Algorithmic aspects of Galois theory in recent times

Michael F. Singer

Department of Mathematics
North Carolina State University
Raleigh, NC 27695-8205
singer@math.ncsu.edu

Bicentenaire de la naissance d'Évariste Galois

l'Institut Henri Poincaré, 28 Octobre 2011

Calculating Galois groups . . . in theory

Calculating Galois groups . . . in theory

Calculating Galois groups . . . in practice

Calculating Galois groups . . . in theory

Calculating Galois groups . . . in practice

Calculating *Differential* Galois groups

Calculating Galois groups in theory

Calculating Galois groups in theory

Can we calculate Galois groups?

Calculating Galois groups in theory

Can we calculate Galois groups?

Yes we can, but ....

An Algorithm

(Kronecker, *Gründzuge . . .* , Crelle, 92, 1882)

An Algorithm

(Kronecker, *Gründzuge . . .* , Crelle, 92, 1882)

$$f(x) \in \mathbb{Z}[x], \;\; \deg(f) = n \;\; \gcd(f, f') = 1$$

An Algorithm

(Kronecker, *Gründzuge ...*, Crelle, 92, 1882)

$$f(x) \in \mathbb{Z}[x], \quad \deg(f) = n \quad \gcd(f, f') = 1$$

1) Let
$$\begin{aligned} R(Y, X_1, \ldots, X_n) &= \prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_{\sigma(1)} X_1 + \ldots + \alpha_{\sigma(n)} X_n)) \\ &= \prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_1 X_{\sigma^{-1}(1)} + \ldots + \alpha_n X_{\sigma^{-1}(n)})) \\ &\in \mathbb{Q}[Y, X_1, \ldots, X_n] \end{aligned}$$

An Algorithm

(Kronecker, *Gründzuge . . .* , Crelle, 92, 1882)

$$f(x) \in \mathbb{Z}[x], \;\; \deg(f) = n \;\; \gcd(f, f') = 1$$

$$\begin{aligned}
\text{1) Let } R(Y, X_1, \ldots, X_n) &= \textstyle\prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_{\sigma(1)} X_1 + \ldots + \alpha_{\sigma(n)} X_n)) \\
&= \textstyle\prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_1 X_{\sigma^{-1}(1)} + \ldots + \alpha_n X_{\sigma^{-1}(n)})) \\
&\in \mathbb{Q}[Y, X_1, \ldots, X_n]
\end{aligned}$$

$$\text{2) Factor } R(Y, X_1, \ldots, X_n) = R_1(Y, X_1, \ldots, X_n) \cdots R_t(Y, X_1, \ldots, X_n)$$

An Algorithm

(Kronecker, *Gründzuge . . .*, Crelle, 92, 1882)

$$f(x) \in \mathbb{Z}[x], \;\; \deg(f) = n \;\; \gcd(f, f') = 1$$

1) Let
$$\begin{aligned} R(Y, X_1, \ldots, X_n) &= \prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_{\sigma(1)} X_1 + \ldots + \alpha_{\sigma(n)} X_n)) \\ &= \prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_1 X_{\sigma^{-1}(1)} + \ldots + \alpha_n X_{\sigma^{-1}(n)})) \\ &\in \mathbb{Q}[Y, X_1, \ldots, X_n] \end{aligned}$$

2) Factor
$$R(Y, X_1, \ldots, X_n) = R_1(Y, X_1, \ldots, X_n) \cdots R_t(Y, X_1, \ldots, X_n)$$

Galois group of f $= \{\sigma \in \mathcal{S}_n \mid R_1(Y, X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = R_1(Y, X_1, \ldots, X_n)\}$

An Algorithm

(Kronecker, *Gründzuge . . .* , Crelle, 92, 1882)

$$f(x) \in \mathbb{Z}[x], \quad \deg(f) = n \quad \gcd(f, f') = 1$$

$$\begin{aligned}
\text{1) Let } R(Y, X_1, \ldots, X_n) &= \prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_{\sigma(1)} X_1 + \ldots + \alpha_{\sigma(n)} X_n)) \\
&= \prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_1 X_{\sigma^{-1}(1)} + \ldots + \alpha_n X_{\sigma^{-1}(n)})) \\
&\in \mathbb{Q}[Y, X_1, \ldots, X_n]
\end{aligned}$$

$$\text{2) Factor } R(Y, X_1, \ldots, X_n) = R_1(Y, X_1, \ldots, X_n) \cdots R_t(Y, X_1, \ldots, X_n)$$

$$\text{Galois group of f} = \{\sigma \in \mathcal{S}_n \mid R_1(Y, X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = R_1(Y, X_1, \ldots, X_n)\}$$

High Complexity!

Polynomial Time Algorithms

Question: Is there an algorithm to compute the Galois group of $f(x) \in \mathbb{Z}[x]$ whose running time is given as a polynomial in the size of f?

Polynomial Time Algorithms

Question: Is there an algorithm to compute the Galois group of $f(x) \in \mathbb{Z}[x]$ whose running time is given as a polynomial in the size of f?

For $m \in \mathbb{Z}$, size(m) = number of digits $\simeq$ log(m)

For $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$, size($f(x)$) = $n \cdot \max_i\{\text{size}(a_i)\}$.

