Galois groups in Enumerative Geometry

London Institute of Mathematical Sciences

23 July 2025

Frank Sottile

sottile@tamu.edu

Work with: Bott, Brooks, Brysiewicz, Leykin, Martín del Campo, Rodriguez, White, Williams, Yahl, and Ying.

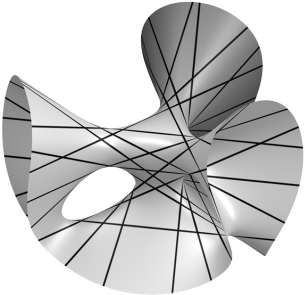
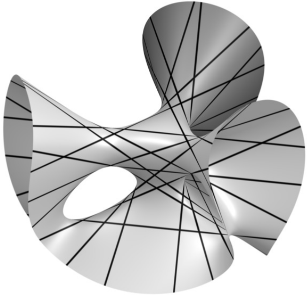


Image courtesy of Oliver Labs

27 Lines on a Cubic Surface



By the Cayley-Salmon Theorem (1849), there are exactly 27 lines on a smooth cubic surface $\mathcal{V}(F) \subset \mathbb{P}^3$.

Schläfli (1858) showed these have a remarkable incidence configuration with symmetry group the Coxeter group E_6.

In his 1870 book (the first book on Galois theory), *Traité des substitutions et des équations algébriques*, Jordan related this to Galois theory.

Suppose that F has rational ($\mathbb{Q}$) coefficients and let K be the field of definition of the lines. Then $K/\mathbb{Q}$ is a Galois extension, and its Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts on the 27 lines.

In fact, he showed that this action is faithful, $\mathrm{Gal}(K/\mathbb{Q}) \subset E_6$.

Modern View

Let us work over $\mathbb{C}$ and consider the incidence variety,

$$\begin{tikzcd}
\Gamma := \{(\ell, F) \in \mathbb{G}(1, \mathbb{P}^3) \times \mathbb{P}^{19}_{\text{cubics}} \,:\, F|_\ell \equiv 0\}\,. \arrow[d] \\
\mathbb{P}^{19}_{\text{cubics}}
\end{tikzcd}$$

The extension $\mathbb{C}(\Gamma)/\mathbb{C}(\mathbb{P}^{19})$ of function fields has degree 27, and if K is the normal closure of $\mathbb{C}(\Gamma)/\mathbb{C}(\mathbb{P}^{19})$, then
$\mathrm{Gal}(K/\mathbb{C}(\mathbb{P}^{19})) = E_6$.
(Many proofs were given in the 20th century.)

Over the locus of smooth cubics (open and dense in $\mathbb{P}^{19}$), this is a covering space of degree 27.

Its monodromy group is also E_6.

Enumerative Geometry

> Enumerative Geometry is the art of determining the number d of geometric figures x having specified positions with respect to other, fixed figures b. — Schubert (1879)

Example: Lines lying on a cubic surface.

$X :=$ the space of the figures x we count, and $B :=$ configuration space of the fixed figures. The *incidence variety* $\Gamma \subset X \times B$ consists of pairs (x, b) where $x \in X$ has the specified position with respect to $b \in B$.

The projection $\Gamma \to B$ has degree d, as its fibers are the solutions.

More generally, a *branched cover* is a dominant map $\pi \colon \Gamma \to B$ of irreducible varieties of the same dimension. Let d be its degree.

Branched covers appear in applications as families (incidence varieties) of systems of polynomial equations.

Galois = Monodromy

Let $\pi\colon \Gamma \to B$ be a branched cover of degree d. Then the extension $\mathbb{C}(\Gamma)/\mathbb{C}(B)$ of function fields has degree d.

Let K be the Galois closure of the field extension $\mathbb{C}(\Gamma)/\mathbb{C}(B)$. The *Galois group* of π is $\mathrm{Gal}_\pi := \mathrm{Gal}(K/\mathbb{C}(B))$.

There is an open dense subset of B over which π is a covering space of degree d. Let Mon_π be the monodromy group.

Both Gal_π and Mon_π are transitive subgroups of the symmetric group $\mathcal{S}_d$, well-defined up to conjugation.

Theorem. [Hermite 1851 $\cdots$ ~~Harris 1979~~ SGA1 V.8.2 1961]
$\mathrm{Gal}_\pi = \mathrm{Mon}_\pi$.

This has an interesting story.

Harris's Principle

In *Galois groups in enumerative geometry* (1979), Harris studied Galois groups of many enumerative problems. Like the 27 lines, some had small (not equal to symmetric group) Galois groups, and he showed how this was explained by structure of their solutions.

