotient $(\mathbf{B}_1, G)$

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 e' is an indecomposable idempotent,
    - $\mathbf{B}_1/(1-e') =: \mathbb{L}$ splitting field of f,
    - $\mathrm{St}(e')$ acts on $\mathbb{L}$ as Galois group of $f(T)$,
    - $\mathbf{B}_1 = \bigoplus_{\sigma \in G/\mathrm{St}(e)} \langle \sigma(e) \rangle \simeq \mathbb{L}^m$
6. 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 Galois Quotient, with fixed field $\mathbb{K}$.



(B ≈ L^r, Sn)
i: galois idempotent
(B_1=B / < 1-i > ≈ L^m, G = St(i))
h: galois idempotent
(B_2=B_1 / < 1-h > ≈ L^t, G = St(h))
σ_1 (e) σ_2 (e) … … σ_t (e) … … σ_m (e) … … σ_{r-1} (e) σ_r (e)
e : minimal idempotent

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 inversible (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 inversible (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 inversible (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 inversible (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:$f(T) \in \mathbb{K}[T]$, $\mathcal{J}(f)$, 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

$\mathbf{B} := \mathrm{Uda}_{\mathbb{K},f}$; $G := \mathrm{S}_n, \mathcal{I} := \mathcal{J}$.

while we find odd elements in **B do**

  Interactive Input: $z \in \mathbf{B}$,

  if odd (z) **then**

    $e := \mathit{idempotent}(z)$;

    $e' := \mathit{galois} - \mathit{idempotent}(e)$;

    $\mathcal{I} := \mathcal{I} + \langle 1 - e' \rangle$;

    $G := \mathrm{Stab}_G(e')$;

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

  end if;

end while;

Examples

But first let me show you how to compute an idempotent from z in the examples.

$$\mathrm{Min}_z(T) = p_1(T) \cdot p_2(T),\ \gcd(p_1, p_2) = 1$$

$$\Downarrow$$

$$1 = p_1(T)q_1(T) + p_2(T)q_2(T)$$

$$\Downarrow$$

$$e := \mathrm{idempotent}(p_1, z) = p_1(z)q_1(z)$$

$$\Downarrow$$

$$e' := e\,\sigma_1(e)\,\ldots\,\sigma_t(e) \text{ nonzero maximal product of conjugates of } e$$

$$\langle 1 - e' \rangle : \text{Galois ideal}$$

Example - Degree 7

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

Example - Degree 7

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

Interactive Input

Example - Degree 7

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

Interactive Input

$$\begin{aligned} z &= x_6 + x_7 \\ \mathrm{Min}_z(T) &= (T^7 - 4T^6 + 5T^5 - T^4 - 3T^3 + 2T^2 - 1)\cdot \\ &\quad (T^7 - 4T^6 + 6T^5 - 5T^4 + 15T^3 - 11T^2 + 6T - 1)\cdot \\ &\quad (T^7 - 4T^6 + 11T^5 - 14T^4 + 4T^3 + 29T^2 - 63T + 49) \\ &= f_1 \cdot f_2 \cdot f_3 \end{aligned}$$

Example - Degree 7

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

Interactive Input

$$\begin{aligned} z &= x_6 + x_7 \\ \mathrm{Min}_z(T) &= (T^7 - 4T^6 + 5T^5 - T^4 - 3T^3 + 2T^2 - 1)\cdot \\ &\quad (T^7 - 4T^6 + 6T^5 - 5T^4 + 15T^3 - 11T^2 + 6T - 1)\cdot \\ &\quad (T^7 - 4T^6 + 11T^5 - 14T^4 + 4T^3 + 29T^2 - 63T + 49) \\ &= f_1 \cdot f_2 \cdot f_3 \end{aligned}$$

1. $e := \text{idempotent}(f_1 \cdot f_3, z) = \frac{1}{11} x_6^5 x_7^5 - \frac{139}{781} x_6^5 x_7^4 - \frac{139}{781} x_6^4 x_7^5 + \ldots$
2. $$\begin{aligned} G := \mathrm{Stab}_G(e') &= \mathrm{Group}([(1,3,5,7,6,4,2),\ (2,3)(4,5)(6,7)]) = Gal(f) \\ &\quad \text{7T2: Transitive Group of order } 14 = 7.2 \end{aligned}$$
3. $\mathbf{B}/\langle \mathcal{I} + \langle 1 - e' \rangle \rangle$ representation of the splitting field.