Polynomial Time Algorithms

Question: Is there an algorithm to compute the Galois group of $f(x) \in \mathbb{Z}[x]$ whose running time is given as a polynomial in the size of f?

For $m \in \mathbb{Z}$, size(m) = number of digits $\simeq \log(m)$

For $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$, size($f(x)$) = $n \cdot \max_i\{\text{size}(a_i)\}$.

Running Time = number of $+, \times, -, \div$

Polynomial Time Algorithms

Question: ~~Is there an algorithm to compute the Galois group of $f(x) \in \mathbb{Z}[x]$ whose running time is given as a polynomial in the size of f?~~

For $m \in \mathbb{Z}$, size(m) = number of digits $\simeq \log(m)$

For $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$, size($f(x)$) = $n \cdot \max_i\{\text{size}(a_i)\}$.

Running Time = number of $+, \times, -, \div$

Revised Question:Is there an algorithm to compute generators of the Galois group of $f(x) \in \mathbb{Z}[x]$ whose running time is given as a polynomial in the size of f?

Polynomial Time Algorithms

Question: ~~Is there an algorithm to compute the Galois group of $f(x) \in \mathbb{Z}[x]$ whose running time is given as a polynomial in the size of f?~~

For $m \in \mathbb{Z}$, size(m) = number of digits $\simeq \log(m)$

For $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$, size($f(x)$) = $n \cdot \max_i\{\text{size}(a_i)\}$.

Running Time = number of $+, \times, -, \div$

Revised Question:Is there an algorithm to compute generators of the Galois group of $f(x) \in \mathbb{Z}[x]$ whose running time is given as a polynomial in the size of f?

We do not know!

Galois (*Discours préliminaire*):

“Si maintenant vous me donnez une équation que vous aurez choisie à votre gré et que vous desiriez connaître si elle est ou non soluble par radicaux, je n’aurai rien à y faire que de vous indiquer le moyen de répondre à votre question, sans vouloir charger ni moi ni personne de le faire. En un mot les calculs sont impraticables.”

Galois (*Discours préliminaire*):

“Si maintenant vous me donnez une équation que vous aurez choisie à votre gré et que vous desiriez connaître si elle est ou non soluble par radicaux, je n’aurai rien à y faire que de vous indiquer le moyen de répondre à votre question, sans vouloir charger ni moi ni personne de le faire. En un mot les calculs sont impraticables.”

Question: Is there an algorithm to decide if $f(x) \in \mathbb{Z}[x]$ is solvable by radicals whose running time is given as a polynomial in the size of f?

Galois (*Discours préliminaire*):

"Si maintenant vous me donnez une équation que vous aurez choisie à votre gré et que vous desiriez connaître si elle est ou non soluble par radicaux, je n'aurai rien à y faire que de vous indiquer le moyen de répondre à votre question, sans vouloir charger ni moi ni personne de le faire. En un mot les calculs sont impraticables."

Question: Is there an algorithm to decide if $f(x) \in \mathbb{Z}[x]$ is solvable by radicals whose running time is given as a polynomial in the size of f?

Landau and Miller (*Solvability by radicals in polynomial time*, J. Comp. Sys. Sci.,1985):

"If now you give us a polynomial which you have chosen at your pleasure, and if you want to know if it is or is not solvable by radicals, we have presented techniques to answer that question in polynomial time."

Ingredients of the Landau-Miller Algorithm

Ingredients of the Landau-Miller Algorithm

- Lenstra-Lenstra-Lovász (1982): Polynomial time algorithm to factor $f(x) \in \mathbb{Q}[x]$.

Ingredients of the Landau-Miller Algorithm

• Lenstra-Lenstra-Lovász (1982): Polynomial time algorithm to factor $f(x) \in \mathbb{Q}[x]$.

$\Rightarrow$ Landau (1985): Construct splitting field and Galois group G in time polynomial in $|G|$ and size(f)

Ingredients of the Landau-Miller Algorithm

• Lenstra-Lenstra-Lovász (1982): Polynomial time algorithm to factor $f(x) \in \mathbb{Q}[x]$.

$\Rightarrow$ Landau (1985): Construct splitting field and Galois group G in time polynomial in $|G|$ and size(f)

- $\diamond$ Adjoin root of $f \Rightarrow \mathbb{Q}(\alpha_1)$, factor f over $\mathbb{Q}(\alpha_1) \Rightarrow f = f_1 f_2 \cdots f_t$
- $\diamond$ Adjoin root of $f_1 \Rightarrow \mathbb{Q}(\alpha_1, \alpha_2)$, factor f over $\mathbb{Q}(\alpha_1, \alpha_2)$
- $\diamond$ Stop when f factors completely over $K = \mathbb{Q}(\alpha_1, \dots, \alpha_\ell)$
- $\diamond$ $K = \mathbb{Q}(\beta),\ \beta = r_1\alpha_1 + \ldots + r_n\alpha_n,\ g(x) =$ min. poly β over $\mathbb{Q}$
- $\diamond$ Galois group = $\{\sigma \in \mathcal{S}_n \mid g(r_1\alpha_{\sigma(1)} + \ldots + r_n\alpha_{\sigma(n)}) = 0\}$

Ingredients of the Landau-Miller Algorithm

• Lenstra-Lenstra-Lovász (1982): Polynomial time algorithm to factor $f(x) \in \mathbb{Q}[x]$.

