Galois groups and functional equations: theory, algorithms, and applications

Carlos E. Arreche

The University of Texas at Dallas

FELIM 2024: Functional Equations in LIMoges
March 26, 2024

Philosophy

A Galois theory associates to a functional equation (polynomial, or differential, or difference, or ...) a Galois group that encodes properties of the solutions.

$$\text{Group Theory}$$
$$\Downarrow \text{Galois Theory}$$
$$\text{Form of Functional Dependencies}$$

Algorithms to compute Galois groups lead directly to computation of relations among the solutions of the corresponding equations.

These relations (or their absence) are interpreted as qualitative information about solutions, even when they remain unknown.

Philosophy

A Galois theory associates to a functional equation (polynomial, or differential, or difference, or ...) a Galois group that encodes properties of the solutions.

$$\text{Group Theory}$$

$$\Big\Downarrow \ \text{Galois Theory}$$

$$\text{Form of Functional Dependencies}$$

Algorithms to compute Galois groups lead directly to computation of relations among the solutions of the corresponding equations.

These relations (or their absence) are interpreted as qualitative information about solutions, even when they remain unknown.

Philosophy

A Galois theory associates to a functional equation (polynomial, or differential, or difference, or ...) a Galois group that encodes properties of the solutions.

$$\text{Group Theory}$$

$$\Big\Updownarrow \quad \text{Galois Theory}$$

$$\text{Form of Functional Dependencies}$$

Algorithms to compute Galois groups lead directly to computation of relations among the solutions of the corresponding equations.

These relations (or their absence) are interpreted as qualitative information about solutions, even when they remain unknown.

Galois Groups of Polynomial Equations

For a field K and a (separable) polynomial $p(y) \in K[y]$ of degree $N \geq 1$, we can create the *splitting field*

$$L := K[y_1, \ldots, y_N] \left[\prod_{i \neq j} \frac{1}{y_i - y_j} \right] \Big/ \mathfrak{m},$$

for $\mathfrak{m}$ some (any) maximal ideal of $L := K[y_1, \ldots, y_N][\prod_{i \neq j} \frac{1}{y_i - y_j}]$ containing $\langle p(y_1), \ldots, p(y_N) \rangle$.

The *Galois group* $\mathrm{Gal}(L/K)$ is the group of K-automorphisms of L over K, realized more concretely as a subgroup of $\mathcal{S}_N$ by its faithful action on $\{\bar{y}_1, \ldots, \bar{y}_N\} \subset L$.

The Galois group encodes in its algebraic structure information about solutions to $p(y) = 0$. E.g., $\mathrm{Gal}(L/K)$ is solvable iff solutions are expressed in terms of radicals, etc., etc.

Galois Groups of Polynomial Equations

For a field K and a (separable) polynomial $p(y) \in K[y]$ of degree $N \geq 1$, we can create the *splitting field*

$$L := K[y_1, \ldots, y_N]\left[\prod_{i \neq j} \frac{1}{y_i - y_j}\right] \Big/ \mathfrak{m},$$

for $\mathfrak{m}$ some (any) maximal ideal of $L := K[y_1, \ldots, y_N][\prod_{i \neq j} \frac{1}{y_i - y_j}]$ containing $\langle p(y_1), \ldots, p(y_N) \rangle$.

The *Galois group* $\mathrm{Gal}(L/K)$ is the group of K-automorphisms of L over K, realized more concretely as a subgroup of $\mathcal{S}_N$ by its faithful action on $\{\bar{y}_1, \ldots, \bar{y}_N\} \subset L$.

The Galois group encodes in its algebraic structure information about solutions to $p(y) = 0$. E.g., $\mathrm{Gal}(L/K)$ is solvable iff solutions are expressed in terms of radicals, etc., etc.

Galois Groups of Polynomial Equations

For a field K and a (separable) polynomial $p(y) \in K[y]$ of degree $N \geq 1$, we can create the *splitting field*

$$L := K[y_1, \ldots, y_N] \left[\prod_{i \neq j} \frac{1}{y_i - y_j} \right] \Big/ \mathfrak{m},$$

for $\mathfrak{m}$ some (any) maximal ideal of $L := K[y_1, \ldots, y_N][\prod_{i \neq j} \frac{1}{y_i - y_j}]$ containing $\langle p(y_1), \ldots, p(y_N) \rangle$.

The *Galois group* $\mathrm{Gal}(L/K)$ is the group of K-automorphisms of L over K, realized more concretely as a subgroup of $\mathcal{S}_N$ by its faithful action on $\{\bar{y}_1, \ldots, \bar{y}_N\} \subset L$.

The Galois group encodes in its algebraic structure information about solutions to $p(y) = 0$. E.g., $\mathrm{Gal}(L/K)$ is solvable iff solutions are expressed in terms of radicals, etc., etc.

Polynomial Equations of Galois Groups

Given: field K and finite group G.

Inverse Galois Problem: does there exist a (separable) polynomial $p(y) \in K[y]$ whose Galois group is isomorphic to G? (Just yes/no).

- Examples: $K = \mathbb{C}(z) \rightarrow$ yes; $K = \mathbb{F}_p \rightarrow$ yes iff G is cyclic; $K = \mathbb{Q} \rightarrow$?, known for some G, conjecturally true for all G.

Constructive Inverse Galois Problem: construct explicitly $p(y) \in K[y]$ whose Galois group is isomorphic to G (if it exists).

Additional constraints/variants, given also a set S with a faithful G-action: (1) does there exist $p(y) \in K[y]$ whose Galois group is $\simeq G$ and $S \simeq \{\bar{y}_1, \ldots, \bar{y}_N\}$ as G-sets?; and (2) can we compute such a $p(y)$ explicitly?

Polynomial Equations of Galois Groups

Given: field K and finite group G.

Inverse Galois Problem: does there exist a (separable) polynomial $p(y) \in K[y]$ whose Galois group is isomorphic to G? (Just yes/no).

- Examples: $K = \mathbb{C}(z) \to$ yes; $K = \mathbb{F}_p \to$ yes iff G is cyclic; $K = \mathbb{Q} \to$?, known for some G, conjecturally true for all G.

Constructive Inverse Galois Problem: construct explicitly $p(y) \in K[y]$ whose Galois group is isomorphic to G (if it exists).

Additional constraints/variants, given also a set S with a faithful G-action: (1) does there exist $p(y) \in K[y]$ whose Galois group is $\simeq G$ and $S \simeq \{\bar{y}_1, \ldots, \bar{y}_N\}$ as G-sets?; and (2) can we compute such a $p(y)$ explicitly?

Polynomial Equations of Galois Groups

Given: field K and finite group G.

Inverse Galois Problem: does there exist a (separable) polynomial $p(y) \in K[y]$ whose Galois group is isomorphic to G? (Just yes/no).

- Examples: $K = \mathbb{C}(z) \to$ yes; $K = \mathbb{F}_p \to$ yes iff G is cyclic; $K = \mathbb{Q} \to$?, known for some G, conjecturally true for all G.

Constructive Inverse Galois Problem: construct explicitly $p(y) \in K[y]$ whose Galois group is isomorphic to G (if it exists).

Additional constraints/variants, given also a set S with a faithful G-action: (1) does there exist $p(y) \in K[y]$ whose Galois group is $\simeq G$ and $S \simeq \{\bar{y}_1, \ldots, \bar{y}_N\}$ as G-sets?; and (2) can we compute such a $p(y)$ explicitly?

Differential Equations over Differential Fields

A Δ-*field* is a field K equipped with a set $\Delta = \{\delta_1, \ldots, \delta_n\}$ of pairwise commuting *derivations*: additive maps satisfying the Leibniz rule $\delta_i(ab) = a\delta_i(b) + \delta_i(a)b$ and $\delta_i \circ \delta_j = \delta_j \circ \delta_i$.

The Δ-*constants* $K^\Delta = \{c \in K \mid \delta_i(c) = 0 \text{ for every } i = 1, \ldots, n\}$.

Main Example: $K = \mathbb{C}(z_1, \ldots, z_n)$ and $\delta_i = \frac{\partial}{\partial z_i}$. Here $K^\Delta = \mathbb{C}$.

A *linear differential system* (of rank N) over K is a collection $\mathcal{A}$

$$\begin{pmatrix} \delta_i(y_1) \\ \vdots \\ \delta_i(y_N) \end{pmatrix} = \begin{pmatrix} a_{11}^{(i)} & \cdots & a_{1N}^{(i)} \\ \vdots & & \vdots \\ a_{N1}^{(i)} & \cdots & a_{NN}^{(i)} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix}; \qquad \text{for} \quad i = 1, \ldots, n,$$

where the $y_1, \ldots, y_N$ are unknowns and $A_i = (a_{rs}^{(i)}) \in \mathfrak{gl}_N(K)$.

