Part I

Introduction
Let \( f \in \mathbb{Z}[x] \) be a monic irreducible polynomial with degree \( n \) and \( \alpha = \{\alpha_1, \ldots, \alpha_n\} \) a set of its roots.

**Aim**

Compute a representation of \( \mathbb{Q}_f = \mathbb{Q}(\alpha) \) the Splitting Field of \( f \).

This corresponds to the normal closure of the number field defined by the polynomial \( f \).
Representations of The Splitting Field of a Polynomial

Representation of \( \mathbb{Q}_f \): as a **simple extension** of degree \( N = |G| \) (the Galois groupe of \( f \) is \( G \))

\[ \Rightarrow \text{Representation of the roots needs polynomials of degree } N \]

Representation of \( \mathbb{Q}_f \): as a **tower of extensions** defined by the quotient algebra

\[ \mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I} \]

where \( \mathcal{I} \) is the **splitting ideal** defined by

The kernel of the valuation map in \( \alpha \)

\[ \mathcal{I} = \{ R \in \mathbb{Q}[x_1, \ldots, x_n] \mid R(\alpha) = 0 \} \]

\[ \Rightarrow \text{Recursive definition of the roots} \]

(Note: \( \mathcal{I} \) depends on the numbering of the roots \( \alpha \))
Representations of The Splitting Field of a Polynomial

Representation of $\mathbb{Q}_f$ as a tower of extensions

$$g_n = x_n^{d_n} + r_n(x_1, \ldots, x_n)$$
$$g_{n-1} = x_{n-1}^{d_{n-1}} + r_{n-1}(x_1, \ldots, x_{n-1})$$
$$g_1 = f(x_1)$$
Computations in this Quotient Algebra

The ideal $\mathcal{I}$ is generated by the following triangular set $\mathcal{T}$

\[ g_1(x_1) = x_1^{d_1} + r_1(x_1) \quad \text{deg}_{x_1}(r_1) < d_1 \]
\[ g_2(x_1, x_2) = x_2^{d_2} + r_2(x_1, x_2) \quad \text{deg}_{x_2}(r_2) < d_2 \]
\[ \ldots \]
\[ g_n(x_1, \ldots, x_n) = x_n^{d_n} + r(x_1, \ldots, x_n) \quad \text{deg}_{x_n}(r_n) < d_n \]

\[ g_i(\alpha_1, \ldots, \alpha_{i-1}, x_i) \]

minimal polynomial of $\alpha_i$ over $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$.

Gröbner basis (LEX $x_1 < x_2 < \ldots < x_n$) $\Rightarrow$ computations $\mathbb{Q}[x_1, \ldots, x_n]/\mathcal{I}$. 

SD10 LORIA, Nancy – Guénaël Renault
The Galois Group in this Representation

The \( \mathbb{Q} \)-automorphism group of \( \mathbb{Q}_f \) can be represented by a subgroup \( G_f \) of \( S_n \), the Galois group of \( f \):

\[
\mathbb{Q}_f = \mathbb{Q}(\alpha) \quad \longrightarrow \quad \mathbb{Q}_f = \mathbb{Q}(\alpha)
\]

\[
\alpha_i \quad \longrightarrow \quad \alpha_j
\]

The permutation group \( G_f \) stabilizes the ideal \( \mathcal{I} \):

\[
G_f = \{ \sigma \in S_n \mid \forall R \in \mathcal{I}, \sigma \cdot R := R(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \in \mathcal{I} \}
\]

(Note: \( G_f \) depends on the numbering of the roots \( \alpha \))
Computation of the Set $\mathcal{T}$

Direct methods
- Successive factorizations (Kronecker-Tchebotarev method)
- Resolvents computations (Arnaudiès, Aubry, Ducos, Valibouze ...)

$\Rightarrow$ We can compute $G_f$ from $\mathcal{T}$

Driven methods

$\Rightarrow$ Very efficient implementation for the computation of the $G_f$ action over $\alpha$ (Magma, Kash).

Problematic

How to use the knowledge of $G_f$ in order to efficiently compute $\mathcal{T}$?
Computation of the Set $\mathcal{I}$

**Driven methods**

⇒ Interpolation method, the action of $G_f$ over $p$-adic approximations of $\alpha$ is known [Yokoyama 97][Lederer 05]: generic

⇒ [R., Yokoyama ANTS’06]: Interpolation based on linear algebra with a careful treatment on reducing computational difficulty (computation scheme).