$\Rightarrow$ Landau (1985): Construct splitting field and Galois group G in time polynomial in $|G|$ and size(f)

Ingredients of the Landau-Miller Algorithm

• Lenstra-Lenstra-Lovász (1982): Polynomial time algorithm to factor $f(x) \in \mathbb{Q}[x]$.

$\Rightarrow$ Landau (1985): Construct splitting field and Galois group G in time polynomial in $|G|$ and size(f)

• Sims (1970): Given a group G can determine if it solvable in time polynomial in $|G|$.

$\Rightarrow$ Can determine if Galois group is solvable in time polynomial in $|G|$ and size(f)

Ingredients of the Landau-Miller Algorithm

• Lenstra-Lenstra-Lovász (1982): Polynomial time algorithm to factor $f(x) \in \mathbb{Q}[x]$.

$\Rightarrow$ Landau (1985): Construct splitting field and Galois group G in time polynomial in $|G|$ and size(f)

• Sims (1970): Given a group G can determine if it solvable in time polynomial in $|G|$.

$\Rightarrow$ Can determine if Galois group is solvable in time polynomial in $|G|$ and size(f)

• P'alfy (1982): $G \subset \mathcal{S}_n$ solvable, transitive and primitive implies $|G| < n^{3.25}$

Ingredients of the Landau-Miller Algorithm

• Lenstra-Lenstra-Lovász (1982): Polynomial time algorithm to factor $f(x) \in \mathbb{Q}[x]$.

$\Rightarrow$ Landau (1985): Construct splitting field and Galois group G in time polynomial in $|G|$ and size(f)

• Sims (1970): Given a group G can determine if it solvable in time polynomial in $|G|$.

$\Rightarrow$ Can determine if Galois group is solvable in time polynomial in $|G|$ and size(f)

• P'alfy (1982): $G \subset \mathcal{S}_n$ solvable, transitive and <u>primitive</u> implies $|G| < n^{3.25}$

• Landau-Miller (1985): Showed how to reduce to the case of equations with transitive, primitive Galois groups.

Calculating Galois groups in practice

Things that work

Mod p techniques

$f(x) \in \mathbb{Z}[x]$, monic, $\deg f = n$ $\qquad \Delta(f) = \prod(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$

Mod p techniques

$$f(x) \in \mathbb{Z}[x], \text{ monic, } \deg f = n \qquad \Delta(f) = \prod(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$$

Fact: For $p \nmid \Delta(f)$, $Gal(f \pmod{p}) \hookrightarrow Gal(f)$

Mod p techniques

$f(x) \in \mathbb{Z}[x]$, monic, $\deg f = n \qquad \Delta(f) = \prod(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$

<u>Fact:</u> For $p \nmid \Delta(f)$, $Gal(f \pmod p) \hookrightarrow Gal(f)$

$$\begin{aligned} R(Y, X_1, \ldots, X_n) &= \prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_{\sigma(1)} X_1 + \ldots + \alpha_{\sigma(n)} X_n)) \\ &= R_1 \qquad \cdots \qquad R_t \qquad \text{over } \mathbb{Q} \end{aligned}$$

Mod p techniques

$$f(x) \in \mathbb{Z}[x], \text{ monic, } \deg f = n \qquad \Delta(f) = \prod(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$$

<u>Fact:</u> For $p \nmid \Delta(f)$, $Gal(f \pmod{p}) \hookrightarrow Gal(f)$

$$\begin{aligned}
R(Y, X_1, \ldots, X_n) &= \prod_{\sigma \in \mathcal{S}_n} (Y - (\alpha_{\sigma(1)} X_1 + \ldots + \alpha_{\sigma(n)} X_n)) \\
&= R_1 \qquad \cdots \qquad R_t \qquad \text{over } \mathbb{Q} \\
&= (R_{1,1} \cdots R_{1,m_1}) \cdots (R_{t,1} \cdots R_{t,m_t}) \bmod p
\end{aligned}$$

Mod p techniques

$$f(x) \in \mathbb{Z}[x], \text{ monic, } \deg f = n \qquad \Delta(f) = \prod(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$$

Fact: For $p \nmid \Delta(f)$, $\; Gal(f \pmod p) \hookrightarrow Gal(f)$

Mod p techniques

$$f(x) \in \mathbb{Z}[x], \text{ monic, } \deg f = n \qquad \Delta(f) = \prod(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$$

<u>Fact:</u> For $p \nmid \Delta(f)$, $\;Gal(f \pmod{p}) \hookrightarrow Gal(f)$

<u>Theorem of Frobenius</u> Let $\quad n = n_1 + \ldots + n_t, \quad n_1 \geq n_2 \ldots \geq n_t$

$$\text{Density of } \{p \mid p \nmid \Delta(f), \quad f = f_1 \cdots f_t \pmod{p}, \ \deg(f_i) = n_i\}$$

$$\|$$

$$\frac{1}{|G|} \cdot |\{\sigma \in G \mid \sigma = \tau_1 \cdots \tau_t, \ \tau_i \text{ a cycle of length } n_i\}|$$