The system $\mathcal{A}$ is *integrable* if $\delta_i(A_j) - \delta_j(A_i) = A_iA_j - A_jA_i$.

Differential Equations over Differential Fields

A Δ-*field* is a field K equipped with a set $\Delta = \{\delta_1, \ldots, \delta_n\}$ of pairwise commuting *derivations*: additive maps satisfying the Leibniz rule $\delta_i(ab) = a\delta_i(b) + \delta_i(a)b$ and $\delta_i \circ \delta_j = \delta_j \circ \delta_i$.

The Δ-*constants* $K^\Delta = \{c \in K \mid \delta_i(c) = 0 \text{ for every } i = 1, \ldots, n\}$.

Main Example: $K = \mathbb{C}(z_1, \ldots, z_n)$ and $\delta_i = \frac{\partial}{\partial z_i}$. Here $K^\Delta = \mathbb{C}$.

A *linear differential system* (of rank N) over K is a collection $\mathcal{A}$

$$\begin{pmatrix} \delta_i(y_1) \\ \vdots \\ \delta_i(y_N) \end{pmatrix} = \begin{pmatrix} a_{11}^{(i)} & \cdots & a_{1N}^{(i)} \\ \vdots & & \vdots \\ a_{N1}^{(i)} & \cdots & a_{NN}^{(i)} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix}; \qquad \text{for} \quad i = 1, \ldots, n,$$

where the $y_1, \ldots, y_N$ are unknowns and $A_i = (a_{rs}^{(i)}) \in \mathfrak{gl}_N(K)$.

The system $\mathcal{A}$ is *integrable* if $\delta_i(A_j) - \delta_j(A_i) = A_i A_j - A_j A_i$.

Differential Equations over Differential Fields

A Δ-*field* is a field K equipped with a set $\Delta = \{\delta_1, \ldots, \delta_n\}$ of pairwise commuting *derivations*: additive maps satisfying the Leibniz rule $\delta_i(ab) = a\delta_i(b) + \delta_i(a)b$ and $\delta_i \circ \delta_j = \delta_j \circ \delta_i$.

The Δ-*constants* $K^\Delta = \{c \in K \mid \delta_i(c) = 0 \text{ for every } i = 1, \ldots, n\}$.

<u>Main Example</u>: $K = \mathbb{C}(z_1, \ldots, z_n)$ and $\delta_i = \frac{\partial}{\partial z_i}$. Here $K^\Delta = \mathbb{C}$.

A *linear differential system* (of rank N) over K is a collection $\mathcal{A}$

$$\begin{pmatrix} \delta_i(y_1) \\ \vdots \\ \delta_i(y_N) \end{pmatrix} = \begin{pmatrix} a_{11}^{(i)} & \cdots & a_{1N}^{(i)} \\ \vdots & & \vdots \\ a_{N1}^{(i)} & \cdots & a_{NN}^{(i)} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix}; \qquad \text{for} \quad i = 1, \ldots, n,$$

where the $y_1, \ldots, y_N$ are unknowns and $A_i = (a_{rs}^{(i)}) \in \mathfrak{gl}_N(K)$.

The system $\mathcal{A}$ is *integrable* if $\delta_i(A_j) - \delta_j(A_i) = A_iA_j - A_jA_i$.

Galois Groups of Differential Equations

Consider K a Δ-field of characteristic zero, with $\Delta = \{\delta_1, \ldots, \delta_n\}$ commuting derivations, and $\mathcal{A} : \delta_i(Y) = A_i Y$, $i = 1, \ldots, n$, an integrable linear differential system with $A_i \in \mathfrak{gl}_N(K)$, as before.

A Δ-field extension L of K is a *Picard-Vessiot field* over K for $\mathcal{A}$ if:

- $L^\Delta = K^\Delta$;
- there exists $U \in \mathrm{GL}_N(L)$ with $\delta_i(U) = A_i U$ for $i = 1, \ldots, n$;
- L is generated by the entries of U as a field extension of K.

If $K^\Delta =: C$ is algebraically closed, there exists essentially unique Picard-Vessiot (= differential splitting) field for any such system $\mathcal{A}$.

The *differential Galois group* of the system $\mathcal{A}$ is

$$\mathrm{Gal}_\Delta(L/K) := \{\gamma \in \mathrm{Aut}_K(L) \mid \gamma \circ \delta_i = \delta_i \circ \gamma \text{ for } i = 1, \ldots, n\}.$$

It gets identified with a linear algebraic subgroup of $\mathrm{GL}_N(C)$, via

$$\gamma \mapsto U^{-1} \cdot \gamma(U) =: M_\gamma \in \mathrm{GL}_N(C).$$

- Depending up to conjugation on *fundamental matrix* $U \in \mathrm{GL}_N(L)$.

Galois Groups of Differential Equations

Consider K a Δ-field of characteristic zero, with $\Delta = \{\delta_1, \ldots, \delta_n\}$ commuting derivations, and $\mathcal{A} : \delta_i(Y) = A_i Y$, $i = 1, \ldots, n$, an integrable linear differential system with $A_i \in \mathfrak{gl}_N(K)$, as before.

A Δ-field extension L of K is a *Picard-Vessiot field* over K for $\mathcal{A}$ if:

- $L^\Delta = K^\Delta$;
- there exists $U \in \mathrm{GL}_N(L)$ with $\delta_i(U) = A_i U$ for $i = 1, \ldots, n$;
- L is generated by the entries of U as a field extension of K.

If $K^\Delta =: C$ is algebraically closed, there exists essentially unique Picard-Vessiot ($=$ differential splitting) field for any such system $\mathcal{A}$.

The *differential Galois group* of the system $\mathcal{A}$ is

$$\mathrm{Gal}_\Delta(L/K) := \{\gamma \in \mathrm{Aut}_K(L) \mid \gamma \circ \delta_i = \delta_i \circ \gamma \text{ for } i = 1, \ldots, n\}.$$

It gets identified with a linear algebraic subgroup of $\mathrm{GL}_N(C)$, via

$$\gamma \mapsto U^{-1} \cdot \gamma(U) =: M_\gamma \in \mathrm{GL}_N(C).$$

- Depending up to conjugation on *fundamental matrix* $U \in \mathrm{GL}_N(L)$.

Galois Groups of Differential Equations

Consider K a Δ-field of characteristic zero, with $\Delta = \{\delta_1, \ldots, \delta_n\}$ commuting derivations, and $\mathcal{A} : \delta_i(Y) = A_i Y$, $i = 1, \ldots, n$, an integrable linear differential system with $A_i \in \mathfrak{gl}_N(K)$, as before.

A Δ-field extension L of K is a *Picard-Vessiot field* over K for $\mathcal{A}$ if:

- $L^\Delta = K^\Delta$;
- there exists $U \in \mathrm{GL}_N(L)$ with $\delta_i(U) = A_i U$ for $i = 1, \ldots, n$;
- L is generated by the entries of U as a field extension of K.

If $K^\Delta =: C$ is algebraically closed, there exists essentially unique Picard-Vessiot ($=$ differential splitting) field for any such system $\mathcal{A}$.

The *differential Galois group* of the system $\mathcal{A}$ is

$$\mathrm{Gal}_\Delta(L/K) := \{\gamma \in \mathrm{Aut}_K(L) \mid \gamma \circ \delta_i = \delta_i \circ \gamma \text{ for } i = 1, \ldots, n\}.$$

It gets identified with a linear algebraic subgroup of $\mathrm{GL}_N(C)$, via

$$\gamma \mapsto U^{-1} \cdot \gamma(U) =: M_\gamma \in \mathrm{GL}_N(C).$$

- Depending <u>up to conjugation</u> on *fundamental matrix* $U \in \mathrm{GL}_N(L)$.

Finite Galois Groups as Differential Galois Groups

If L is a separable extension of K, each derivation δ on K extends uniquely to a derivation on L.

- Indeed, for $\alpha \in L$ with minimal polynomial $p(y) \in K[y]$, we have $\delta(\alpha) = -p^{\delta}(\alpha)/p'(\alpha)$, where $p^{\delta}(y)$ is obtained by applying δ to the coefficients of $p(y)$ and $p'(y) = \frac{d}{dy}p(y)$.

Thus if L is a separable algebraic extension of a Δ-field K then L is automatically a Δ-field extension of K: the zero derivation $\delta_i\delta_j - \delta_j\delta_i$ on K extends uniquely to the zero derivation on L!

Theorem (Kolchin)

If K is a Δ-field with K^{Δ} algebraically closed of characteristic zero, L is a finite Picard-Vessiot extension of K if and only if L is a finite Galois extension of K. In this case, $\mathrm{Gal}(L/K) = \mathrm{Gal}_{\Delta}(L/K)$.

Finite Galois Groups as Differential Galois Groups

If L is a separable extension of K, each derivation δ on K extends uniquely to a derivation on L.

