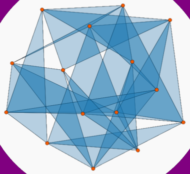


Geometry and arithmetic of components of Hurwitz spaces

Béranger Seguin

Laboratoire Paul Painlevé

July 6th, 2023

Part I.

Motivation and context

Galois theory and its historical role

History

Classical problem: study of (polynomial) equations (e.g. trisection)

Early 19th century: breakthroughs by Abel, Galois, ...

Key objects introduced by Galois:

- **field extensions:** different number systems needed to solve various equations
- **Galois groups:**

  measures the symmetries of an equation

  more complicated Galois group $\approx$ harder to solve

No general solution for equations of degree ≥ 5

$\rightsquigarrow$ Galois shows that some "complicated enough" groups are Galois groups

Inverse/counting problems in Galois theory

Natural question:

Is every finite group the Galois group of a polynomial with rational coefficients?

Inverse Galois Problem (IGP)

Is every finite group isomorphic to the Galois group of a Galois extension of $\mathbb{Q}$?

$$\begin{array}{c} F \\ G \Big| \\ \mathbb{Q} \end{array}$$

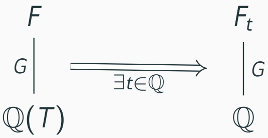
Studied by Hilbert ($\approx$ 1892), Noether ($\approx$ 1918), Shafarevitch ($\approx$ 1954).

The function field case

The regular inverse Galois problem (RIGP)

Is every finite group isomorphic to the Galois group of a Galois extension $F \mid \mathbb{Q}(T)$ with $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$?

Hilbert's irreducibility theorem: For a given group G, RIGP $\Rightarrow$ IGP

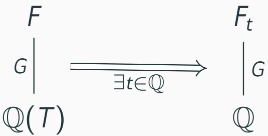


The function field case

The regular inverse Galois problem (RIGP)

Is every finite group isomorphic to the Galois group of a Galois extension $F \mid \mathbb{Q}(T)$ with $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$?

Hilbert's irreducibility theorem: For a given group G, RIGP $\Rightarrow$ IGP



Function fields: extensions are understood geometrically as *covers of the projective line*

Covers and field extensions of function fields

A series of equivalences:

$$\left\{\begin{matrix}\text{extensions of } K(T) \\ \text{with Galois group } G\end{matrix}\right\} \simeq \left\{\begin{matrix}\text{ramified connected covers of } \mathbb{P}^1_K \\ \text{with monodromy group } G\end{matrix}\right\}$$

Covers and field extensions of function fields

A series of equivalences:

$$\left\{\begin{array}{c}\text{extensions of } K(T) \\ \text{with Galois group } G\end{array}\right\} \simeq \left\{\begin{array}{c}\text{ramified connected covers of } \mathbb{P}^1_K \\ \text{with monodromy group } G\end{array}\right\}$$

If K is algebraically closed of characteristic 0, further equivalences:

$$\left\{\begin{array}{c}G\text{-covers of } \mathbb{P}^1_K \\ \text{unramified outside} \\ \{t_1, \dots, t_n\}\end{array}\right\} \simeq \left\{\begin{array}{c}\text{topological } G\text{-covers of} \\ \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \dots, t_n\}\end{array}\right\} \simeq \left\{\begin{array}{c}\text{tuples } (g_1, \dots, g_n) \in G^n \\ \text{where } g_1 \cdots g_n = 1 \\ \text{(modulo conjugacy)}\end{array}\right\}$$

Here a *G-cover* is a ramified Galois cover (algebraic or topological) with an action of G, such that G acts freely/transitively on the (geometric) points of any unramified fiber.

Covers and field extensions of function fields

A series of equivalences:

$$\left\{\begin{matrix}\text{extensions of } K(T) \\ \text{with Galois group } G\end{matrix}\right\} \simeq \left\{\begin{matrix}\text{ramified connected covers of } \mathbb{P}^1_K \\ \text{with monodromy group } G\end{matrix}\right\}$$

If K is algebraically closed of characteristic 0, further equivalences:

$$\left\{\begin{matrix}G\text{-covers of } \mathbb{P}^1_K \\ \text{unramified outside} \\ \{t_1, \dots, t_n\}\end{matrix}\right\} \simeq \left\{\begin{matrix}\text{topological } G\text{-covers of} \\ \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \dots, t_n\}\end{matrix}\right\} \simeq \left\{\begin{matrix}\text{tuples } (g_1, \dots, g_n) \in G^n \\ \text{where } g_1 \cdots g_n = 1 \\ \text{(modulo conjugacy)}\end{matrix}\right\}$$

Here a *G-cover* is a ramified Galois cover (algebraic or topological) with an action of G, such that G acts freely/transitively on the (geometric) points of any unramified fiber.

