Constructive Galois Theory
Computation of Galois groups: degree 24 and beyond

Jürgen Klüners

Universität Paderborn

8th Nov 2014 / Barcelona
Fundamental theorem of Galois theory

\[ \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \]
\[ \mathbb{Q}(\beta_1) \]
\[ \mathbb{Q}(\alpha_1) \]
\[ \mathbb{Q} \]

\( G \) permutes the zeros \( \alpha_1, \ldots, \alpha_n \) of the minimal polynomial \( f \in \mathbb{Z}[x] \) of \( \alpha_1 \).

The subgroups of \( G \) are in bijection to the subfields of \( \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \).

**Discriminant criterion**

\[ G \leq A_n \iff \text{Disc}(f) = (-1)^{n(n-1)/2} \text{Res}(f, f') = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \] is a square in \( \mathbb{Z} \).

For \( n = 3 \) this gives an algorithm to compute Galois groups.
Fundamental theorem of Galois theory

\begin{equation}
\mathbb{Q}(\alpha_1, \ldots, \alpha_n) \quad \{\text{id}\} \quad \mathbb{Q}(\beta_1) \quad H
\end{equation}

$G$ permutes the zeros $\alpha_1, \ldots, \alpha_n$ of the minimal polyn. $f \in \mathbb{Z}[x]$ of $\alpha_1$. The subgroups of $G$ are in bijection to the subfields of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

**Discriminant criterion**

\begin{equation}
G \leq A_n \iff \text{Disc}(f) = (-1)^{n(n-1)/2} \text{Res}(f, f') = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \text{ is a square in } \mathbb{Z}.
\end{equation}

For $n = 3$ this gives an algorithm to compute Galois groups.
Setup

- $f \in \mathbb{Z}[x]$ square-free and monic
- $\alpha_1, \ldots, \alpha_n$ roots of $f$ in some field
- $\Gamma := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ splitting field.

Then $G := \text{Aut}(\Gamma/\mathbb{Q}) \leq \text{Sym}(\alpha_1, \ldots, \alpha_n) \sim S_n$ is the Galois group of $f$.

**Aim:** To compute $G$.

**Note:** This is more than just the structure of $G$ or the conjugacy class.
The trivial approach

The construction of a generic splitting field by factorization already gives a method for the computation of \( G \).

Example

\[ f(x) := x^4 - 3 \in \mathbb{Q}[x] \text{ (which is irreducible)}. \]

Set \( K_1 := \mathbb{Q}(\alpha) \sim \mathbb{Q}[x]/\langle f \rangle \).

Factorize \( f \) over \( K_1 \):

\[ f = (x - \alpha)(x + \alpha)(x^2 + \alpha^2). \]

Next we adjoin a root of the quadratic factor to \( K_1 \):

\[ K_2 := K_1(\beta) \sim K_1[x]/\langle x^2 + \alpha^2 \rangle. \]
Example $f(x) = x^4 - 3$ continued

- $K_1 := \mathbb{Q}(\alpha) \sim \mathbb{Q}[x]/\langle f \rangle$.
- $f = (x - \alpha)(x + \alpha)(x^2 + \alpha^2) \in K_1[x]$.
- $K_2 := K_1(\beta) \sim K_1[x]/\langle x^2 + \alpha^2 \rangle$.

**Splitting field $\Gamma := K_2 = \mathbb{Q}(\alpha, \beta)$**

- $G = \text{Gal}(f)$ acts on the roots $\pm \alpha$ and $\pm \beta$.
- There is only one transitive subgroup of the $\text{Sym}(4)$ of order 8.
- The Galois group is $D_4$ - but how does $G$ act on the roots?

As a permutation group acting on $(\alpha, -\alpha, \beta, -\beta)$, $G$ is generated by $(1, 4, 2, 3)$ and $(1, 4)(2, 3)$. 
Some useful tools

Cycle types, $p \nmid \text{Disc}(f)$ and $f \equiv f_1 \ldots f_r \mod p\mathbb{Z}[x]$

$\text{Gal}(f)$ contains an element $\pi$ of cycle type $(\deg(f_1), \ldots, \deg(f_r))$. If $G = S_n$, this will determined quickly.

Resolvent method

$$F_m(x) := \prod_{1 \leq i_1 < \ldots < i_m \leq n} (x - (\alpha_{i_1} + \ldots \alpha_{i_m})) \in \mathbb{Z}[x].$$

If $F_m$ is squarefree, then the degrees of the factors of $F_m$ coincide with the orbit lengths of the operation of $\text{Gal}(f)$ on the $m$-sets. $F_m$ can be computed only using the coefficients.
Problems and history

Problems

- Computation of splitting fields not efficient, degree might be $n!$.
- How to represent the roots of $f$?