- Indeed, for $\alpha \in L$ with minimal polynomial $p(y) \in K[y]$, we have $\delta(\alpha) = -p^{\delta}(\alpha)/p'(\alpha)$, where $p^{\delta}(y)$ is obtained by applying δ to the coefficients of $p(y)$ and $p'(y) = \frac{d}{dy}p(y)$.

Thus if L is a separable algebraic extension of a Δ-field K then L is automatically a Δ-field extension of K: the zero derivation $\delta_i\delta_j - \delta_j\delta_i$ on K extends uniquely to the zero derivation on L!

Theorem (Kolchin)

If K is a Δ-field with K^{Δ} algebraically closed of characteristic zero, L is a finite Picard-Vessiot extension of K if and only if L is a finite Galois extension of K. In this case, $\mathrm{Gal}(L/K) = \mathrm{Gal}_{\Delta}(L/K)$.

Finite Galois Groups as Differential Galois Groups

If L is a separable extension of K, each derivation δ on K extends uniquely to a derivation on L.

- Indeed, for $\alpha \in L$ with minimal polynomial $p(y) \in K[y]$, we have $\delta(\alpha) = -p^{\delta}(\alpha)/p'(\alpha)$, where $p^{\delta}(y)$ is obtained by applying δ to the coefficients of $p(y)$ and $p'(y) = \frac{d}{dy}p(y)$.

Thus if L is a separable algebraic extension of a Δ-field K then L is automatically a Δ-field extension of K: the zero derivation $\delta_i\delta_j - \delta_j\delta_i$ on K extends uniquely to the zero derivation on L!

Theorem (Kolchin)

If K is a Δ-field with K^{Δ} algebraically closed of characteristic zero, L is a finite Picard-Vessiot extension of K if and only if L is a finite Galois extension of K. In this case, $\mathrm{Gal}(L/K) = \mathrm{Gal}_{\Delta}(L/K)$.

Finite Galois Groups as Differential Galois Groups

If L is a separable extension of K, each derivation δ on K extends uniquely to a derivation on L.

- Indeed, for $\alpha \in L$ with minimal polynomial $p(y) \in K[y]$, we have $\delta(\alpha) = -p^{\delta}(\alpha)/p'(\alpha)$, where $p^{\delta}(y)$ is obtained by applying δ to the coefficients of $p(y)$ and $p'(y) = \frac{d}{dy}p(y)$.

Thus if L is a separable algebraic extension of a Δ-field K then L is automatically a Δ-field extension of K: the zero derivation $\delta_i\delta_j - \delta_j\delta_i$ on K extends uniquely to the zero derivation on L!

Theorem (Kolchin)

If K is a Δ-field with K^{Δ} algebraically closed of characteristic zero, L is a finite Picard-Vessiot extension of K if and only if L is a finite Galois extension of K. In this case, $\mathrm{Gal}(L/K) = \mathrm{Gal}_{\Delta}(L/K)$.

Differential Equations of Finite Galois Groups

Given: Δ-field K with $K^{\Delta} =: C$ algebraically closed of char. zero and a finite group G.

Inverse Differential Galois Problem (for finite groups): does there exist an integrable system $\mathcal{A}$ whose differential Galois group is isomorphic to G? (Just yes/no).

- By Kolchin's Theorem, the differential and non-differential versions of the inverse Galois problem are equivalent for $|G| < \infty$ and $C = \bar{C}$.

Constructive Inverse Differential Galois Problem (for finite groups): construct explicitly a differential system $\mathcal{A}$ whose differential Galois group is isomorphic to G (if it exists).

Additional constraints/variants, given also a faithful representation $\rho : G \hookrightarrow \mathrm{GL}_N(C)$: (1) does there exist a differential system $\mathcal{A}$ whose Galois group is conjugate to $\rho(G)$?; and (2) can we compute such a system $\mathcal{A}$ explicitly?

Differential Equations of Finite Galois Groups

Given: Δ-field K with $K^\Delta =: C$ algebraically closed of char. zero and a finite group G.

Inverse Differential Galois Problem (for finite groups): does there exist an integrable system $\mathcal{A}$ whose differential Galois group is isomorphic to G? (Just yes/no).

- By Kolchin's Theorem, the differential and non-differential versions of the inverse Galois problem are equivalent for $|G| < \infty$ and $C = \bar{C}$.

Constructive Inverse Differential Galois Problem (for finite groups): construct explicitly a differential system $\mathcal{A}$ whose differential Galois group is isomorphic to G (if it exists).

Additional constraints/variants, given also a faithful representation $\rho : G \hookrightarrow \mathrm{GL}_N(C)$: (1) does there exist a differential system $\mathcal{A}$ whose Galois group is conjugate to $\rho(G)$?; and (2) can we compute such a system $\mathcal{A}$ explicitly?

Differential Equations of Finite Galois Groups

Given: Δ-field K with $K^{\Delta} =: C$ algebraically closed of char. zero and a finite group G.

Inverse Differential Galois Problem (for finite groups): does there exist an integrable system $\mathcal{A}$ whose differential Galois group is isomorphic to G? (Just yes/no).

- By Kolchin's Theorem, the differential and non-differential versions of the inverse Galois problem are equivalent for $|G| < \infty$ and $C = \bar{C}$.

Constructive Inverse Differential Galois Problem (for finite groups): construct explicitly a differential system $\mathcal{A}$ whose differential Galois group is isomorphic to G (if it exists).

Additional constraints/variants, given also a faithful representation $\rho : G \hookrightarrow \mathrm{GL}_N(C)$: (1) does there exist a differential system $\mathcal{A}$ whose Galois group is conjugate to $\rho(G)$?; and (2) can we compute such a system $\mathcal{A}$ explicitly?

Complex Reflection Groups: Definition

We say $g \in \mathrm{GL}_n(\mathbb{C})$ is a *reflection* if $\dim(\ker(1-g)) = n-1$, i.e., g fixes a complex hyperplane pointwise, and g has finite order.

Equivalently, $g \in \mathrm{GL}_n(\mathbb{C})$ is a reflection if it is conjugate to

$$\begin{pmatrix} \zeta & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

for some root of unity $1 \neq \zeta \in \mathbb{C}$.

A *(complex) reflection group* is a finite subgroup $G \subset \mathrm{GL}_n(\mathbb{C})$ that is generated by reflections.

Complex Reflection Groups: Definition

We say $g \in \mathrm{GL}_n(\mathbb{C})$ is a *reflection* if $\dim(\ker(1-g)) = n-1$, i.e., g fixes a complex hyperplane pointwise, and g has finite order.

Equivalently, $g \in \mathrm{GL}_n(\mathbb{C})$ is a reflection if it is conjugate to

$$\begin{pmatrix} \zeta & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

for some root of unity $1 \neq \zeta \in \mathbb{C}$.

A *(complex) reflection group* is a finite subgroup $G \subset \mathrm{GL}_n(\mathbb{C})$ that is generated by reflections.

Complex Reflection Groups: Background

Complex reflection groups were introduced by Shephard, and completely classified by Shephard and Todd, in the 1950's.

The irreducible ones are either cyclic $\mathcal{C}_m$, or symmetric $\mathcal{S}_{n+1}$, or imprimitive $G(ab, b, n)$, or one of 34 primitive groups $G_4, \ldots, G_{37}$.

Replacing $\mathbb{C}$ with $\mathbb{R}$ above, one obtains *real reflection groups*, which are "the same as" *finite Coxeter groups*

$$\langle r_1, \ldots, r_n \mid (r_i r_j)^{m_{ij}} = 1 \rangle$$

where $m_{ii} = 1$ and $m_{ij} \geq 2$ for $i \neq j$.

Weyl groups of complex semisimple Lie algebras are real reflection groups (and "most" real reflection groups are Weyl groups).

Applications: representation theory of reductive algebraic groups, Hecke algebras, knot theory and algebraic topology, moduli spaces, invariant theory, differential equations, mathematical physics, ...

Complex Reflection Groups: Background

Complex reflection groups were introduced by Shephard, and completely classified by Shephard and Todd, in the 1950's.

The irreducible ones are either cyclic $\mathcal{C}_m$, or symmetric $\mathcal{S}_{n+1}$, or imprimitive $G(ab, b, n)$, or one of 34 primitive groups $G_4, \ldots, G_{37}$.

Replacing $\mathbb{C}$ with $\mathbb{R}$ above, one obtains *real reflection groups*, which are "the same as" *finite Coxeter groups*

$$\langle r_1, \ldots, r_n \mid (r_i r_j)^{m_{ij}} = 1 \rangle$$

where $m_{ii} = 1$ and $m_{ij} \geq 2$ for $i \neq j$.

Weyl groups of complex semisimple Lie algebras are real reflection groups (and "most" real reflection groups are Weyl groups).