The regular inverse problem over K

Is every finite group the automorphism group of a connected cover of $\mathbb{P}^1$ over K?

Fields of definition of covers

Over $\mathbb{C}$ and $\overline{\mathbb{Q}}$ $\rightsquigarrow$ Yes by topological arguments!

Idea

To find G-covers of $\mathbb{P}^1_{\mathbb{Q}}$, find G-covers of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ which are invariant under the Galois action of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$

Works when G is centerless (e.g. G is simple noncyclic)

Fields of definition of covers

Over $\mathbb{C}$ and $\overline{\mathbb{Q}}$ $\rightsquigarrow$ Yes by topological arguments!

Idea

To find G-covers of $\mathbb{P}^1_{\mathbb{Q}}$, find G-covers of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ which are invariant under the Galois action of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$

Works when G is centerless (e.g. G is simple noncyclic)

Example: rigidity

Find properties invariant under the Galois action and prove that they uniquely characterize a given cover (e.g. conjugacy classes of monodromy elements)

Thompson (1984): the Monster group is a Galois group over $\mathbb{Q}$

Covers: a language between geometry and arithmetic

Geometry

Extensions of $\overline{\mathbb{Q}}(T)$

↕

Ramified algebraic covers of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$

↔

Topological covers of the punctured sphere

↕

Tuples of elements of a group

Dessins d'enfants

Combinatorics

Arithmetic

Extensions of $\mathbb{Q}(T)$ → Extensions of $\mathbb{Q}$

↕

Ramified algebraic covers of $\mathbb{P}^1_{\mathbb{Q}}$

- **Inverse Galois problem:**
  Is every finite group the Galois group of an extension of $\mathbb{Q}$?
- **Malle conjecture:**
  Count extensions with a given Galois group by discriminant.

Hurwitz moduli spaces

A further geometrization of the problem: **Hurwitz spaces**

- **moduli spaces** for G-covers of $\mathbb{P}^1$ ramified at n points: each point is a G-cover
- itself a cover of the space of configurations Conf_n of n points of $\mathbb{P}^1(\mathbb{C})$.
- variants:

  Hurwitz space of **marked** G-covers

  subspace of **connected** G-covers, or covers of monodromy group H

  possibility to **fix the monodromy classes**

Hurwitz moduli spaces

A further geometrization of the problem: **Hurwitz spaces**

- **moduli spaces** for G-covers of $\mathbb{P}^1$ ramified at n points: each point is a G-cover
- itself a cover of the space of configurations Conf_n of n points of $\mathbb{P}^1(\mathbb{C})$.
- variants:

  Hurwitz space of **marked** G-covers

  subspace of **connected** G-covers, or covers of monodromy group H

  possibility to **fix the monodromy classes**

The Hurwitz space is the analytification ($\mathbb{C}$-points) of a scheme over $\mathbb{Z}[\frac{1}{|G|}]$:

$\mathbb{Q}$-points of the Hurwitz scheme	$\approx$	G-covers defined over $\mathbb{Q}$	$\approx$	extensions of $\mathbb{Q}(T)$ with Galois group G	$\rightsquigarrow$	extensions of $\mathbb{Q}$ with Galois group G

Turns RIGP into a **Diophantine problem**: *we look for rational points on Hurwitz spaces*

Part II.
Connected components of Hurwitz spaces and their asymptotics

Why count components?

G a group, c a conjugacy class which generates G.

Since 2009, Ellenberg, Tran, Venkatesh, Westerland:

Study extensions of $\mathbb{F}_q(T)$	$\Leftarrow$	Count $\mathbb{F}_q$-points of Hurwitz spaces	$\Leftarrow$	Homology of Hurwitz spaces + Grothendieck-Lefschetz trace formula

EVW 2012: as the number of branch points grows, the homology is eventually stable when: *for all subgroups $H \subseteq G$, if $c \cap H$ is nonempty, then it is a conjugacy class of H.*

Why count components?

G a group, c a conjugacy class which generates G.

Since 2009, Ellenberg, Tran, Venkatesh, Westerland:

Study extensions of $\mathbb{F}_q(T)$	$\Leftarrow$	Count $\mathbb{F}_q$-points of Hurwitz spaces	$\Leftarrow$	Homology of Hurwitz spaces + Grothendieck-Lefschetz trace formula

EVW 2012: as the number of branch points grows, the homology is eventually stable when: *for all subgroups $H \subseteq G$, if $c \cap H$ is nonempty, then it is a conjugacy class of H.*

Count components (i.e. H_0) in the general case:

c

$$c \cap H = d_1 \sqcup d_2 \sqcup \dots \sqcup d_{\Omega(H)+1}$$

$\Omega(H)$ is the **splitting number** of H. What happens if $\Omega(H) > 0$?