Mod p techniques

$$f(x) \in \mathbb{Z}[x], \text{ monic, } \deg f = n \qquad \Delta(f) = \prod(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$$

Fact: For $p \nmid \Delta(f)$, $Gal(f \pmod p) \hookrightarrow Gal(f)$

Theorem of Frobenius Let $n = n_1 + \ldots + n_t$, $n_1 \geq n_2 \ldots \geq n_t$

$$\text{Density of } \{p \mid p \nmid \Delta(f),\ \ f = f_1 \cdots f_t \pmod p),\ \deg(f_i) = n_i\}$$

$$\|$$

$$\frac{1}{|G|} \cdot |\{\sigma \in G \mid \sigma = \tau_1 \cdots \tau_t,\ \tau_i \text{ a cycle of length } n_i\}|$$

Advantages:

- Easy to factor mod p (Berlekamp, 1967)
- Gives a good probabilistic test for $\mathcal{S}_n, \mathcal{A}_n$; good evidence for other groups.

Mod p techniques

$$f(x) \in \mathbb{Z}[x], \text{ monic, } \deg f = n \qquad \Delta(f) = \prod(\alpha_i - \alpha_j)^2 \in \mathbb{Z}$$

Fact: For $p \nmid \Delta(f)$, $Gal(f \pmod p) \hookrightarrow Gal(f)$

Theorem of Frobenius Let $n = n_1 + \ldots + n_t, \quad n_1 \geq n_2 \ldots \geq n_t$

$$\text{Density of } \{p \mid p \nmid \Delta(f), \ \ f = f_1 \cdots f_t \pmod p, \ \deg(f_i) = n_i\}$$

$$\|$$

$$\frac{1}{|G|} \cdot |\{\sigma \in G \mid \sigma = \tau_1 \cdots \tau_t, \ \tau_i \text{ a cycle of length } n_i\}|$$

Advantages:

- Easy to factor mod p (Berlekamp, 1967)
- Gives a good probabilistic test for $\mathcal{S}_n, \mathcal{A}_n$; good evidence for other groups.

Disadvantages:

- Asymptotic result
- Groups not determined by distribution of cycle patterns - already in deg. 8

Invariant Theoretic Techniques

Invariant Theoretic Techniques

Example: $f(x) = x^3 + bx + c \in \mathbb{Q}[x]$ $\mathrm{Gal}(f) \subset \mathcal{S}_3$

Invariant Theoretic Techniques

<u>Example:</u> $f(x) = x^3 + bx + c \in \mathbb{Q}[x] \qquad \mathrm{Gal}(f) \subset \mathcal{S}_3$

$f(x) = (x+\alpha)(x+\beta x+\gamma), \;\; \alpha, \beta, \gamma \in \mathbb{Q} \Longrightarrow \mathrm{Gal}(f) = \mathcal{S}_2$ or $\{id\}$

Invariant Theoretic Techniques

<u>Example:</u> $f(x) = x^3 + bx + c \in \mathbb{Q}[x] \qquad \mathrm{Gal}(f) \subset \mathcal{S}_3$

$f(x) = (x+\alpha)(x+\beta x+\gamma), \;\; \alpha, \beta, \gamma \in \mathbb{Q} \Longrightarrow \mathrm{Gal}(f) = \mathcal{S}_2$ or $\{id\}$

$f(x)$ irreducible $\Longrightarrow \mathrm{Gal}(f)$ acts transitively on the roots $\alpha_1, \alpha_2, \alpha_3$
Group Theory $\Longrightarrow \mathrm{Gal}(f) = \mathcal{S}_3$ or $\mathcal{A}_3$

Invariant Theoretic Techniques

<u>Example:</u> $f(x) = x^3 + bx + c \in \mathbb{Q}[x] \qquad \mathrm{Gal}(f) \subset \mathcal{S}_3$

$f(x) = (x+\alpha)(x+\beta x+\gamma), \quad \alpha, \beta, \gamma \in \mathbb{Q} \Longrightarrow \mathrm{Gal}(f) = \mathcal{S}_2$ or $\{id\}$

$f(x)$ irreducible $\Longrightarrow \mathrm{Gal}(f)$ acts transitively on the roots $\alpha_1, \alpha_2, \alpha_3$
Group Theory $\Longrightarrow \mathrm{Gal}(f) = \mathcal{S}_3$ or $\mathcal{A}_3$

Let
$F(z) = z^2 + 4b^3 + 27c^2 = (z+\delta)(z-\delta) \quad \delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$

δ is an invariant of $\mathcal{A}_3$ but not of $\mathcal{S}_3$ so

$$\mathrm{Gal}(f) = \mathcal{A}_3 \Leftrightarrow F(z) \text{ factors over } \mathbb{Q}.$$

Invariant Theoretic Techniques

Example: $f(x) = x^3 + bx + c \in \mathbb{Q}[x] \qquad \mathrm{Gal}(f) \subset \mathcal{S}_3$