Applications: representation theory of reductive algebraic groups, Hecke algebras, knot theory and algebraic topology, moduli spaces, invariant theory, differential equations, mathematical physics, ...

Complex Reflection Groups: Background

Complex reflection groups were introduced by Shephard, and completely classified by Shephard and Todd, in the 1950's.

The irreducible ones are either cyclic $\mathcal{C}_m$, or symmetric $\mathcal{S}_{n+1}$, or imprimitive $G(ab, b, n)$, or one of 34 primitive groups $G_4, \ldots, G_{37}$.

Replacing $\mathbb{C}$ with $\mathbb{R}$ above, one obtains *real reflection groups*, which are "the same as" *finite Coxeter groups*

$$\langle r_1, \ldots, r_n \mid (r_i r_j)^{m_{ij}} = 1 \rangle$$

where $m_{ii} = 1$ and $m_{ij} \geq 2$ for $i \neq j$.

Weyl groups of complex semisimple Lie algebras are real reflection groups (and "most" real reflection groups are Weyl groups).

Applications: representation theory of reductive algebraic groups, Hecke algebras, knot theory and algebraic topology, moduli spaces, invariant theory, differential equations, mathematical physics, ...

Invariant Theory of Complex Reflection Groups

Let $G \subset \mathrm{GL}_n(\mathbb{C})$ be a (finite) subgroup. A polynomial

$$p(\mathbf{x}) \in \mathbb{C}[x_1, \ldots, x_n] =: S$$

is *G-invariant* if $p(\mathbf{x} \cdot g) = p(\mathbf{x})$ for every $g \in G$. The subset

$$S^G := \{p \in S \mid p \text{ is } G\text{-invariant}\}$$

is a $\mathbb{C}$-subalgebra of S, called the *algebra of G-invariants*.

Theorem (Shephard-Todd, Chevalley, Serre)

A finite subgroup $G \subset \mathrm{GL}_n(\mathbb{C})$ is a complex reflection group if and only if S^G is generated by n homogeneous algebraically independent polynomials $\phi_1(\mathbf{x}), \ldots, \phi_n(\mathbf{x})$, or equivalently,

$$\mathbb{C}[z_1, \ldots, z_n] \to S^G : z_i \mapsto \phi_i(\mathbf{x})$$

is an isomorphism of S^G with a ring of polynomials in n variables. Moreover, in this case the coinvariant algebra $S/\langle \phi_1(\mathbf{x}), \ldots, \phi_n(\mathbf{x}) \rangle$ is G-isomorphic to the regular representation $\mathbb{C}[G]$.

Invariant Theory of Complex Reflection Groups

Let $G \subset \mathrm{GL}_n(\mathbb{C})$ be a (finite) subgroup. A polynomial

$$p(\mathbf{x}) \in \mathbb{C}[x_1, \ldots, x_n] =: S$$

is *G-invariant* if $p(\mathbf{x} \cdot g) = p(\mathbf{x})$ for every $g \in G$. The subset

$$S^G := \left\{ p \in S \;\middle|\; p \text{ is } G\text{-invariant} \right\}$$

is a $\mathbb{C}$-subalgebra of S, called the *algebra of G-invariants*.

Theorem (Shephard-Todd, Chevalley, Serre)

A finite subgroup $G \subset \mathrm{GL}_n(\mathbb{C})$ is a complex reflection group if and only if S^G is generated by n homogeneous algebraically independent polynomials $\phi_1(\mathbf{x}), \ldots, \phi_n(\mathbf{x})$, or equivalently,

$$\mathbb{C}[z_1, \ldots, z_n] \to S^G : z_i \mapsto \phi_i(\mathbf{x})$$

is an isomorphism of S^G with a ring of polynomials in n variables. Moreover, in this case the coinvariant algebra $S/\langle \phi_1(\mathbf{x}), \ldots, \phi_n(\mathbf{x}) \rangle$ is G-isomorphic to the regular representation $\mathbb{C}[G]$.

Invariant Theory of Complex Reflection Groups

Let $G \subset \mathrm{GL}_n(\mathbb{C})$ be a (finite) subgroup. A polynomial

$$p(\mathbf{x}) \in \mathbb{C}[x_1, \ldots, x_n] =: S$$

is *G-invariant* if $p(\mathbf{x} \cdot g) = p(\mathbf{x})$ for every $g \in G$. The subset

$$S^G := \{p \in S \mid p \text{ is } G\text{-invariant}\}$$

is a $\mathbb{C}$-subalgebra of S, called the *algebra of G-invariants*.

Theorem (Shephard-Todd, Chevalley, Serre)

A finite subgroup $G \subset \mathrm{GL}_n(\mathbb{C})$ is a complex reflection group if and only if S^G is generated by n homogeneous algebraically independent polynomials $\phi_1(\mathbf{x}), \ldots, \phi_n(\mathbf{x})$, or equivalently,

$$\mathbb{C}[z_1, \ldots, z_n] \to S^G : z_i \mapsto \phi_i(\mathbf{x})$$

is an isomorphism of S^G with a ring of polynomials in n variables. Moreover, in this case the coinvariant algebra $S/\langle \phi_1(\mathbf{x}), \ldots, \phi_n(\mathbf{x})\rangle$ is G-isomorphic to the regular representation $\mathbb{C}[G]$.

Complex Reflection Groups as Topological Galois Groups

Let $\mathrm{Ref}(G) =$ set of reflections in a reflection group $G \subset \mathrm{GL}_n(\mathbb{C})$.

For $g \in \mathrm{Ref}(G)$, its *reflecting hyperplane* is $H_g := \ker(1-g)$.

The *hyperplane arrangement* of G is $\mathcal{H}_G := \bigcup_{g \in \mathrm{Ref}(G)} H_g$.

Let $X := \mathbb{C}^n$ as complex manifold with G-action, and $\omega : X \twoheadrightarrow Z$ the quotient map to the *space of orbits* $Z := X/G$. Letting

$$X^\circ := X - \mathcal{H}_G \qquad \text{and} \qquad Z^\circ := Z - \omega(\mathcal{H}_G),$$

the restriction $\omega^\circ : X^\circ \twoheadrightarrow Z^\circ$ is a finite covering space map, whose

$$\mathrm{Deck}(\omega^\circ) := \left\{\text{homeomorphisms } \gamma : X^\circ \to X^\circ \;\middle|\; \omega^\circ \circ \gamma = \omega^\circ\right\} \simeq G.$$

- Note: $Z \simeq \mathbb{C}^n$ also. For any $b \in X^\circ$, we have a short exact sequence

  $$1 \longrightarrow \pi_1(X^\circ, b) \longrightarrow \pi_1(Z^\circ, \omega(b)) \longrightarrow G \longrightarrow 1.$$

  The fundamental groups $\pi_1(X^\circ, b)$ and $\pi_1(Z^\circ, \omega(b))$ are called the *pure braid group of type G* and the *braid group of type G*, respectively. For the symmetric group $G = \mathcal{S}_{n+1}$, these are Artin's $\mathcal{P}_{n+1}$ and $\mathcal{B}_{n+1}$.

Complex Reflection Groups as Topological Galois Groups

Let $\mathrm{Ref}(G)$ = set of reflections in a reflection group $G \subset \mathrm{GL}_n(\mathbb{C})$.

For $g \in \mathrm{Ref}(G)$, its *reflecting hyperplane* is $H_g := \ker(1 - g)$.

The *hyperplane arrangement* of G is $\mathcal{H}_G := \bigcup_{g \in \mathrm{Ref}(G)} H_g$.

Let $X := \mathbb{C}^n$ as complex manifold with G-action, and $\omega : X \twoheadrightarrow Z$ the quotient map to the *space of orbits* $Z := X/G$. Letting

$$X^\circ := X - \mathcal{H}_G \qquad \text{and} \qquad Z^\circ := Z - \omega(\mathcal{H}_G),$$

the restriction $\omega^\circ : X^\circ \twoheadrightarrow Z^\circ$ is a finite covering space map, whose

$$\mathrm{Deck}(\omega^\circ) := \left\{\text{homeomorphisms } \gamma : X^\circ \to X^\circ \;\middle|\; \omega^\circ \circ \gamma = \omega^\circ\right\} \simeq G.$$

- Note: $Z \simeq \mathbb{C}^n$ also. For any $b \in X^\circ$, we have a short exact sequence

$$1 \longrightarrow \pi_1(X^\circ, b) \longrightarrow \pi_1(Z^\circ, \omega(b)) \longrightarrow G \longrightarrow 1.$$

  The fundamental groups $\pi_1(X^\circ, b)$ and $\pi_1(Z^\circ, \omega(b))$ are called the *pure braid group of type G* and the *braid group of type G*, respectively. For the symmetric group $G = \mathcal{S}_{n+1}$, these are Artin's $\mathcal{P}_{n+1}$ and $\mathcal{B}_{n+1}$.