The gluing operation

Gluing

Two marked G-covers can be glued (over $\mathbb{C}$ or $\overline{\mathbb{Q}}$)

# of branch points	n	n'	$\rightarrow$	$n + n'$
Monodromy group	H	H'	$\rightarrow$	$\langle H, H' \rangle$
Monodromy elements	$(g_1, \dots, g_n)$	$(g'_1, \dots, g'_{n'})$	$\rightarrow$	$(g_1, \dots, g_n, g'_1, \dots, g'_{n'})$

$\rightsquigarrow$ gluing operation at the level of components

The gluing operation

Gluing

Two marked G-covers can be glued (over $\mathbb{C}$ or $\overline{\mathbb{Q}}$)

# of branch points	n	n'	$\to$	$n+n'$
Monodromy group	H	H'	$\to$	$\langle H, H' \rangle$
Monodromy elements	$(g_1, \ldots, g_n)$	$(g'_1, \ldots, g'_{n'})$	$\to$	$(g_1, \ldots, g_n, g'_1, \ldots, g'_{n'})$

$\rightsquigarrow$ gluing operation at the level of components

$\rightsquigarrow$ a **monoid of components** (and its associated monoid ring over a field k)

Count components of Hurwitz spaces = study the Hilbert function of that ring.

General philosophy: asymptotical behaviour

Why is this easier?

Guiding principle

Many branch points $\rightsquigarrow$ the monoid of components behaves like a group.

We can reason as if components had ”inverses”: very useful for counting.

EVW-Wood describe the corresponding group in terms of group homology.

Counting results

Theorem 4.3.1

The count of components of the Hurwitz space of **marked** G-covers of the **affine** line $\mathbb{A}^1(\mathbb{C})$, branched at n points, with monodromy elements belonging to c and monodromy group H, is asymptotically equivalent to:

$$\frac{|H|\,|H_2(H,c)|}{|H^{\mathrm{ab}}|\,\Omega(H)!}\,n^{\Omega(H)}.$$

Counting results

Theorem 4.3.1

The count of components of the Hurwitz space of **marked** G-covers of the **affine** line $\mathbb{A}^1(\mathbb{C})$, branched at n points, with monodromy elements belonging to c and monodromy group H, is asymptotically equivalent to:

$$\frac{|H|\,|H_2(H,c)|}{|H^{\mathrm{ab}}|\,\Omega(H)!}\,n^{\Omega(H)}.$$

If the affine line is replaced by the **projective** line $\mathbb{P}^1(\mathbb{C})$, an average order of this count is given by:

$$\frac{|H_2(H,c)|}{|H^{\mathrm{ab}}|\,\Omega(H)!}\,n^{\Omega(H)}.$$

Overview of the argument

Step 1

Count the number of ways that the conjugacy classes of H included in $c \cap H$ can be attributed to n different branch points. Asymptotically:

$$\frac{n^{\Omega(H)}}{\Omega(H)!}$$

Overview of the argument

Step 1

Count the number of ways that the conjugacy classes of H included in $c \cap H$ can be attributed to n different branch points. Asymptotically:

$$\frac{n^{\Omega(H)}}{\Omega(H)!}$$

Step 2

Show that for most choices, there are exactly:

$$\frac{|H|\,|H_2(H,c)|}{|H^{\mathrm{ab}}|}$$

components (in the affine case).

The case of symmetric groups

If $G = \mathfrak{S}_d$, $c = \{\text{transpositions}\}$ (classical case of Lüroth/Clebsch/Hurwitz):

- A presentation of the ring of components (Theorem 6.1.1):

$$R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c) \simeq \frac{k[(X_{ij})_{1\leq i<j\leq d}]}{(X_{ij}X_{jk} - X_{ik}X_{jk},\ X_{ij}X_{jk} - X_{ij}X_{ik})_{1\leq i<j<k\leq d}},$$

The case of symmetric groups

If $G = \mathfrak{S}_d$, $c = \{\text{transpositions}\}$ (classical case of Lüroth/Clebsch/Hurwitz):

- A presentation of the ring of components (Theorem 6.1.1)
- The Hilbert function is a polynomial of degree $d' = \lfloor d/2 \rfloor$ and leading term

$$\begin{aligned} &\frac{d!}{2^{d'}(d')!(d'-1)!} n^{d'-1} && \text{if } d \text{ is even} \\ \left(1 + \frac{d'}{3}\right) &\frac{d!}{2^{d'}(d')!(d'-1)!} n^{d'-1} && \text{if } d \text{ is odd} \end{aligned}$$