- Stauduhar, 1973, method up to degree 7
- Geyer, 1992, degree 9
- Eichenlaub, Olivier, 1995, degree 11
- Geißler, 1997, degree 12, still using complex approximations
- Geißler, Klüners, 2000, degree 15, $p$-adic approximations
- Geißler, 2003, degree 23

Current implementation in Magma

- Fieker-Klüners (without degree restriction)
- Many improvements by Stephan Elsenhans (invariant theory)
The Stauduhar algorithm I

Goal

Compute Galois groups including the action on the roots

Idea

- Situation: \( \text{Gal}(f) \leq G, H < G \) maximal subgroup.
- Decide, if \( \text{Gal}(f) \leq H^\tau \) for a \( \tau \in G//H \).
- Here \( \text{Gal}(f) \) operates on the zeros \( \alpha_1, \ldots, \alpha_n \) of \( f \).
Relative invariants

- Compute $F \in \mathbb{Z}[x_1, \ldots, x_n]$ with $F^H = F$ (pointwise) and $F^g \neq F \ \forall g \in G \setminus H$.
- Therefore $R_{G,H,F}(x) := \prod_{\tau \in G/\!\!/H} (x - F^\tau(\alpha_1, \ldots, \alpha_n)) \in \mathbb{Z}[x]$.

Main theorem of Stauduhar

Let $R_{G,H,F}(x)$ be squarefree. Then: $\text{Gal}(f) \leq H^\tau \iff F^\tau(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. 
Problems

- Computation of maximal subgroups up to conjugation.
- Computation of the invariants.
  - Special invariants (wreath products, index-2-subgroups, ...).
  - Example: \( \prod_{1 \leq j < k \leq n} (x_j - x_k) \) is \( A_n \)-invariant, \( S_n \)-relative.
- Representation of \( \alpha_1, \ldots, \alpha_n \) (\( \rightarrow p \)-adic approximation).
- Decide, if \( F^\tau(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z} \).
- Large indices (\( G : H \)) (e.g. 40 million in degree 13,14).
  - Computation of \( G/\!/H \).
  - \( p \)-adic Precision is \( p^k > (2M)^{(G:H)} \).
Maximal transitive subgroups of $S_n$ and $A_n$:

$(S_{14} : 14T_{61}) = 1716$ \hspace{1cm} $(A_{14} : 14T_{59}^+) = 3432$

$(S_{14} : 14T_{57}) = 135135$ \hspace{1cm} $(A_{14} : 14T_{55}^+) = 270270$

$(S_{14} : 14T_{39}) = 39916800$ \hspace{1cm} $(A_{14} : 14T_{30}^+) = 39916800$

$(S_{15} : 15T_{102}) = 126126$ \hspace{1cm} $(A_{15} : 15T_{99}^+) = 126126$

$(S_{15} : 15T_{93}) = 1401400$ \hspace{1cm} $(A_{15} : 15T_{89}^+) = 1401400$

$(S_{15} : 15T_{82}) = 32432400$ \hspace{1cm} $(A_{15} : 15T_{72}^+) = 32432400$

$(S_{23} : AGL(1, 23)) = 21!$ \hspace{1cm} $(A_{23} : M_{23}) = 1.267.136.462.592.000$
Unramified $p$-adic extensions

- $p 
mid \text{Disc}(f)$ be a prime number and $f \equiv f_1 \ldots f_r \mod p$.
- Then $\bar{\alpha}_1, \ldots, \bar{\alpha}_n \subset \mathbb{F}_q$, where $q = p^\ell$ with $\ell := \text{lcm}(\deg(f_i))$.
- $E := \{ \sum_{i=n_0}^{\infty} a_i p^i \mid a_i \in \mathbb{F}_q, n_0 \in \mathbb{Z} \}$ is unramified over $\mathbb{Q}_p$.
- $\alpha_1, \ldots, \alpha_n \in o_E = \{ \sum_{i=0}^{\infty} a_i p^i \mid a_i \in \mathbb{F}_q \}$.
- Modulo $p^k$-approximation: $\sum_{i=0}^{k-1} a_i p^i$.

When is a number in $\mathbb{Z}$?

Is 1.0000000000001 an integer or perhaps 1.57?

$\mathbb{Z} \subset \mathbb{Z}_p \subset \mathbb{Q}_p \subset E$.

Easy observation: If $a \in E \setminus \mathbb{Q}_p \Rightarrow a \notin \mathbb{Z}$. 
How can we prove that $a \in \mathbb{Z}$?