⇒ [R., Yokoyama ISSAC’08]: Linear algebra $\rightarrow$ Lagrange Formulae and multi-modular strategy.
Part II

Computation Scheme
The generic shape of $g_i$’s and $\mathcal{T}$

From the knowledge of $G_f$ we obtain:

$$Q(\alpha_1, \ldots, \alpha_n) \xrightarrow{\text{Stab}_{G_f[1, \ldots, i]} \leftarrow} Q(\alpha_1, \ldots, \alpha_i) \xrightarrow{\text{Stab}_{G_f[1, \ldots, i-1]}} Q(\alpha_1, \ldots, \alpha_{i-1})$$

$$g_i = x_i^{d_i} + r_i(x_1, \ldots, x_i)$$

$$g_1 = f(x_1)$$
The generic shape of $g_i$’s and $\mathcal{T}$

From the knowledge of $G_f$ we obtain:

$$d_i = \frac{|\text{Stab}_{G_f}([1, \ldots, i - 1])|}{|\text{Stab}_{G_f}([1, \ldots, i])|}.$$ 

↓

$$g_i = x_i^{d_i} + \sum_{0 \leq k_j < d_j} c x_1^{k_1} x_2^{k_2} \cdots x_i^{k_i}$$

With this generic shape, there are $d_1 d_2 \cdots d_i$ indeterminate coefficients to compute for identifying $g_i$ ([Yokoyama 97], [Lederer 05]).

$\mathcal{T}$ contains $n$ polynomials with $\sim |G_f|$ indeterminate coefficients.
The principle of the computation scheme

⇒ [R., Yokoyama ANTS’06] [R. ISSAC’06]

Definition

Be given a permutation group \( G \), a **computation scheme** consists of a pre-computed data that guides the computation of the splitting field of a polynomial with Galois group \( G \).

- reducing the number of indeterminates to compute
- reducing the number of polynomials to compute

⇒ \( c(G) \) will denote the number of coefficients to compute in \( T \)
Sparse shape of \( g_i \)

**i-relation**

\[
E = \{ e_1 < \ldots < e_s < i \} \subset \{ 1, \ldots, i \}
\]

\[
\exists r_i \in \mathbb{Q}[x_{e_1}, \ldots, x_{e_s}, x_i] : \quad \alpha_i^{d_i} + r_i(\alpha) = 0 \text{ and } \deg_{x_i}(r_i) < d_i
\]

\( i \)-relations with minimal \( D(E) \) ⇒ minimal number of coefficients for \( g_i \).
Avoiding some computations

Techniques

From a polynomial \( g \in \mathcal{T} \) already computed it is possible to deduce a new one by using the knowledge of \( G_f \):

- By action of \( G_f \) over \( g \) (Transporter technique)
- By \textit{divided differences} of \( g \) (generalized Cauchy moduls)
Avoiding some computations: \((i, j)\)-transporters

\[ E_i = \{ e_1 < e_2 < \cdots < e_s = i \} \] is an \(i\)-relation and \(j \in \{ i + 1, \ldots, n \} \).

**Definition**

\[ \sigma \in G_f \text{ is a (}i, j\text{)-transporter if } d_i = d_j \text{ and } \]

\[ \sigma(i) = j \text{ with } j = \max(\{ \sigma(e) : e \in E_i \}) \]

\[
\begin{cases}
    g_1 = x_1^{d_1} + \ldots \\
    \vdots \\
    g_i(X_{E_i}) = x_i^{d_i} + r(X_{E_i}) \\
    \vdots \\
    g_j = x_j^{d_j} + \ldots = \sigma.g_i \\
    \vdots 
\end{cases}
\]
Avoiding some computations: Cauchy moduls

Let $O = \{i_1 = i < i_2 < \cdots < i_{d_i}\}$ be the orbit of $i$ under the action of $\text{Stab}_{G_f}([1, \ldots, i - 1])$.

Definition

The generalized Cauchy moduls of $g_i$ are

\[
\begin{align*}
c_1(g_i)(\ldots, x_{i_1}) &= g_i \\
c_2(g_i)(\ldots, x_{i_2}) &= \frac{c_1(g_i)(x_{i_2}) - c_1(g_i)(x_{i_1})}{(x_{i_2} - x_{i_1})} \\
& \vdots \\
c_{d_i}(g_i)(\ldots, x_{i_{d_i}}) &= \frac{c_{d_i-1}(g_i)(x_{i_{d_i}}) - c_{d_i-1}(g_i)(x_{i_{d_i-1}})}{(x_{i_{d_i}} - x_{i_{d_i-1}})}
\end{align*}
\]