The case of symmetric groups

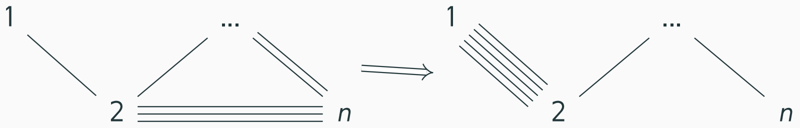
If $G = \mathfrak{S}_d$, $c = \{\text{transpositions}\}$ (classical case of Lüroth/Clebsch/Hurwitz):

- A presentation of the ring of components (Theorem 6.1.1)
- The Hilbert function is a polynomial of degree $d' = \lfloor d/2 \rfloor$ and leading term

$$\frac{d!}{2^{d'}(d')!(d'-1)!} n^{d'-1} \qquad \text{if } d \text{ is even}$$

$$\left(1 + \frac{d'}{3}\right) \frac{d!}{2^{d'}(d')!(d'-1)!} n^{d'-1} \qquad \text{if } d \text{ is odd}$$

- A ”visual” proof of irreducibility using multigraphs:



Braids are interpreted as operations on these graphs (7-Γ-V-equivalence).

The algebraic geometry of the ring of components 1/2

The ring of components for $\mathbb{P}^1(\mathbb{C})$ is commutative $\rightsquigarrow$ geometry

Geometrical takeaways

- The spectrum is stratified in a family of subschemes $\gamma(H)$ for subgroups H

$\rightsquigarrow$ An invitation to the study of the geometry of the homology of Hurwitz spaces.

The algebraic geometry of the ring of components 1/2

The ring of components for $\mathbb{P}^1(\mathbb{C})$ is commutative $\rightsquigarrow$ geometry

Geometrical takeaways

- The spectrum is stratified in a family of subschemes $\gamma(H)$ for subgroups H
- The Krull dimension of $\gamma(H)$ is $\Omega(H) + 1$.
  $\rightsquigarrow$ the Krull dimension of the ring of components is the maximal splitting number $+1$

$\rightsquigarrow$ An invitation to the study of the geometry of the homology of Hurwitz spaces.

The algebraic geometry of the ring of components 1/2

The ring of components for $\mathbb{P}^1(\mathbb{C})$ is commutative $\rightsquigarrow$ geometry

Geometrical takeaways

- The spectrum is stratified in a family of subschemes $\gamma(H)$ for subgroups H
- The Krull dimension of $\gamma(H)$ is $\Omega(H) + 1$.
  $\rightsquigarrow$ the Krull dimension of the ring of components is the maximal splitting number $+1$
- In specific situations (e.g. symmetric groups) we can describe the strata (and hence the spectrum) fully

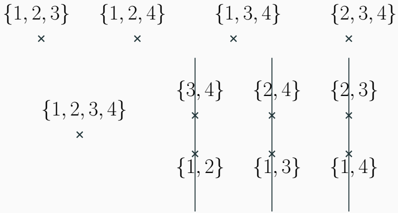
$\rightsquigarrow$ An invitation to the study of the geometry of the homology of Hurwitz spaces.

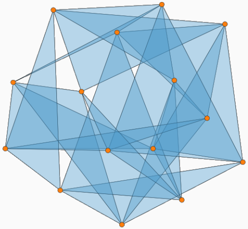
The algebraic geometry of the ring of components 2/2

Unsolved questions

- Which $\gamma(H')$ intersect the closure of $\gamma(H)$? (necessarily $H' \subseteq H$)
- How does the spectrum compare to that of the group ring?
- What can be done with the (braided-commutative) ring for covers of $\mathbb{A}^1(\mathbb{C})$? with higher homology?

Drawings for symmetric groups ($d = 4, 6$):





Part III.

Fields of definition of connected components of Hurwitz spaces

Fields of definition

A rational point of a Hurwitz space has to lie in a component defined over $\mathbb{Q}$.

$\rightsquigarrow$ **Weak form of RIGP:** Find components defined over $\mathbb{Q}$.

A goal

Understand/count components defined over $\mathbb{Q}$.

Previous work: Dèbes-Emsalem, Cau.

Fields of definition and concatenation

Question

Are the components obtained by gluing components defined over $\mathbb{Q}$ also defined over $\mathbb{Q}$?

Gluing is a transcendental operation... Too good to be true?

Fields of definition and concatenation

Question

Are the components obtained by gluing components defined over $\mathbb{Q}$ also defined over $\mathbb{Q}$?