Complex Reflection Groups as Topological Galois Groups

Let $\mathrm{Ref}(G)$ = set of reflections in a reflection group $G \subset \mathrm{GL}_n(\mathbb{C})$.

For $g \in \mathrm{Ref}(G)$, its *reflecting hyperplane* is $H_g := \ker(1-g)$.

The *hyperplane arrangement* of G is $\mathcal{H}_G := \bigcup_{g\in\mathrm{Ref}(G)} H_g$.

Let $X := \mathbb{C}^n$ as complex manifold with G-action, and $\omega : X \twoheadrightarrow Z$ the quotient map to the *space of orbits* $Z := X/G$. Letting

$$X^\circ := X - \mathcal{H}_G \qquad \text{and} \qquad Z^\circ := Z - \omega(\mathcal{H}_G),$$

the restriction $\omega^\circ : X^\circ \twoheadrightarrow Z^\circ$ is a finite covering space map, whose

$$\mathrm{Deck}(\omega^\circ) := \left\{\text{homeomorphisms } \gamma : X^\circ \to X^\circ \;\middle|\; \omega^\circ \circ \gamma = \omega^\circ\right\} \simeq G.$$

- Note: $Z \simeq \mathbb{C}^n$ also. For any $b \in X^\circ$, we have a short exact sequence

$$1 \longrightarrow \pi_1(X^\circ, b) \longrightarrow \pi_1(Z^\circ, \omega(b)) \longrightarrow G \longrightarrow 1.$$

  The fundamental groups $\pi_1(X^\circ, b)$ and $\pi_1(Z^\circ, \omega(b))$ are called the *pure braid group of type G* and the *braid group of type G*, respectively. For the symmetric group $G = \mathcal{S}_{n+1}$, these are Artin's $\mathcal{P}_{n+1}$ and $\mathcal{B}_{n+1}$.

Complex Reflection Groups as Finite Galois Groups

Let $G \subset \mathrm{GL}_n(\mathbb{C})$ be a complex reflection group. Let

$$S = \mathbb{C}[x_1, \ldots, x_n] \qquad \text{and} \qquad S^G = \mathbb{C}[z_1, \ldots, z_n]$$

as before[1], with G acting on S by $g \cdot p(\mathbf{x}) := p(\mathbf{x} \cdot g^{-1})$.

The action of G on polynomials in S extends to rational functions

$$L := \mathbb{C}(x_1, \ldots, x_n); \qquad \text{and} \qquad K := L^G = \mathbb{C}(z_1, \ldots, z_n).$$

By Artin's Theorem, L is finite Galois over K with $\mathrm{Gal}(L/K) \simeq G$. Chevalley proves $S/\langle \mathbf{z} \rangle \simeq \mathbb{C}[G]$ from this fundamental observation.

- To address the constructive version of the inverse Galois problem, It suffices to compute explicitly the minimal polynomial of each x_i over K. In theory, this is not a problem. In practice, it can be a real problem.

[1] The identification $S^G = \mathbb{C}[\mathbf{z}]$ depends on choice of fundamental invariants!

Complex Reflection Groups as Finite Galois Groups

Let $G \subset \mathrm{GL}_n(\mathbb{C})$ be a complex reflection group. Let

$$S = \mathbb{C}[x_1, \ldots, x_n] \qquad \text{and} \qquad S^G = \mathbb{C}[z_1, \ldots, z_n]$$

as before[1], with G acting on S by $g \cdot p(\mathbf{x}) := p(\mathbf{x} \cdot g^{-1})$.

The action of G on polynomials in S extends to rational functions

$$L := \mathbb{C}(x_1, \ldots, x_n); \qquad \text{and} \qquad K := L^G = \mathbb{C}(z_1, \ldots, z_n).$$

By Artin's Theorem, L is finite Galois over K with $\mathrm{Gal}(L/K) \simeq G$. Chevalley proves $S/\langle \mathbf{z} \rangle \simeq \mathbb{C}[G]$ from this fundamental observation.

- To address the constructive version of the inverse Galois problem, It suffices to compute explicitly the minimal polynomial of each x_i over K. In theory, this is not a problem. In practice, it can be a real problem.

[1] The identification $S^G = \mathbb{C}[\mathbf{z}]$ depends on choice of fundamental invariants!

Complex Reflection Groups as Finite Galois Groups

Let $G \subset \mathrm{GL}_n(\mathbb{C})$ be a complex reflection group. Let

$$S = \mathbb{C}[x_1, \ldots, x_n] \qquad \text{and} \qquad S^G = \mathbb{C}[z_1, \ldots, z_n]$$

as before[1], with G acting on S by $g \cdot p(\mathbf{x}) := p(\mathbf{x} \cdot g^{-1})$.

The action of G on polynomials in S extends to rational functions

$$L := \mathbb{C}(x_1, \ldots, x_n); \qquad \text{and} \qquad K := L^G = \mathbb{C}(z_1, \ldots, z_n).$$

By Artin's Theorem, L is finite Galois over K with $\mathrm{Gal}(L/K) \simeq G$. Chevalley proves $S/\langle \mathbf{z} \rangle \simeq \mathbb{C}[G]$ from this fundamental observation.

- To address the constructive version of the inverse Galois problem, It suffices to compute explicitly the minimal polynomial of each x_i over K. In theory, this is not a problem. In practice, it can be a real problem.

[1] The identification $S^G = \mathbb{C}[\mathbf{z}]$ depends on choice of fundamental invariants!

Concrete Example: a Dihedral Group

$$D_8 := \langle r_1, r_2 \mid r_1^2 = r_2^2 = (r_1 r_2)^4 = 1 \rangle$$

acts by reflections on $\mathbb{C}^2$ by

$$r_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \text{and} \qquad r_2 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

and on polynomials $p(\mathbf{x}) \in S = \mathbb{C}[x_1, x_2]$ by

$$r_1 \cdot p(x_1, x_2) = p(x_1, -x_2) \qquad \text{and} \qquad r_2 \cdot p(x_1, x_2) = p(x_2, x_1).$$

The algebra of D_8-invariants is $S^{D_8} = \mathbb{C}[z_1, z_2]$, where

$$z_1 := x_1^2 + x_2^2 \qquad \text{and} \qquad z_2 := x_1^2 x_2^2.$$

Here $L = \mathbb{C}(x_1, x_2)$ is the splitting field over $K = \mathbb{C}(z_1, z_2)$ of

$$p(y) = y^4 - z_1 y^2 + z_2 = (y - x_1)(y - x_2)(y + x_1)(y + x_2);$$

so each $x_i = \pm\sqrt{\frac{z_1 \pm \sqrt{z_1^2 - 4z_2}}{2}}$. This example is tiny and lucky.

Concrete Example: a Dihedral Group

$$D_8 := \langle r_1, r_2 \mid r_1^2 = r_2^2 = (r_1 r_2)^4 = 1 \rangle$$

acts by reflections on $\mathbb{C}^2$ by

$$r_1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \text{and} \qquad r_2 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

and on polynomials $p(\mathbf{x}) \in S = \mathbb{C}[x_1, x_2]$ by

$$r_1 \cdot p(x_1, x_2) = p(x_1, -x_2) \qquad \text{and} \qquad r_2 \cdot p(x_1, x_2) = p(x_2, x_1).$$

The algebra of D_8-invariants is $S^{D_8} = \mathbb{C}[z_1, z_2]$, where

$$z_1 := x_1^2 + x_2^2 \qquad \text{and} \qquad z_2 := x_1^2 x_2^2.$$

Here $L = \mathbb{C}(x_1, x_2)$ is the splitting field over $K = \mathbb{C}(z_1, z_2)$ of

$$p(y) = y^4 - z_1 y^2 + z_2 = (y - x_1)(y - x_2)(y + x_1)(y + x_2);$$

so each $x_i = \pm\sqrt{\frac{z_1 \pm \sqrt{z_1^2 - 4z_2}}{2}}$. This example is tiny and lucky.

Concrete Example: an Icosahedral Group

$$G_{19} := \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \frac{\zeta_3}{2}\begin{pmatrix} -1-\zeta_4 & 1-\zeta_4 \\ -1-\zeta_4 & -1+\zeta_4 \end{pmatrix}, \frac{\zeta_5^2}{2}\begin{pmatrix} \tau+\zeta_4 & -\tau+1 \\ \tau-1 & -\tau-\zeta_4 \end{pmatrix} \right\rangle,$$

where $\zeta_r := \exp(2\pi\sqrt{-1}/r)$ and $\tau := \frac{1+\sqrt{5}}{2}$.