$c_j(g_i) \in \mathbb{Q}[x_1, \ldots, x_j] \cap \mathcal{I}$ monic in $x_j$ and $\text{deg}_j(c_j(g_i)) = d_i - j + 1$. $c_j(g_i)(\alpha, x_j)$ is a univariate polynomial which vanishes on $\alpha_{ij}$. 
Avoiding some computations: Cauchy moduls

\[ c_j(g_i) \in \mathbb{Q}[x_1, \ldots, x_{ij}] \cap \mathcal{I} \text{ monic in } x_{ij} \text{ and } \deg_j(c_j(g_i)) = d_i - j + 1. \]

\[ c_j(g_i)(\alpha, x_{ij}) \text{ is a univariate polynomial which vanishes on } \alpha_{ij}. \]

\[ \begin{align*}
  g_1 &= x_1^{d_1} + \ldots \\
  \vdots \\
  g_i &= x_i^{d_i} + \ldots \\
  \vdots \\
  g_j &= x_j^{d_j} + \ldots \\
  \vdots 
\end{align*} \]
Conclusion

Given $G_f$ we can obtain a sparse shape for each polynomial $g_i$ or a technique to obtain it without computation:

1: Compute $d_i$.
2: Search for generalized Cauchy moduls.
3: Search for a transporter.
4: If necessary, compute an $i$-relation $E_i$ with minimal $D(E_i)$.

We denote by $c(G_f) = \sum D(E_i)$ the total number of indeterminate coefficients of polynomials in $\mathcal{T}$ we have to compute.

- The integer $c(G_f)$ is not an invariant for a conjugacy class.
- A representative with minimal $c$-size can be pre-computed and stored with its attached computation scheme.
Example: \( G_2 \simeq 8T_{44} \simeq [2^4]S_4, \quad |G_2| = 384, \text{ imprimitive} \)

\[ G_2 = \langle (2, 1), (8, 6, 4, 1)(7, 5, 3, 2), (8, 1)(7, 2) \rangle \]

\begin{align*}
E_2 &= \{2, 1\} \\
D(E_2) &\quad \text{Transporters} \\
\text{Cauchy} &\quad \left\{ \begin{align*}
g_1 &= x_1^8 + \ldots \\
g_2 &= x_2^1 + \ldots \\
g_3 &= x_3^6 + \ldots \\
g_4 &= x_4^1 + \ldots \\
g_5 &= x_5^4 + \ldots \\
g_6 &= x_6^1 + \ldots \\
g_7 &= x_7^2 + \ldots \\
g_8 &= x_8^1 + \ldots 
\end{align*} \right. \\
c(G_2) &= 8
\end{align*}
Example: \( G_2 \simeq 8T_{44} \simeq [2^4]S_4, |G_2| = 384, \) imprimitive

\[ G_2 = \langle (2, 1), (8, 6, 4, 1)(7, 5, 3, 2), (8, 1)(7, 2) \rangle \]

\[
\begin{align*}
g_1 &= x_1^8 + \ldots & 8 \\
g_2 &= x_2^1 + \ldots & 8 \\
g_3 &= x_3^6 + \ldots & 8x6 \\
g_4 &= x_4^1 + \ldots & 8x6 \\
g_5 &= x_5^4 + \ldots & 8x6x4 \\
g_6 &= x_6^1 + \ldots & 8x6x4 \\
g_7 &= x_7^2 + \ldots & 8x6x4x2 \\
g_8 &= x_8^1 + \ldots & 8x6x4x2
\end{align*}
\]
Part III

Modular method for computing $\mathcal{T}$
Computation of a candidate: inputs

⇒ From the knowledge of $G_f$ we know a computation scheme, thus a subset

$$S := \{g_{i_1}, \ldots, g_{i_k}\} \subset T$$

of polynomials to compute and techniques for obtaining the others.

⇒ To $g$ in $S$ corresponds an $i$-relation $E = \{e_1 < e_2 < \cdots < e_s = i\}$:

$$g = x_i^{d_i} + r(x_{e_1}, x_{e_2}, \ldots, x_i)$$

D(E) indeterminate coefficients to compute
Computation of a candidate: interpolation

From the action of $G_f$ over $\alpha \mod p^k$ ([Yokoyama 97], [Geissler, Klüners 00]) we can reconstruct $g \mod p^k$ by interpolation.

[ R., Yokoyama ANTS’06]:

- $g(\beta) = 0 \mod p^k, \forall \beta \in G_f \cdot \alpha \Rightarrow D(E)$ linear equations

\[
\begin{pmatrix}
D(E)^2 \\
\end{pmatrix}
\]

$D(E) = d_{e_1} d_{e_2} \cdots d_i$
Computation of a candidate: interpolation

From the action of $G_f$ over $\alpha \mod p^k$ ([Yokoyama 97], [Geissler, Klüners 00]) we can reconstruct $g \mod p^k$ by interpolation.