Gluing is a transcendental operation... Too good to be true?

An important starting point:

Theorem (Cau)

If x and y are components defined over $\mathbb{Q}$, the set of "all possible gluings":

$$\{x^{\gamma}y^{\gamma'} \mid (\gamma, \gamma') \in G^2\}$$

is globally defined over $\mathbb{Q}$. If this is a singleton, xy is defined over $\mathbb{Q}$.

A rigidity criterion for rationality

Theorem 8.1.2, i) and ii)

Let x, y be components defined over K. Denote by H_1, H_2 their respective monodromy groups, and let $H = \langle H_1, H_2 \rangle$. Then:

i) If $H_1 H_2 = H$, then xy is defined over K.

ii) If every conjugacy class of H which appears in xy appears at least M times (for some integer M depending only on the group G), then xy is defined over K.

Another result: the $G_{\mathbb{Q}}$-action on components is determined by its action of components with few branch points (Prop 8.2.8). Unsurprising in the light of Belyi's theorem/faithfulness of the Galois action on dessins d'enfants (covers with three branch points). But here we have fixed group/conjugacy classes.

Patching components over a number field

A different result that does not follow from a rigidity principle/Cau's theorem:

Theorem 8.1.2, iii)

Let x, y be components defined over K. Denote by H_1, H_2 their respective monodromy groups, and let $H = \langle H_1, H_2 \rangle$. Then there is an element $\gamma \in H$ such that $H = \langle H_1, H_2^{\gamma} \rangle$ and such that xy^{γ} is defined over K.

Patching components over a number field

Theorem 8.1.2, iii)

Let x, y be components defined over K. Denote by H_1, H_2 their respective monodromy groups, and let $H = \langle H_1, H_2 \rangle$. Then there is an element $\gamma \in H$ such that $H = \langle H_1, H_2^\gamma \rangle$ and such that xy^γ is defined over K.

Sketch of proof.

- Construct a sequence $K_1, K_2, \ldots$ of linearly disjoint extensions of K such that there are marked covers f_i, g_i defined over K_i in the components x, y.
  This is accomplished by using Hilbert's irreducibility theorem repeatedly on Hurwitz spaces themselves.

Patching components over a number field

Theorem 8.1.2, iii)

Let x, y be components defined over K. Denote by H_1, H_2 their respective monodromy groups, and let $H = \langle H_1, H_2 \rangle$. Then there is an element $\gamma \in H$ such that $H = \langle H_1, H_2^\gamma \rangle$ and such that xy^γ is defined over K.

Sketch of proof.

- Construct a sequence $K_1, K_2, \ldots$ of linearly disjoint extensions of K such that there are marked covers f_i, g_i defined over K_i in the components x, y.
- Patch f_i, g_i over the complete valued field $K_i((X))$. A result of Cau ensures that the patched cover lies in a component c_i of the form $x^\gamma y^{\gamma'}$.

Patching components over a number field

Theorem 8.1.2, iii)

Let x, y be components defined over K. Denote by H_1, H_2 their respective monodromy groups, and let $H = \langle H_1, H_2 \rangle$. Then there is an element $\gamma \in H$ such that $H = \langle H_1, H_2^\gamma \rangle$ and such that xy^γ is defined over K.

Sketch of proof.

- Construct a sequence $K_1, K_2, \dots$ of linearly disjoint extensions of K such that there are marked covers f_i, g_i defined over K_i in the components x, y.
- Patch f_i, g_i over the complete valued field $K_i((X))$. A result of Cau ensures that the patched cover lies in a component c_i of the form $x^\gamma y^{\gamma'}$.
- There are finitely many $x^\gamma y^{\gamma'}$ $\rightsquigarrow$ there is some $i \neq i'$ such that $c_i = c_{i'}$.
  It is defined over $\overline{\mathbb{Q}} \cap K_i((X)) \cap K_{i'}((X)) = K$. □

Applications

Proposition 8.4.8

If $\langle g_1, \ldots, g_n \rangle = G$, there is a component def. $/\mathbb{Q}$ of connected G-covers with:

$$|\{i \mid \mathrm{ord}(g_i) = 2\}| + \sum_{i=1}^{n} \varphi(\mathrm{ord}(g_i))$$

branch points.

- **Mathieu group** M_{23}: generated by two order 3 elements $\rightsquigarrow$ 4 branch points. Cau's criterion gave 15 branch points.
- $\mathrm{PSL}_2(16) \rtimes \mathbb{Z}/2\mathbb{Z}$: generated by two order 6 elements $\rightsquigarrow$ 4 branch points.