$f(x) = (x+\alpha)(x+\beta x+\gamma), \ \ \alpha, \beta, \gamma \in \mathbb{Q} \Longrightarrow \mathrm{Gal}(f) = \mathcal{S}_2$ or $\{id\}$

$f(x)$ irreducible $\Longrightarrow \mathrm{Gal}(f)$ acts transitively on the roots $\alpha_1, \alpha_2, \alpha_3$
Group Theory $\Longrightarrow \mathrm{Gal}(f) = \mathcal{S}_3$ or $\mathcal{A}_3$

Let
$F(z) = z^2 + 4b^3 + 27c^2 = (z+\delta)(z-\delta) \quad \delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$

δ is an invariant of $\mathcal{A}_3$ but not of $\mathcal{S}_3$ so

$$\mathrm{Gal}(f) = \mathcal{A}_3 \Leftrightarrow F(z) \text{ factors over } \mathbb{Q}.$$

Reduce calculation of Galois groups to factorization of associated polynomials

Why does this work?

Why does this work?

I. A finite group is determined by its permutation representations.

Why does this work?

I. A finite group is determined by its permutation representations.

Given $H \subsetneq G$, $\exists \rho : G \longrightarrow \mathcal{S}_N$ such that G acts transitively but H does not.

Why does this work?

I. A finite group is determined by its permutation representations.

Given $H \subsetneq G$, $\exists \rho : G \to \mathcal{S}_N$ such that G acts transitively but H does not.

II. One can find permutation representations of $G = \mathrm{Gal}(K/k)$ in K.

Let $\rho : G \to \mathcal{S}_N$, then $\exists\ \beta_1, \ldots, \beta_N \in K$ such that

$$\sigma(\alpha_i) = \alpha_{\rho(\sigma)(i)}, \quad \text{for all } \sigma \in G$$

Why does this work?

I. A finite group is determined by its permutation representations.

Given $H \subsetneq G$, $\exists \rho : G \to \mathcal{S}_N$ such that G acts transitively but H does not.

II. One can find permutation representations of $G = \mathrm{Gal}(K/k)$ in K.

Let $\rho : G \to \mathcal{S}_N$, then $\exists\ \beta_1, \ldots, \beta_N \in K$ such that

$$\sigma(\alpha_i) = \alpha_{\rho(\sigma)(i)}, \quad \text{for all } \sigma \in G$$

Given $\mathrm{Gal}(K/k) \subset G$, to show $\mathrm{Gal}(K/k) = G$:

- For each maximal subgroup $H \subsetneq G$, find a representation as in I.
- Find $\beta_1, \ldots, \beta_N \in K$ as in II.
- Form $F_H(z) = \prod(z - \beta_i) \in k[z]$.
- If $F_H(z)$ is irreducible for each H, then $\mathrm{Gal}(K/k) = G$.

Differential Galois Groups

Differential Galois Groups

What are Diffferential Galois Groups and what do they measure?

Differential Galois Groups

What are Diffferential Galois Groups and what do they measure?

Calculating Differential Galois Groups . . . in theory

Differential Galois Groups

What are Diffferential Galois Groups and what do they measure?

Calculating Differential Galois Groups . . . in theory

Calculating Differential Galois Groups . . . in practice

Picard-Vessiot Theory

Picard-Vessiot Theory

Consider a linear differential equation

$$L(y) = \frac{d^n y}{dz^n} + a_{n-1}(z)\frac{d^{n-1} y}{dz^{n-1}} + \ldots + a_0 y = 0, \quad a_i(z) \in \mathbb{C}(z)$$

Picard-Vessiot Theory

Consider a linear differential equation

$$L(y) = \frac{d^n y}{dz^n} + a_{n-1}(z)\frac{d^{n-1}y}{dz^{n-1}} + \ldots + a_0 y = 0, \quad a_i(z) \in \mathbb{C}(z)$$

z_0 a nonsingular point $\Rightarrow \exists$ solutions $y_1, \ldots, y_n$ anal. near z_0, lin. indep. $/\mathbb{C}$.

Picard-Vessiot Theory

Consider a linear differential equation

$$L(y) = \frac{d^n y}{dz^n} + a_{n-1}(z)\frac{d^{n-1}y}{dz^{n-1}} + \ldots + a_0 y = 0, \quad a_i(z) \in \mathbb{C}(z)$$

z_0 a nonsingular point $\Rightarrow \exists$ solutions $y_1, \ldots, y_n$ anal. near z_0, lin. indep. $/\mathbb{C}$.

PV-extension $K = \mathbb{C}(z)(y_1, \ldots, y_n, y_1', \ldots, y_n', \ldots, y_1^{(n-1)}, \ldots, y_n^{(n-1)})$.

Picard-Vessiot Theory

Consider a linear differential equation

$$L(y) = \frac{d^n y}{dz^n} + a_{n-1}(z)\frac{d^{n-1}y}{dz^{n-1}} + \ldots + a_0 y = 0, \quad a_i(z) \in \mathbb{C}(z)$$

z_0 a nonsingular point $\Rightarrow \exists$ solutions $y_1, \ldots, y_n$ anal. near z_0, lin. indep. $/\mathbb{C}$.