[ R., Yokoyama ISSAC’08]:

- We can directly apply [Dahan, Schost 04] on sub-triangular set,
- and the formula can be established by Galois theory

\[
g = \sum_{\sigma \in G_f/\text{Stab}_Gf(E_i \setminus \{i\})} \left( \prod_{j \in E_i \setminus \{i\}} \prod_{\beta \in B(\sigma,j,E_i)} \frac{x_j - \beta}{\alpha \sigma(j) - \beta} \right) \prod_{\beta \in B(\sigma,i,E_i)} \frac{x_i - \beta}{\alpha \sigma(i) - \beta}
\]
Correctness test

⇒ After rational reconstruction, how to check the result?

**Theoretical Bounds**: ([Lederer 05] for a generic shape of ideal $\mathcal{T}$).

\[
d(E_i) \left( \frac{d_1 - 1}{k_1} \right)^\nu d_1^{-1-k_1} \ldots \left( \frac{d_s}{k_s} \right)^\nu d_s^{-k_s} \mathbb{B}.
\]

where $\nu$ and $\mathbb{B}$ are bounds computed from numerical app. roots of $f$

**Normal Form Computation**: Let $h_i$ be the rational reconstruction of $g_i$ mod $p^k$. Assume that $g_1, \ldots, g_{i-1}$ are already computed.

**Theorem**. We have the following equivalence

\[
h_i = g_i \iff NF_{\{g_1, \ldots, g_{i-1}, h_i\}}(\text{CauchyMod}_i(f)) = 0.
\]
First comparisons

**Complexity:** Interpolation based on lin. algebra $c(G) \omega \rightarrow$ Lagrange formulae $c(G)^2$.

**Experiments:** Magma 2.14-13 (1.5GHz Intel Pentium 4, GNU/Linux), $k = 10$, $f$ splits completely modulo $p$. All timings in seconds.

<table>
<thead>
<tr>
<th>group</th>
<th>gen.</th>
<th>$c(G)$</th>
<th>Lagrange</th>
<th>NF</th>
<th>Total</th>
<th>Magma</th>
<th>Lederer</th>
</tr>
</thead>
<tbody>
<tr>
<td>$7T_6$</td>
<td>3611</td>
<td>1260</td>
<td>47.5</td>
<td>3.04</td>
<td>52.5</td>
<td>&gt;</td>
<td>1508.3</td>
</tr>
<tr>
<td>$8T_{32}$</td>
<td>624</td>
<td>96 + 96</td>
<td>0.55</td>
<td>0.14</td>
<td>0.72</td>
<td>33.5</td>
<td>12.5</td>
</tr>
<tr>
<td>$8T_{42}$</td>
<td>1008</td>
<td>24 + 24</td>
<td>0.05</td>
<td>0.02</td>
<td>0.1</td>
<td>17.9</td>
<td>20.08</td>
</tr>
<tr>
<td>$8T_{47}$</td>
<td>1008</td>
<td>24</td>
<td>0.03</td>
<td>0.0</td>
<td>0.5</td>
<td>422.3</td>
<td>238.3</td>
</tr>
<tr>
<td>$9T_{25}$</td>
<td>828</td>
<td>27 + 324</td>
<td>3.41</td>
<td>0.33</td>
<td>3.77</td>
<td>106.1</td>
<td>67.9</td>
</tr>
<tr>
<td>$9T_{27}$</td>
<td>3096</td>
<td>504</td>
<td>7.98</td>
<td>105.49</td>
<td>116.3</td>
<td>&gt;</td>
<td>397.3</td>
</tr>
<tr>
<td>$9T_{31}$</td>
<td>2178</td>
<td>18</td>
<td>0.01</td>
<td>0.03</td>
<td>0.5</td>
<td>&gt;</td>
<td>403.3</td>
</tr>
<tr>
<td>$9T_{32}$</td>
<td>9648</td>
<td>1512 + 1512</td>
<td>142.17</td>
<td>752.4</td>
<td>905.4</td>
<td>&gt;&gt;</td>
<td>1967.1</td>
</tr>
</tbody>
</table>

$(> , >>)$: we wait at least (600, 2000) seconds
Part IV

Conclusion
KASH/KANT : Galois action over $p$-adic approximations of the roots $\alpha$
GAP : Computation Scheme
Singular : Multivariate polynomials and normal forms computations

⇒ This algorithm could be easily implemented in SAGE.