The algebra of G_{19}-invariants is $S^{G_{19}} = \mathbb{C}[z_1, z_2]$, where

$$z_1 := \begin{pmatrix} x_1^{20} - \frac{38\sqrt{5}}{3}x_1^{18}x_2^2 - 19x_1^{16}x_2^4 - 152\sqrt{5}x_1^{14}x_2^6 - 494x_1^{12}x_2^8 + \frac{988\sqrt{5}}{3}x_1^{10}x_2^{10} \\ -494x_1^8x_2^{12} - 152\sqrt{5}x_1^6x_2^{14} - 19x_1^4x_2^{16} - \frac{38\sqrt{5}}{3}x_1^2x_2^{18} + x_2^{20} \end{pmatrix}^3;$$

$$z_2 := \begin{pmatrix} x_1^{29}x_2 - \frac{116}{9\sqrt{5}}x_1^{27}x_2^3 + \frac{1769}{25}x_1^{25}x_2^5 + \frac{464}{\sqrt{5}}x_1^{23}x_2^7 + \frac{2001}{5}x_1^{21}x_2^9 - \frac{2668}{3\sqrt{5}}x_1^{19}x_2^{11} + \frac{12673}{5}x_1^{17}x_2^{13} \\ -\frac{12673}{5}x_1^{13}x_2^{17} + \frac{2668}{3\sqrt{5}}x_1^{11}x_2^{19} - \frac{2001}{5}x_1^9x_2^{21} - \frac{464}{\sqrt{5}}x_1^7x_2^{23} - \frac{1769}{25}x_1^5x_2^{25} + \frac{116}{9\sqrt{5}}x_1^3x_2^{27} - x_1x_2^{29} \end{pmatrix}^2.$$

Now $|G_{19}| = 3600$. It is not impossible to compute $p(y) \in K[y]$ such that L is its splitting field in this case. It is immediate that such a $p(y)$ must have degree at least 10 (perhaps at least 30).

Moreover, it is impossible to solve for $\mathbf{x}$ in terms of $\mathbf{z}$ using radicals because G_{19} is not solvable. This example is small-ish and unlucky.

Concrete Example: an Icosahedral Group

$$G_{19} := \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \frac{\zeta_3}{2}\begin{pmatrix} -1-\zeta_4 & 1-\zeta_4 \\ -1-\zeta_4 & -1+\zeta_4 \end{pmatrix}, \frac{\zeta_5^2}{2}\begin{pmatrix} \tau+\zeta_4 & -\tau+1 \\ \tau-1 & -\tau-\zeta_4 \end{pmatrix} \right\rangle,$$

where $\zeta_r := \exp(2\pi\sqrt{-1}/r)$ and $\tau := \frac{1+\sqrt{5}}{2}$.

The algebra of G_{19}-invariants is $S^{G_{19}} = \mathbb{C}[z_1, z_2]$, where

$$z_1 := \begin{pmatrix} x_1^{20} - \frac{38\sqrt{5}}{3}x_1^{18}x_2^2 - 19x_1^{16}x_2^4 - 152\sqrt{5}x_1^{14}x_2^6 - 494x_1^{12}x_2^8 + \frac{988\sqrt{5}}{3}x_1^{10}x_2^{10} \\ -494x_1^8x_2^{12} - 152\sqrt{5}x_1^6x_2^{14} - 19x_1^4x_2^{16} - \frac{38\sqrt{5}}{3}x_1^2x_2^{18} + x_2^{20} \end{pmatrix}^3;$$

$$z_2 := \begin{pmatrix} x_1^{29}x_2 - \frac{116}{9\sqrt{5}}x_1^{27}x_2^3 + \frac{1769}{25}x_1^{25}x_2^5 + \frac{464}{\sqrt{5}}x_1^{23}x_2^7 + \frac{2001}{5}x_1^{21}x_2^9 - \frac{2668}{3\sqrt{5}}x_1^{19}x_2^{11} + \frac{12673}{5}x_1^{17}x_2^{13} \\ -\frac{12673}{5}x_1^{13}x_2^{17} + \frac{2668}{3\sqrt{5}}x_1^{11}x_2^{19} - \frac{2001}{5}x_1^9x_2^{21} - \frac{464}{\sqrt{5}}x_1^7x_2^{23} - \frac{1769}{25}x_1^5x_2^{25} + \frac{116}{9\sqrt{5}}x_1^3x_2^{27} - x_1x_2^{29} \end{pmatrix}^2.$$

Now $|G_{19}| = 3600$. It is not impossible to compute $p(y) \in K[y]$ such that L is its splitting field in this case. It is immediate that such a $p(y)$ must have degree at least 10 (perhaps at least 30).

Moreover, it is impossible to solve for $\mathbf{x}$ in terms of $\mathbf{z}$ using radicals because G_{19} is not solvable. This example is small-ish and unlucky.

Concrete Example: an Icosahedral Group

$$G_{19} := \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \frac{\zeta_3}{2} \begin{pmatrix} -1-\zeta_4 & 1-\zeta_4 \\ -1-\zeta_4 & -1+\zeta_4 \end{pmatrix}, \frac{\zeta_5^2}{2} \begin{pmatrix} \tau+\zeta_4 & -\tau+1 \\ \tau-1 & -\tau-\zeta_4 \end{pmatrix} \right\rangle,$$

where $\zeta_r := \exp(2\pi\sqrt{-1}/r)$ and $\tau := \frac{1+\sqrt{5}}{2}$.

The algebra of G_{19}-invariants is $S^{G_{19}} = \mathbb{C}[z_1, z_2]$, where

$$z_1 := \begin{pmatrix} x_1^{20} - \frac{38\sqrt{5}}{3}x_1^{18}x_2^2 - 19x_1^{16}x_2^4 - 152\sqrt{5}x_1^{14}x_2^6 - 494x_1^{12}x_2^8 + \frac{988\sqrt{5}}{3}x_1^{10}x_2^{10} \\ -494x_1^8x_2^{12} - 152\sqrt{5}x_1^6x_2^{14} - 19x_1^4x_2^{16} - \frac{38\sqrt{5}}{3}x_1^2x_2^{18} + x_2^{20} \end{pmatrix}^3;$$

$$z_2 := \begin{pmatrix} x_1^{29}x_2 - \frac{116}{9\sqrt{5}}x_1^{27}x_2^3 + \frac{1769}{25}x_1^{25}x_2^5 + \frac{464}{\sqrt{5}}x_1^{23}x_2^7 + \frac{2001}{5}x_1^{21}x_2^9 - \frac{2668}{3\sqrt{5}}x_1^{19}x_2^{11} + \frac{12673}{5}x_1^{17}x_2^{13} \\ -\frac{12673}{5}x_1^{13}x_2^{17} + \frac{2668}{3\sqrt{5}}x_1^{11}x_2^{19} - \frac{2001}{5}x_1^9x_2^{21} - \frac{464}{\sqrt{5}}x_1^7x_2^{23} - \frac{1769}{25}x_1^5x_2^{25} + \frac{116}{9\sqrt{5}}x_1^3x_2^{27} - x_1x_2^{29} \end{pmatrix}^2.$$

Now $|G_{19}| = 3600$. It is not impossible to compute $p(y) \in K[y]$ such that L is its splitting field in this case. It is immediate that such a $p(y)$ must have degree at least 10 (perhaps at least 30).

Moreover, it is impossible to solve for $\mathbf{x}$ in terms of $\mathbf{z}$ using radicals because G_{19} is not solvable. This example is small-ish and unlucky.

Complex Reflection Groups as Differential Galois Groups

The standard derivations $\frac{\partial}{\partial z_i}$ on $K = \mathbb{C}(z_1, \ldots, z_n)$ extend uniquely to pairwise commuting derivations δ_i on $L = \mathbb{C}(x_1, \ldots, x_n)$, and by Kolchin's Theorem,

$$\underline{L \text{ is a Picard-Vessiot extension of } K}.$$

So there must exist (and we would like to compute explicitly):

- $A_1, \ldots, A_n \in \mathfrak{gl}_N(K)$ satisfying the integrability conditions

$$\delta_i(A_j) - \delta_j(A_i) = A_iA_j - A_jA_i \qquad \text{for} \quad 1 \leq i, j \leq N; \text{ and}$$

- a fundamental matrix $U \in \mathrm{GL}_N(L)$ such that $L = K(U)$ and

$$\delta_i(U) = A_i U \qquad \text{for} \quad 1 \leq i \leq n.$$

Complex Reflection Groups as Differential Galois Groups

The standard derivations $\frac{\partial}{\partial z_i}$ on $K = \mathbb{C}(z_1, \ldots, z_n)$ extend uniquely to pairwise commuting derivations δ_i on $L = \mathbb{C}(x_1, \ldots, x_n)$, and by Kolchin's Theorem,

$$\underline{L \text{ is a Picard-Vessiot extension of } K}.$$

So there must exist (and we would like to compute explicitly):

- $A_1, \ldots, A_n \in \mathfrak{gl}_N(K)$ satisfying the integrability conditions

$$\delta_i(A_j) - \delta_j(A_i) = A_iA_j - A_jA_i \qquad \text{for} \quad 1 \leq i, j \leq N; \text{ and}$$

- a fundamental matrix $U \in \mathrm{GL}_N(L)$ such that $L = K(U)$ and

$$\delta_i(U) = A_iU \qquad \text{for} \quad 1 \leq i \leq n.$$

Realizing Reflection Groups as PV Groups: Obstacles

By general theory, L is a PV extension of K with $\mathrm{Gal}_\Delta(L/K) \simeq G$.