PV-extension $K = \mathbb{C}(z)(y_1, \ldots, y_n, y_1', \ldots, y_n', \ldots, y_1^{(n-1)}, \ldots, y_n^{(n-1)})$.

PV-group $\mathrm{DGal}(K/k) = \{\sigma : K \to K \mid \sigma$ is a $\mathbb{C}(z)-$ diff. autom. of $K\}$

- $\diamond$ $\mathrm{DGal}(K/k)$ leaves $\mathrm{Soln}(L)$ invariant $\Rightarrow$ $\mathrm{DGal}(K/k) \subset \mathrm{GL}_n(\mathbb{C})$.
- $\diamond$ $\mathrm{DGal}(K/k)$ is Zariski-closed.

Picard-Vessiot Theory

Consider a linear differential equation

$$L(y) = \frac{d^n y}{dz^n} + a_{n-1}(z)\frac{d^{n-1}y}{dz^{n-1}} + \ldots + a_0 y = 0, \quad a_i(z) \in \mathbb{C}(z)$$

z_0 a nonsingular point $\Rightarrow \exists$ solutions $y_1, \ldots, y_n$ anal. near z_0, lin. indep. $/\mathbb{C}$.

PV-extension $K = \mathbb{C}(z)(y_1, \ldots, y_n, y_1', \ldots, y_n', \ldots, y_1^{(n-1)}, \ldots, y_n^{(n-1)})$.

PV-group $\mathrm{DGal}(K/k) = \{\sigma : K \to K \mid \sigma$ is a $\mathbb{C}(z)-$ diff. autom. of $K\}$

- $\diamond$ $\mathrm{DGal}(K/k)$ leaves $\mathrm{Soln}(L)$ invariant $\Rightarrow$ $\mathrm{DGal}(K/k) \subset \mathrm{GL}_n(\mathbb{C})$.
- $\diamond$ $\mathrm{DGal}(K/k)$ is Zariski-closed.

Galois Correspondence: $H^{\text{Zariski closed } \subset \mathrm{DGal}(K/\mathbb{C}(z))} \Leftrightarrow F^{\text{Diff. field, } \mathbb{C}(z) \subset F \subset K}$

What do Differential Galois Groups Measure?

What do Differential Galois Groups Measure?

- Algebraic Dependence: K - a PV-extension of $\mathbb{C}(z)$ with PV-group G

$$\text{tr. deg.}_{\mathbb{C}(z)} K = \dim_{\mathbb{C}} G$$

What do Differential Galois Groups Measure?

- Algebraic Dependence: K - a PV-extension of $\mathbb{C}(z)$ with PV-group G

$$\text{tr. deg.}_{\mathbb{C}(z)} K = \dim_{\mathbb{C}} G$$

Example:

$$\begin{aligned} L(y) &= y'' + \frac{1}{z} + (1 - \frac{\lambda^2}{z^2})y = 0, \qquad \lambda - \frac{1}{2} \notin \mathbb{Z} \\ &\Rightarrow \mathrm{DGal} = \mathrm{SL}_n(\mathbb{C}) \\ &\Rightarrow \text{tr. deg.}_{\mathbb{C}(z)} \mathbb{C}(z)(J_\lambda, Y_\lambda, J'_\lambda, Y'_\lambda) = 3 \end{aligned}$$

- Solvability

• Solvability

$L(y) = 0$ is solvable in terms of liouvillian functions if there exists a tower of fields $\mathbb{C}(z) = K_0 \subset \ldots \subset K_n$ such that $K_{i+1} = K_i(t_i)$ with

- t_i algebraic over K_i, or
- $t_i' \in K_i$, i.e., $t_i = \int u_i, \; u_i \in K_i$, or
- $t_i'/t_i \in K_i$, i.e., $t_i = e^{\int u_i}, \; u_i \in K_i$.

with $K \subset K_n$, where K is the PV-extension associated with $L(y) = 0$.

- Solvability

$L(y) = 0$ is solvable in terms of liouvillian functions if there exists a tower of fields $\mathbb{C}(z) = K_0 \subset \ldots \subset K_n$ such that $K_{i+1} = K_i(t_i)$ with

- t_i algebraic over K_i, or
- $t_i' \in K_i$, i.e., $t_i = \int u_i,\ u_i \in K_i$, or
- $t_i'/t_i \in K_i$, i.e., $t_i = e^{\int u_i},\ u_i \in K_i$.

with $K \subset K_n$, where K is the PV-extension associated with $L(y) = 0$.

Example:

$$L(y) = \frac{d^2y}{dx^2} - \frac{1}{2x}\frac{dy}{dx} - xy$$

$$K_0 = \mathbb{C}(x) \subset K_1 = K_0(\sqrt{x}) \subset K_2 = K_1(e^{\int \sqrt{x}})$$

$$\{e^{\int \sqrt{x}}, e^{-\int \sqrt{x}}\} \text{ is a basis for } \mathrm{Soln}(L = 0)$$

• Solvability

$L(y) = 0$ is solvable in terms of liouvillian functions if there exists a tower of fields $\mathbb{C}(z) = K_0 \subset \ldots \subset K_n$ such that $K_{i+1} = K_i(t_i)$ with

- $\diamond$ t_i algebraic over K_i, or
- $\diamond$ $t_i' \in K_i$, i.e., $t_i = \int u_i,\ u_i \in K_i$, or
- $\diamond$ $t_i'/t_i \in K_i$, i.e., $t_i = e^{\int u_i},\ u_i \in K_i$.

with $K \subset K_n$, where K is the PV-extension associated with $L(y) = 0$.