Example - Degree 7

$\mathcal{I} + \langle 1 - e' \rangle =$
$\langle x_7^7 - 2x_7^6 + 2x_7^5 + x_7^3 - 3x_7^2 + x_7 - 1$

$11x_6^2 - x_6x_7^6 - 5x_6x_7^5 + 7x_6x_7^4 - 6x_6x_7^3 - 10x_6x_7^2 - x_6x_7 + 3x_6 -$
$x_7^6 + 6x_7^5 - 4x_7^4 + 5x_7^3 + x_7^2 + 10x_7 + 3,$

$11x_5 + 11x_6 - x_7^6 - 5x_7^5 + 7x_7^4 - 6x_7^3 - 10x_7^2 - x_7 + 3,$

$11x_4 - 5x_6x_7^6 + 7x_6x_7^5 - 2x_6x_7^4 - 8x_6x_7^3 - x_6x_7^2 + 13x_6x_7 + 7x_6 - 6x_7^6 +$
$10x_7^5 - 7x_7^4 - 3x_7^3 - 7x_7^2 + 22x_7 - 3,$

$11x_3 + 5x_6x_7^6 - 7x_6x_7^5 + 2x_6x_7^4 + 8x_6x_7^3 + x_6x_7^2 - 13x_6x_7 - 7x_6 - 2x_7^6 +$
$5x_7^5 - 3x_7^4 - x_7^3 + 4x_7^2 + 14x_7 - 6,$

$11x_2 + x_6x_7^6 - 3x_6x_7^5 + 5x_6x_7^4 - 5x_6x_7^3 + 6x_6x_7^2 - 9x_6x_7 + 10x_6 + 5x_7^6 -$
$7x_7^5 + 2x_7^4 + 8x_7^3 + x_7^2 - 13x_7 - 7,$

$11x_1 - x_6x_7^6 + 3x_6x_7^5 - 5x_6x_7^4 + 5x_6x_7^3 - 6x_6x_7^2 + 9x_6x_7 - 10x_6 + 4x_7^6 -$
$3x_7^5 + x_7^4 + 2x_7^3 + 12x_7^2 - 11x_7 - 9\rangle,$

Example - Degree 6

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

Example - Degree 6

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

Interactive Input

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

Example - Degree 6

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

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

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

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$(f_1, z) = \frac{1}{12} x_4^3 x_5^3 + \frac{1}{12} x_4^3 x_6^3 + \ldots$
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. $e :=$ idempotent$(f_2, z) = \frac{2}{21} x_3 x_4^2 x_6^3 + \frac{2}{7} x_3 x_4^2 x_6^2 + \ldots$
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

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

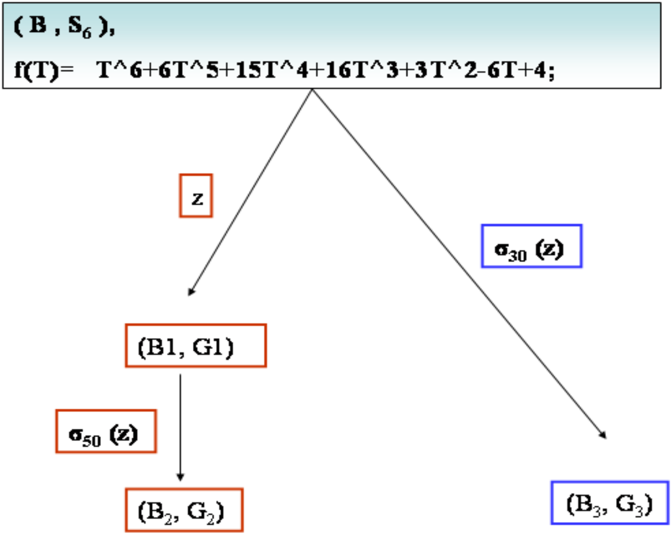
Example - Degree 6, Bis

Interactive Input

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

1. $e :=$ idempotent$(f_2, z) = \frac{1}{42} x_2 x_3 x_4 x_5 x_6^5 + \frac{1}{42} x_3^2 x_4 x_5 x_6^5 + \dots$
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);

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

- 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 $\mathbf{B}_2$)

In the future

1. $\mathbb{K} \neq \mathbb{Q}$.
2. How to identify a field?
3. What about the choice of z?
4. MAGMA
5. How to take advantages of Group Theory?

In the future

1. $\mathbb{K} \neq \mathbb{Q}$.
2. How to identify a field?
3. What about the choice of z?
4. MAGMA
5. How to take advantages of Group Theory?

THANK YOU