Goal: Construct an explicit integrable system of linear differential equations $\delta_i Y = A_i Y$ over K whose PV field is L.

Obstacle 1: How to compute explicitly the action of $\delta_i \in \Delta$ on L?

- Normally, to find $\delta(\alpha)$ for $\alpha \in L$ we first find a separable polynomial $0 \neq p(y) \in K[y]$ such that $p(\alpha) = 0$ and set $\delta(\alpha) = -p^\delta(\alpha)/p'(\alpha)$.

Obstacle 2: How do we guarantee integrability?

- A familiar Wronskian trick produces a scalar differential equation for each δ_i whose solution space is spanned by $x_1, \ldots, x_n$. But the associated companion matrix equations do not form an integrable system.

Obstacle 3: How large does the system have to be?

- We know L is a $|G|$-dimensional Δ-K-module, but $|G|$ is LARGE.
- The z_i are often unwieldy polynomials — it is reasonable to expect the matrix entries of the A_i to be unreasonable in general.

Realizing Reflection Groups as PV Groups: Obstacles

By general theory, L is a PV extension of K with $\mathrm{Gal}_\Delta(L/K) \simeq G$.

Goal: Construct an explicit integrable system of linear differential equations $\delta_i Y = A_i Y$ over K whose PV field is L.

Obstacle 1: How to compute explicitly the action of $\delta_i \in \Delta$ on L?

- Normally, to find $\delta(\alpha)$ for $\alpha \in L$ we first find a separable polynomial $0 \neq p(y) \in K[y]$ such that $p(\alpha) = 0$ and set $\delta(\alpha) = -p^\delta(\alpha)/p'(\alpha)$.

Obstacle 2: How do we guarantee integrability?

- A familiar Wronskian trick produces a scalar differential equation for each δ_i whose solution space is spanned by $x_1, \ldots, x_n$. But the associated companion matrix equations do not form an integrable system.

Obstacle 3: How large does the system have to be?

- We know L is a $|G|$-dimensional Δ-K-module, but $|G|$ is LARGE.
- The z_i are often unwieldy polynomials — it is reasonable to expect the matrix entries of the A_i to be unreasonable in general.

Realizing Reflection Groups as PV Groups: Obstacles

By general theory, L is a PV extension of K with $\mathrm{Gal}_\Delta(L/K) \simeq G$.

Goal: Construct an explicit integrable system of linear differential equations $\delta_i Y = A_i Y$ over K whose PV field is L.

Obstacle 1: How to compute explicitly the action of $\delta_i \in \Delta$ on L?

- Normally, to find $\delta(\alpha)$ for $\alpha \in L$ we first find a separable polynomial $0 \neq p(y) \in K[y]$ such that $p(\alpha) = 0$ and set $\delta(\alpha) = -p^\delta(\alpha)/p'(\alpha)$.

Obstacle 2: How do we guarantee integrability?

- A familiar Wronskian trick produces a scalar differential equation for each δ_i whose solution space is spanned by $x_1, \ldots, x_n$. But the associated companion matrix equations do not form an integrable system.

Obstacle 3: How large does the system have to be?

- We know L is a $|G|$-dimensional Δ-K-module, but $|G|$ is LARGE.
- The z_i are often unwieldy polynomials — it is reasonable to expect the matrix entries of the A_i to be unreasonable in general.

Realizing Reflection Groups as PV Groups: Obstacles

By general theory, L is a PV extension of K with $\mathrm{Gal}_\Delta(L/K) \simeq G$.

Goal: Construct an explicit integrable system of linear differential equations $\delta_i Y = A_i Y$ over K whose PV field is L.

Obstacle 1: How to compute explicitly the action of $\delta_i \in \Delta$ on L?

- Normally, to find $\delta(\alpha)$ for $\alpha \in L$ we first find a separable polynomial $0 \neq p(y) \in K[y]$ such that $p(\alpha) = 0$ and set $\delta(\alpha) = -p^\delta(\alpha)/p'(\alpha)$.

Obstacle 2: How do we guarantee integrability?

- A familiar Wronskian trick produces a scalar differential equation for each δ_i whose solution space is spanned by $x_1, \ldots, x_n$. But the associated companion matrix equations do not form an integrable system.

Obstacle 3: How large does the system have to be?

- We know L is a $|G|$-dimensional Δ-K-module, but $|G|$ is LARGE.
- The z_i are often unwieldy polynomials — it is reasonable to expect the matrix entries of the A_i to be unreasonable in general.

Realizing Reflection Groups as PV Groups: Examples

For tiny and lucky D_8 we computed the integrable system

$$\delta_1(Y) = \frac{1}{z_1^2-4z_2}\begin{pmatrix} \frac{z_1}{2} & -1 \\ -z_2 & \frac{z_1}{2} \end{pmatrix} Y; \quad \delta_2(Y) = \frac{1}{z_1^2-4z_2}\begin{pmatrix} -1 & \frac{z_1}{2z_2} \\ \frac{z_1}{2} & \frac{z_1^2-6z_2}{2z_2} \end{pmatrix} Y.$$

This is not bad, but not better than $p(y) = y^4 - z_1 y^2 + z_2 = 0$.

- For cyclic and imprimitive groups one can write down the $p(y) \in K[y]$ immediately – our differential equations are never simpler in these cases.

For small-ish and unlucky G_{19} we computed the integrable system

$$\delta_1(Y) = \frac{1}{z_1+60\sqrt{5}z_2}\begin{pmatrix} \frac{59}{60} + \frac{40\sqrt{5}z_2}{z_1} & -19\sqrt{5} \\ -\frac{29z_2}{60z_1} & -\frac{29}{60} \end{pmatrix} Y;$$

$$\delta_2(Y) = \frac{1}{z_1+60\sqrt{5}z_2}\begin{pmatrix} -19\sqrt{5} & -\frac{19\sqrt{5}z_1}{z_2} \\ -\frac{29}{60} & \frac{z_1+118\sqrt{5}z_2}{2z_2} \end{pmatrix} Y.$$

This is not bad, and much better than $p(y) = ??? \in K[y]$.

Realizing Reflection Groups as PV Groups: Examples

For tiny and lucky D_8 we computed the integrable system

$$\delta_1(Y) = \frac{1}{z_1^2-4z_2}\begin{pmatrix} \frac{z_1}{2} & -1 \\ -z_2 & \frac{z_1}{2} \end{pmatrix} Y; \quad \delta_2(Y) = \frac{1}{z_1^2-4z_2}\begin{pmatrix} -1 & \frac{z_1}{2z_2} \\ \frac{z_1}{2} & \frac{z_1^2-6z_2}{2z_2} \end{pmatrix} Y.$$

This is not bad, but not better than $p(y) = y^4 - z_1 y^2 + z_2 = 0$.

- For cyclic and imprimitive groups one can write down the $p(y) \in K[y]$ immediately – our differential equations are never simpler in these cases.

For small-ish and unlucky G_{19} we computed the integrable system

$$\delta_1(Y) = \frac{1}{z_1+60\sqrt{5}z_2}\begin{pmatrix} \frac{59}{60} + \frac{40\sqrt{5}z_2}{z_1} & -19\sqrt{5} \\ -\frac{29z_2}{60z_1} & -\frac{29}{60} \end{pmatrix} Y;$$

$$\delta_2(Y) = \frac{1}{z_1+60\sqrt{5}z_2}\begin{pmatrix} -19\sqrt{5} & -\frac{19\sqrt{5}z_1}{z_2} \\ -\frac{29}{60} & \frac{z_1+118\sqrt{5}z_2}{2z_2} \end{pmatrix} Y.$$

This is not bad, and much better than $p(y) = ??? \in K[y]$.