Example:

$$L(y) = \frac{d^2y}{dx^2} - \frac{1}{2x}\frac{dy}{dx} - xy$$

$$K_0 = \mathbb{C}(x) \subset K_1 = K_0(\sqrt{x}) \subset K_2 = K_1(e^{\int \sqrt{x}})$$

$$\{e^{\int \sqrt{x}}, e^{-\int \sqrt{x}}\} \text{ is a basis for } \mathrm{Soln}(L = 0)$$

Thm: $L(y) = 0$ solvable in terms of liouvillian functions
$\Leftrightarrow \mathrm{DGal}$ contains a solvable subgroup of finite index.

Calculating Differential Galois Groups . . . in theory

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0 y \qquad a_i \in \overline{\mathbb{Q}}(x)$$

Calculating Differential Galois Groups . . . in theory

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0 y \qquad a_i \in \overline{\mathbb{Q}}(x)$$

- One can decide if $L(y) = 0$ has algebraic solutions

  $n = 2$: Schwarz, Klein :: Baldassari-Dwork, van Hoeij-Weil, ...

  $n \geq 2$: Jordan, Boulanger, Painlevé :: Risch, S.

Calculating Differential Galois Groups . . . in theory

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0 y \qquad a_i \in \overline{\mathbb{Q}}(x)$$

- One can decide if $L(y) = 0$ has algebraic solutions

  $n = 2$: Schwarz, Klein :: Baldassari-Dwork, van Hoeij-Weil, ...

  $n \geq 2$: Jordan, Boulanger, Painlevé :: Risch, S.

- One can decide if $L(y) = 0$ is solvable in terms of liouvillian functions.

  $n = 2$: Pepin :: Kovacic.

  $n \geq 2$: Marotte :: S., Ulmer, ... ($n = 3$ van Hoeij, Weil, Ulmer, ..)

Calculating Differential Galois Groups . . . in theory

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0 y \qquad a_i \in \overline{\mathbb{Q}}(x)$$

• One can decide if $L(y) = 0$ has algebraic solutions

$n = 2$: Schwarz, Klein :: Baldassari-Dwork, van Hoeij-Weil, ...

$n \geq 2$: Jordan, Boulanger, Painlevé :: Risch, S.

• One can decide if $L(y) = 0$ is solvable in terms of liouvillian functions.

$n = 2$: Pepin :: Kovacic.

$n \geq 2$: Marotte :: S., Ulmer, ... ($n = 3$ van Hoeij, Weil, Ulmer, ..)

• Can characterize when $L(y) = 0$ is solvable in terms of linear DE of lower order and decide for $n = 3$.

Can decide if $L(y) = 0$ solvable in terms of Airy, Bessel, Cylinder, Kummer, Laguerre, Whittaker . . . (van Hoeij et al)

Calculating Differential Galois Groups . . . in theory

$$L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_0 y \qquad a_i \in \overline{\mathbb{Q}}(x)$$

• One can decide if $L(y) = 0$ has algebraic solutions

$n = 2$: Schwarz, Klein :: Baldassari-Dwork, van Hoeij-Weil, ...

$n \geq 2$: Jordan, Boulanger, Painlevé :: Risch, S.

• One can decide if $L(y) = 0$ is solvable in terms of liouvillian functions.

$n = 2$: Pepin :: Kovacic.

$n \geq 2$: Marotte :: S., Ulmer, ... ($n = 3$ van Hoeij, Weil, Ulmer, ..)

• Can characterize when $L(y) = 0$ is solvable in terms of linear DE of lower order and decide for $n = 3$.

Can decide if $L(y) = 0$ solvable in terms of Airy, Bessel, Cylinder, Kummer, Laguerre, Whittaker . . . (van Hoeij et al)

• One can compute the Galois group. (Hrushovsky)

Calculating Differential Galois Groups . . . in practice

Calculating Differential Galois Groups . . . in practice

Ideas based on Tannakian philosophy:

Calculating Differential Galois Groups . . . in practice

Ideas based on Tannakian philosophy:

- A linear algebraic group G is determined by its linear representations.

Calculating Differential Galois Groups . . . in practice

Ideas based on Tannakian philosophy:

- A linear algebraic group G is determined by its linear representations.
  - ◇ Can recover G from its category of fin. dim. G-modules
  - ◇ Can construct all fin. dim. G-modules from a single faithful G-module via sums, submodules, quotients and duals.

Calculating Differential Galois Groups . . . in practice

Ideas based on Tannakian philosophy:

- A linear algebraic group G is determined by its linear representations.
  - ◇ Can recover G from its category of fin. dim. G-modules
  - ◇ Can construct all fin. dim. G-modules from a single faithful G-module via sums, submodules, quotients and duals.
- A linear differential equation is an avatar for the representation theory of its PV-group.