**Situation**

$a \equiv b \mod p^k$ and $|a| < M$ with $p^k > 2M$.

Choose $b$ in the symmetric residue system $\left\{ \frac{-(p^k-1)}{2}, \ldots, \frac{p^k-1}{2} \right\}$.

If $|b| > M$, then $a \notin \mathbb{Z}$.

If $|b| < M$, then: If $a \in \mathbb{Z}$, then $a = b$.

**Theorem**

Let $M \in \mathbb{R}$ with $|F^\sigma(\alpha_1, \ldots, \alpha_n)| < M \ \forall \sigma \in S_n$ and $p^k > (2M)^{(G:H)}$.

Then:

$F^\tau(\alpha_1, \ldots, \alpha_n) = b \in \mathbb{Z} \iff F^\tau(\alpha_1, \ldots, \alpha_n) \equiv b \mod p^k$ and $|b| < M$.

**Proof:**

$R_{G,H,F}(x) = \prod_{\sigma \in G//H} (x - F^\sigma(\alpha_1, \ldots, \alpha_n)) \in \mathbb{Z}[x]$.

Then: $R_{G,H,F}(b) < (2M)^{(G:H)}$ and congruent to 0 modulo $p^k$. 
Subfields

Computation of non-trivial subfields

- gives smaller starting group.
- avoids the most difficult descents.

Subfield computation is more efficient than Galois group computation. (My PhD-thesis, 1997).

Generating Subfields, joint with Mark van Hoeij, Andrew Novocin, 2013

- Determination of all generating subfields in polynomial time (degree, size of coefficient).
- All subfields can be computed as intersections of those (linear in the number of subfields).
**Definition**

∅ ≠ Δ ⊆ Ω is called block, if Δ^τ ∩ Δ ∈ {∅, Δ} for all τ ∈ G. The orbit Δ_1, ..., Δ_m of a block Δ_1 of G is called block system.

**Lemma**

Assume that \text{Gal}(f) has a block Δ of size d. Then \text{Gal}(f) ≤ S_d \wr S_m.
Subfields III

Problem

**Determine** \( \text{Gal}(f) \leq S_d \wr S_m \) **including the operation on** \( \alpha_1, \ldots, \alpha_n \).

- \( L = \mathbb{Q}(\beta_1) \subset K = \mathbb{Q}(\alpha_1), \beta_1, \ldots, \beta_m \) are the conjugates of \( \beta_1 \).
- Then there exists an \( h \in \mathbb{Q}[x] \) with \( h(\alpha_1) = \beta_1 \).
- We have \( h(\alpha_i) = \beta_j \) for some \( 1 \leq j \leq m \).

Lemma

**Define** \( \Delta_j := \{ \alpha_i \mid h(\alpha_i) = \beta_j \} \). **Then** \( \Delta_1, \ldots, \Delta_m \) is a block system corresponding to \( L \).

This gives an improvement for imprimitive Galois groups.
Short Cosets

1. Is \( \text{Gal}(f) \leq \tau H \tau^{-1} \) for a \( \tau \in G//H \)?
2. Known: Frobenius–automorphism \( \sigma \in \text{Gal}(f) \) with \( \sigma(\alpha_i) \equiv \alpha_i^p \mod p \).
3. \( (G//H)_\sigma := \{ \tau \in G//H \mid \sigma \in \tau H \tau^{-1} \} \), explicitly computable via centralizer computation.

Example

\[ H := 14 T_{39}^+ \cong \text{PGL}_2(13) < G := S_{14}, \ (G : H) = 39.916.800 \]

Choose \( \sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14) \) and we get \( |(G//H)_\sigma| = 1 \).
Short Cosets

- Is $\text{Gal}(f) \leq \tau H \tau^{-1}$ for a $\tau \in G/H$?
- Known: Frobenius–automorphism $\sigma \in \text{Gal}(f)$ with $\sigma(\alpha_i) \equiv \alpha_i^p \mod p$.
- $(G//H)_\sigma := \{ \tau \in G//H \mid \sigma \in \tau H \tau^{-1} \}$,
- explicitly computable via centralizer computation.

Example

$H := 14 T_{39}^+ \cong PGL_2(13) < G := S_{14}, \ (G : H) = 39.916.800$
Choose $\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14)$ and we get $|(G//H)_\sigma| = 1$. 
Proof for primitive groups

Problem:

\[(G/H)_\sigma \text{ small, but } p^k > (2M)^{(G:H)}.\]

Choose \(k\) with \(p^k > (2M)^{10}\) and get \(\text{Gal}(f) = H\) incl. operation on the roots with "high probability".