Realizing Reflection Groups as PV Groups: Recipes (1 of 2)

First we compute $\eta_{ij} \in L$ such that $\delta_j(x_i) = \eta_{ij}$, so that

$$\delta_j = \sum_{i=1}^{n} \eta_{ij} \frac{\partial}{\partial x_i}$$

acting on $L = \mathbb{C}(x_1, \ldots, x_n)$. For the *Jacobian matrix*

$$J := \begin{pmatrix} \frac{\partial z_1}{\partial x_1} & \cdots & \frac{\partial z_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial z_n}{\partial x_1} & \cdots & \frac{\partial z_n}{\partial x_n} \end{pmatrix} \implies J^{-1} = \begin{pmatrix} \eta_{11} & \cdots & \eta_{1n} \\ \vdots & & \vdots \\ \eta_{n1} & \cdots & \eta_{nn} \end{pmatrix}.$$

- Analytic interpretation:
  the coordinates x_i on X° are (algebraic, multivalued, holomorphic) functions $\chi_i(z_1, \ldots, z_n)$ of the coordinates z_j on Z°.
  In fact $\omega^\circ(\mathbf{x}) = \mathbf{z} = (\phi_1(\mathbf{x}), \ldots, \phi_n(\mathbf{x}))$ (where ϕ_i are the fundamental invariants), and (locally) $(\omega^\circ)^{-1}(\mathbf{z}) = (\chi_1(\mathbf{z}), \ldots, \chi_n(\mathbf{z}))$.
  Now $J = \mathrm{Jac}(\omega^\circ)$ so $J^{-1} = \mathrm{Jac}((\omega^\circ)^{-1})$, i.e., $\eta_{ij} = \frac{\partial \chi_i}{\partial z_j}$.

Realizing Reflection Groups as PV Groups: Recipes (1 of 2)

First we compute $\eta_{ij} \in L$ such that $\delta_j(x_i) = \eta_{ij}$, so that

$$\delta_j = \sum_{i=1}^{n} \eta_{ij} \frac{\partial}{\partial x_i}$$

acting on $L = \mathbb{C}(x_1, \ldots, x_n)$. For the *Jacobian matrix*

$$J := \begin{pmatrix} \frac{\partial z_1}{\partial x_1} & \cdots & \frac{\partial z_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial z_n}{\partial x_1} & \cdots & \frac{\partial z_n}{\partial x_n} \end{pmatrix} \implies J^{-1} = \begin{pmatrix} \eta_{11} & \cdots & \eta_{1n} \\ \vdots & & \vdots \\ \eta_{n1} & \cdots & \eta_{nn} \end{pmatrix}.$$

- Analytic interpretation:
  the coordinates x_i on X° are (algebraic, multivalued, holomorphic) functions $\chi_i(z_1, \ldots, z_n)$ of the coordinates z_j on Z°.
  In fact $\omega^\circ(\mathbf{x}) = \mathbf{z} = (\phi_1(\mathbf{x}), \ldots, \phi_n(\mathbf{x}))$ (where ϕ_i are the fundamental invariants), and (locally) $(\omega^\circ)^{-1}(\mathbf{z}) = (\chi_1(\mathbf{z}), \ldots, \chi_n(\mathbf{z}))$.
  Now $J = \mathrm{Jac}(\omega^\circ)$ so $J^{-1} = \mathrm{Jac}((\omega^\circ)^{-1})$, i.e., $\eta_{ij} = \frac{\partial \chi_i}{\partial z_j}$.

Realizing Reflection Groups as PV Groups: Recipes (2 of 2)

Now that we computed the action of δ_i on L from the entries of the inverse of the Jacobian matrix J for the polynomial map $\mathbf{x} \mapsto \mathbf{z}$, we can next compute:

$$A_i := \delta_i(J)J^{-1} \quad \text{for} \quad 1 \leq i \leq n.$$

Theorem (A.-Bainbridge-Obert-Ullah)

1. $A_i \in \mathrm{gl}_n(K)$ *for each* $1 \leq i \leq n$*;*
2. $\delta_i(A_j) - \delta_j(A_i) = A_iA_j - A_jA_i$ *for* $1 \leq i, j \leq n$*; and*
3. *L is a PV-extension of K for the system* $\mathcal{A} : \delta_i(Y) = A_iY$*.*

Proof sketch.

1. G acts on L by Δ-automorphisms. For M_g the matrix of $g \in G$, the action $g(J) = J \cdot M_g$. So $g(A_i) = A_i$ for all $g \in G$.
2. A familiar computation using the fact that δ_i commute on L.
3. Since $g \mapsto J^{-1}g(J) = M_g$ is injective, G acts faithfully on $L' := K(J) \subseteq L$, so $L' = L$ by the Galois correspondence. $\square$

Realizing Reflection Groups as PV Groups: Recipes (2 of 2)

Now that we computed the action of δ_i on L from the entries of the inverse of the Jacobian matrix J for the polynomial map $\mathbf{x} \mapsto \mathbf{z}$, we can next compute:

$$A_i := \delta_i(J)J^{-1} \quad \text{for} \quad 1 \leq i \leq n.$$

Theorem (A.-Bainbridge-Obert-Ullah)

1. *$A_i \in \mathrm{gl}_n(K)$ for each $1 \leq i \leq n$;*
2. *$\delta_i(A_j) - \delta_j(A_i) = A_iA_j - A_jA_i$ for $1 \leq i, j \leq n$; and*
3. *L is a PV-extension of K for the system $\mathcal{A} : \delta_i(Y) = A_iY$.*

Proof sketch.

1. G acts on L by Δ-automorphisms. For M_g the matrix of $g \in G$, the action $g(J) = J \cdot M_g$. So $g(A_i) = A_i$ for all $g \in G$.
2. A familiar computation using the fact that δ_i commute on L.
3. Since $g \mapsto J^{-1}g(J) = M_g$ is injective, G acts faithfully on $L' := K(J) \subseteq L$, so $L' = L$ by the Galois correspondence. $\square$

Realizing Reflection Groups as PV Groups: Recipes (2 of 2)

Now that we computed the action of δ_i on L from the entries of the inverse of the Jacobian matrix J for the polynomial map $\mathbf{x} \mapsto \mathbf{z}$, we can next compute:

$$A_i := \delta_i(J)J^{-1} \quad \text{for} \quad 1 \leq i \leq n.$$

Theorem (A.-Bainbridge-Obert-Ullah)

1. $A_i \in \mathrm{gl}_n(K)$ *for each* $1 \leq i \leq n$*;*
2. $\delta_i(A_j) - \delta_j(A_i) = A_iA_j - A_jA_i$ *for* $1 \leq i, j \leq n$*; and*
3. *L is a PV-extension of K for the system* $\mathcal{A} : \delta_i(Y) = A_iY$*.*

Proof sketch.

1. G acts on L by Δ-automorphisms. For M_g the matrix of $g \in G$, the action $g(J) = J \cdot M_g$. So $g(A_i) = A_i$ for all $g \in G$.
2. A familiar computation using the fact that δ_i commute on L.
3. Since $g \mapsto J^{-1}g(J) = M_g$ is injective, G acts faithfully on $L' := K(J) \subseteq L$, so $L' = L$ by the Galois correspondence. $\square$

Concluding Remarks

- Our recipe works for any choice of fundamental invariants. Choosing the "wrong" invariants produces disastrous results. Even with the "right" invariants, the A_i are initially written in terms of $\mathbf{x}$, and the rewriting in terms of $\mathbf{z}$ can be very expensive if not handled with care.
- Ours is not the first recipe for realizing reflection groups as differential Galois groups. In Beukers-Heckman[2] there are tables specifying parameters for which the hypergeometric (ordinary!) differential equation $D_{\alpha,\beta}(y) = 0$ has any given reflection group as differential Galois group, where

$$D_{\alpha,\beta} := (\theta + \beta_1 - 1) \cdots (\theta + \beta_n - 1) - z(\theta + \alpha_1) \cdots (\theta + \alpha_n)$$

and $\theta = z\frac{d}{dz}$. We do not yet know in what way(s) our and their realizations are related.

[2] *Monodromy for the hypergeometric function ${}_nF_{n-1}$.* Invent. math. **95**, 325–354, (1989). Thanks to Michael Singer and to Jacques-Arthur Weil for independently pointing out this reference.

Concluding Remarks

- Our recipe works for any choice of fundamental invariants. Choosing the "wrong" invariants produces disastrous results. Even with the "right" invariants, the A_i are initially written in terms of $\mathbf{x}$, and the rewriting in terms of $\mathbf{z}$ can be very expensive if not handled with care.
- Ours is not the first recipe for realizing reflection groups as differential Galois groups. In Beukers-Heckman[2] there are tables specifying parameters for which the hypergeometric (ordinary!) differential equation $D_{\boldsymbol{\alpha},\boldsymbol{\beta}}(y) = 0$ has any given reflection group as differential Galois group, where

$$D_{\boldsymbol{\alpha},\boldsymbol{\beta}} := (\theta + \beta_1 - 1)\cdots(\theta + \beta_n - 1) - z(\theta + \alpha_1)\cdots(\theta + \alpha_n)$$

and $\theta = z\frac{d}{dz}$. We do not yet know in what way(s) our and their realizations are related.

---

[2] *Monodromy for the hypergeometric function ${}_nF_{n-1}$*. Invent. math. **95**, 325–354, (1989). Thanks to Michael Singer and to Jacques-Arthur Weil for independently pointing out this reference.