Calculating Differential Galois Groups . . . in practice

Ideas based on Tannakian philosophy:

- A linear algebraic group G is determined by its linear representations.
  - ◇ Can recover G from its category of fin. dim. G-modules
  - ◇ Can construct all fin. dim. G-modules from a single faithful G-module via sums, submodules, quotients and duals.
- A linear differential equation is an avatar for the representation theory of its PV-group.
  - ◇ Given $L(y)$ with $V = \mathrm{Soln}(L(y))$, for any fin. dim. G-module W, can construct an $\bar{L}(y)$ with $\mathrm{Soln}(\bar{L}(y)) = W$.

Calculating Differential Galois Groups . . . in practice

Ideas based on Tannakian philosophy:

- A linear algebraic group G is determined by its linear representations.
  - ◇ Can recover G from its category of fin. dim. G-modules
  - ◇ Can construct all fin. dim. G-modules from a single faithful G-module via sums, submodules, quotients and duals.

- A linear differential equation is an avatar for the representation theory of its PV-group.
  - ◇ Given $L(y)$ with $V = \mathrm{Soln}(L(y))$, for any fin. dim. G-module W, can construct an $\bar{L}(y)$ with $\mathrm{Soln}(\bar{L}(y)) = W$.

    (i) $W \subset V \quad \rightsquigarrow L = \tilde{L} \circ \bar{L}, \quad \mathrm{Soln}(\bar{L}) = W$

Calculating Differential Galois Groups . . . in practice

Ideas based on Tannakian philosophy:

- A linear algebraic group G is determined by its linear representations.
  - ◇ Can recover G from its category of fin. dim. G-modules
  - ◇ Can construct all fin. dim. G-modules from a single faithful G-module via sums, submodules, quotients and duals.

- A linear differential equation is an avatar for the representation theory of its PV-group.
  - ◇ Given $L(y)$ with $V = \mathrm{Soln}(L(y))$, for any fin. dim. G-module W, can construct an $\bar{L}(y)$ with $\mathrm{Soln}(\bar{L}(y)) = W$.

(i) $W \subset V \quad \rightsquigarrow L = \tilde{L} \circ \bar{L}, \quad \mathrm{Soln}(\bar{L}) = W$

(ii) $V = \mathrm{Soln}(L(y)), W = \mathrm{Soln}(\bar{L}(y)), V \cap W = (0)$
$\rightsquigarrow V \oplus W = \mathrm{Soln}(LCLM(L, \bar{L})(y))$

Calculating Differential Galois Groups . . . in practice

Ideas based on Tannakian philosophy:

- A linear algebraic group G is determined by its linear representations.
  - ◇ Can recover G from its category of fin. dim. G-modules
  - ◇ Can construct all fin. dim. G-modules from a single faithful G-module via sums, submodules, quotients and duals.

- A linear differential equation is an avatar for the representation theory of its PV-group.
  - ◇ Given $L(y)$ with $V = \mathrm{Soln}(L(y))$, for any fin. dim. G-module W, can construct an $\bar{L}(y)$ with $\mathrm{Soln}(\bar{L}(y)) = W$.

(i) $W \subset V \quad \rightsquigarrow L = \tilde{L} \circ \bar{L}, \quad \mathrm{Soln}(\bar{L}) = W$

(ii) $V = \mathrm{Soln}(L(y)), W = \mathrm{Soln}(\bar{L}(y)), V \cap W = (0)$
$\rightsquigarrow V \oplus W = \mathrm{Soln}(LCLM(L, \bar{L})(y))$

(iii) $\mathrm{Sym}^m(V) = \{y_1 \cdots y_m \mid y_i \in V\} = \mathrm{Soln}(L^{ⓢ m}(y))$

<u>Thm.</u> Assume $L(y) = y'' + r(x)y$.

$L(y) = 0$ is solvable in terms of liouvillian functions

Thm. Assume $L(y) = y'' + r(x)y$.

$$L(y) = 0 \text{ is solvable in terms of liouvillian functions}$$
$$\Updownarrow$$
$$L^{ⓢ 6} \text{ factors.}$$

Thm. Assume $L(y) = y'' + r(x)y$.

$$L(y) = 0 \text{ is solvable in terms of liouvillian functions}$$
$$\Updownarrow$$
$$L^{\circledS 6} \text{ factors.}$$

Thm. Assume $L(y) = y''' + r(x)y$.

$$\text{DGal = Valentiner Group } A_6^{\mathrm{SL}_3} \text{ of order 1080}$$

Thm. Assume $L(y) = y'' + r(x)y$.

$$L(y) = 0 \text{ is solvable in terms of liouvillian functions}$$
$$\Updownarrow$$
$$L^{Ⓢ 6} \text{ factors.}$$

Thm. Assume $L(y) = y''' + r(x)y$.

$$\text{DGal = Valentiner Group } A_6^{\mathrm{SL}_3} \text{ of order 1080}$$
$$\Updownarrow$$
$$L^{Ⓢ 2} \text{ and } L^{Ⓢ 3} \text{ are irreducible}$$
$$L^{Ⓢ 4} = L_9 \circ L_6, \quad L_9, L_6 \text{ irreducible.}$$