Is \(\text{Gal}(f) = H\) or \(\text{Gal}(f) = G\), where \(H < G\)?

Proof using the so-called resolvent method.
Implementations
with Claus Fieker

Algorithm for arbitrary degree

- over $\mathbb{Q}$, other ground fields in Magma
- Complete rewrite!
- Maximal subgroups computation (already done in magma)
- Computation of special invariants (big improvements by Stephan Elsenhans)
- Choosing a good prime (for short cosets, cheap arithmetic)
- Many new problems in higher degrees, e.g. computation of conjugacy classes for big 2-groups
Reminder: $H < G$ maximal subgroup, compute:

$F \in \mathbb{Z}[x_1, \ldots, x_n]$ with $F^H = F$ (pointwise) and $F^g \neq F \; \forall g \in G \setminus H$.

If $(G : H)$ is small, then $G$ and $H$ are almost equal.

Other interpretation:

$F$ is a primitive element of the field extension

$$\mathbb{Q}(x_1, \ldots, x_n)^H / \mathbb{Q}(x_1, \ldots, x_n)^G.$$ 

Example

$H_1, H_2, H_3$ 3 subgroups of $G$ of index 2 with $H_1 \cap H_2 \subset H_3 \subset G$. Then determine invariant $F_3$ from invariants $F_1$ and $F_2$. If done properly, we get $F_3 = F_1 F_2$. 

Special invariants – block systems

$H$ has a block system

$$\{x_1, \ldots, x_d\}, \ldots, \{x_{(m-1)d+1}, \ldots, x_n\},$$

which is not a block system of $G$. Then:

$$F(x_1, \ldots, x_n) := (x_1 + \ldots + x_d) \cdots (x_{(m-1)d+1} + \ldots + x_n)$$

$\Delta_1, \ldots, \Delta_m$ block system of $H$ and $G$

- $\tilde{H}, \tilde{G}$ operation of $H$ and $G$, resp., on $\Delta_1, \ldots, \Delta_m$. If $\tilde{H} \subsetneq \tilde{G}$, then $
\tilde{H}$–invariant $\tilde{F}(y_1, \ldots, y_m)$ produces $F(x_1, \ldots, x_n) = \tilde{F}(x_1 + \ldots + x_d, \ldots, x_{(m-1)d+1} + \ldots + x_n)$.

- Analogue reduction, if operation within the blocks is different.
Special invariants – wreath products

Idea:

Generalization of discriminant criterion: $G = S_d \wr S_m$.

$$d_k := \prod_{1 \leq i < j \leq d} (x_{i,k} - x_{j,k}), \quad (1 \leq k \leq m)$$

$s_k$ elementary symmetric polynomials $(1 \leq k \leq m)$

$$D := \prod_{1 \leq i < j \leq m} (y_i - y_j) \text{ with } y_j = x_{(j-1)d+1} + \ldots + x_{jd}$$

Lemma

$S_d \wr S_m$ has at least 3 subgroups of index 2, i.e. the stabilizers of $s_m(d_1, \ldots, d_m), D(y_1, \ldots, y_m)$ (this is $S_d \wr A_m$) and $D(y_1, \ldots, y_m)s_m(d_1, \ldots, d_m)$. 
Explicit realization of transitive groups of small degree

Problem $G \leq S_n$ transitive

Compute a polynomial $f \in \mathbb{Q}[x]$ with $\text{Gal}(f) = G$.

Known theoretical results

- All solvable groups over $\mathbb{Q}$ are realizable.
- $S_n$, $A_n$, all abelian groups, and all sporadic groups with the possible exception $M_{23}$ are realizable over $\mathbb{Q}$ (and regularly over $\mathbb{Q}(t)$).

<table>
<thead>
<tr>
<th>degree</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>16</td>
<td>7</td>
<td>50</td>
<td>34</td>
<td>45</td>
<td>8</td>
<td>301</td>
<td>9</td>
<td>63</td>
<td>104</td>
<td>1954</td>
</tr>
</tbody>
</table>
Results

Theorem (Klüners-Malle, 2000)

All transitive groups up to degree 15 are regularly realizable over $\mathbb{Q}(t)$.

Theorem (Klüners-Malle, 2000)

For all transitive groups up to degree 15 we have computed a polynomial $f \in \mathbb{Q}[x]$ with $\text{Gal}(f) = G$.

Current progress: Realizations over $\mathbb{Q}$

Degree 16: All 1954 groups are realized
Degree 17: All groups, but $L_2(16) : 2$ ($L_2(16)$ realized by J. Bosman)
Degree 18: All 983 groups over $\mathbb{Q}$ realized
Degree 19-23 All groups (except $M_{23}$) over $\mathbb{Q}$ realized
Construction methods

- Compute polynomial for other permutation representation or quotient
- Direct products $A \times H$
- Wreath products $A \wr H$ of $A$ with $H$.
- Split extensions $A \rtimes H$ with abelian kernel $A$
- Subdirect products (fiber products)
- Rigidity and generalizations
- Class field theory

Inductive reduction to smaller groups

Let $H \triangleleft G$ and $A \trianglelefteq G$ abelian with $G = AH$. Then $G$ is quotient of $A \rtimes H$. 
Irreducible non semiabelian groups

Definition

$G$ is called **irreducible non semiabelian**, if there exists no subgroup $H \leq G$ with $G = AH$ for some abelian normal subgroup $A$.

<table>
<thead>
<tr>
<th>12 (23)</th>
<th>13 (3)</th>
<th>14 (13)</th>
<th>15 (18)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12T57</td>
<td>$L_3(3)$</td>
<td>$L_2(13)$</td>
<td>$A_5 \wr 3$</td>
</tr>
<tr>
<td>12T124</td>
<td>14T33</td>
<td></td>
<td>15T94</td>
</tr>
<tr>
<td>$PGL_2(11)$</td>
<td>$PGL_2(13)$</td>
<td></td>
<td>15T95</td>
</tr>
<tr>
<td>12T287</td>
<td>$L_2(7) \wr 2$</td>
<td></td>
<td>$A_5 \wr S_3$</td>
</tr>
<tr>
<td>$M_{12}$</td>
<td></td>
<td>$A_7 \wr 2$</td>
<td>15T97-100</td>
</tr>
<tr>
<td>$A_6 \wr 2$</td>
<td>14T59</td>
<td></td>
<td>$S_5 \wr 3$</td>
</tr>
<tr>
<td>12T297-298</td>
<td>14T60</td>
<td></td>
<td>$S_5 \wr S_3$</td>
</tr>
<tr>
<td>$S_6 \wr 2$</td>
<td></td>
<td>$S_7 \wr 2$</td>
<td></td>
</tr>
</tbody>
</table>

Critical groups are: 12T57, 12T124, 14T33.
Goal of the database

- Compute a polynomial for each group and signature (Number of real roots).
- Determine the number field with the smallest discriminant for each entry.

Web address
galoisdb.math.uni-paderborn.de

Theorem (Serre)

*All groups are realizable over \( \mathbb{Q} \) ⇔ all groups are realizable over \( \mathbb{Q} \) with a totally real polynomial.*
Missing entries

Missing entries for signatures up to degree 15
totally real: $L_2(13)$, $PGL_2(13)$

- Emmanuel Hallouine: $9T_{27} = L_2(8)$ and $9T_{32} = PGL_2(8)$.
- Joachim König: $PGL_2(11)$, $L_3(3)$.
Complete up to degree 7
Complete in degree 8 for imprimitive groups
Many groups in degrees 9-12

**Minima**

<table>
<thead>
<tr>
<th>$G$</th>
<th>$r_1$</th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$8T_{25}$</td>
<td>594823321</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>9745585291264</td>
</tr>
<tr>
<td>$8T_{36}$</td>
<td>1817487424</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>6423507767296</td>
</tr>
<tr>
<td>$8T_{37}$</td>
<td>$\leq 37822859361$</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>$\leq 235163942523136$</td>
</tr>
<tr>
<td>$8T_{43}$</td>
<td>$\leq 418195493$</td>
<td>$\geq -1997331875$</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>$\leq 312349488740352$</td>
</tr>
<tr>
<td>$8T_{48}$</td>
<td>$\leq 32684089$</td>
<td>—</td>
<td>$\leq 293471161$</td>
<td>—</td>
<td>—</td>
<td>$\leq 81366421504$</td>
</tr>
<tr>
<td>$8T_{49}$</td>
<td>$\leq 20912329$</td>
<td>—</td>
<td>$\leq 144889369$</td>
<td>—</td>
<td>—</td>
<td>$\leq 46664208361$</td>
</tr>
<tr>
<td>$8T_{50}$</td>
<td>$\leq 1282789$</td>
<td>$\geq -4296211$</td>
<td>$\leq 15908237$</td>
<td>$\geq -65106259$</td>
<td>—</td>
<td>483345053</td>
</tr>
</tbody>
</table>
Thank you very much for your attention

Web address of the database
galoisdb.math.uni-paderborn.de