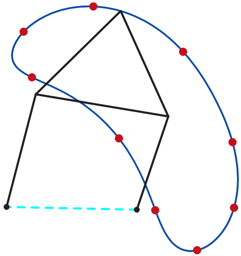
He showed that others—such as the problem of 3264 conics—were fully symmetric and had no apparent structure.

Harris's Principle: An (enumerative) Galois group should be as large as possible, given the structure of the solutions.

A Galois/monodromy group that is not full-symmetric is *enriched*, as the solutions (should be) enriched with extra structure.

Examples of this are in the beautiful paper of Hashimoto and Kadets: *38406501359372282063949 & all that: Monodromy of Fano Problems*.

Some Enriched Problems



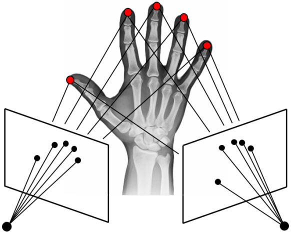
The four bar synthesis problem of Alt is to find the four bar mechanisms whose coupler curve passes through 9 points in the plane. The Roberts-Chebyschev Theorem reveals a hidden symmetry: each coupler curve is generated by three cognate linkages.

Standard formulations have left↔right label-swapping, which implies that the Galois group is enriched, lying in $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^{1442} \rtimes \mathcal{S}_{1442}$.

We still do not have a proof that $6 \cdot 1442 = 8652$ is the correct number, or if the Galois group is the full wreath product (the second, if true, is easier to establish).

Five-point Reconstruction Problem:

Given images of five points in two views of a camera, find the relative pose of the cameras (and the world points).
This problem possesses a hidden symmetry, called a *twisted pair*: Rotating the second camera 180° about the line connecting the two camera centres (and a reflection of the world points) gives a second solution.



This implies that Galois group is a subgroup of $(\mathbb{Z}/2\mathbb{Z})^{10} \rtimes \mathcal{S}_{10}$, which is exploited in solvers.

There are many other examples from applications. To paraphrase Joos Heintz: "You may not care about Galois, but Galois cares about you(r problems)".

Sparse Polynomial Systems

Let $\mathcal{A} \subset \mathbb{Z}^n$ be exponents for monomials in $x_1, \ldots, x_n$. Then

$$f \;=\; \sum_{a \in \mathcal{A}} c_a x^a \qquad (c_a \in \mathbb{C})$$

is a *sparse polynomial* with *support* $\mathcal{A}$. These form the vector space $\mathbb{C}^{\mathcal{A}}$.

Given a list $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ of supports, consider
$\mathbb{C}^{\mathcal{A}_\bullet}$:= space of polynomials $(f_1, \ldots, f_n)$ with $\mathcal{A}_i$ = support of f_i.

Bernstein-Kuchnirenko Theorem. *The number of solutions in* $(\mathbb{C}^\times)^n$ *to a system* $f_1 = \cdots = f_n = 0$ *of polynomials with support* $\mathcal{A}_\bullet$ *is* $\mathrm{MV}(\mathcal{A}_\bullet)$, *the mixed volume of the convex hulls of the* $\mathcal{A}_i$*.*

Let $\Gamma \subset (\mathbb{C}^\times)^n \times \mathbb{C}^{\mathcal{A}_\bullet}$ be the corresponding incidence variety.
Then $\Gamma \to \mathbb{C}^{\mathcal{A}_\bullet}$ is a branched cover of degree $\mathrm{MV}(\mathcal{A}_\bullet)$.

Let $\mathrm{Gal}_{\mathcal{A}_\bullet}$ be the corresponding Galois group of systems with support $\mathcal{A}_\bullet$.

Esterov's Theorem

There are two obvious ways for $\mathrm{Gal}_{\mathcal{A}_\bullet} \neq \mathcal{S}_{\mathrm{MV}(\mathcal{A}_\bullet)}$:

Lacunary: $f(x)$ has the form $g(x^3)$.

Triangular: The system is $f(x,y) = g(y) = 0$.

For both, the system is solved in stages, which implies that $\mathrm{Gal}_{\mathcal{A}_\bullet}$ lies in a wreath product, so that it is imprimitive and is not the full symmetric group.

Esterov's Theorem. *$Gal_{\mathcal{A}_\bullet} = \mathcal{S}_{\mathrm{MV}(\mathcal{A}_\bullet)}$ unless $\mathcal{A}_\bullet$ is lacunary or triangular.*

$\rightsquigarrow$ With Lionel Lang, Alex has been working to understand $\mathrm{Gal}_{\mathcal{A}_\bullet}$. It is still not clear what $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is in general.

You may exploit the imprimitivity given by Esterov's Theorem for solving, even when $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is unknown.
(Joint work with Brysiewicz, Rodriguez, and Yahl.)

The Problem of Four Lines

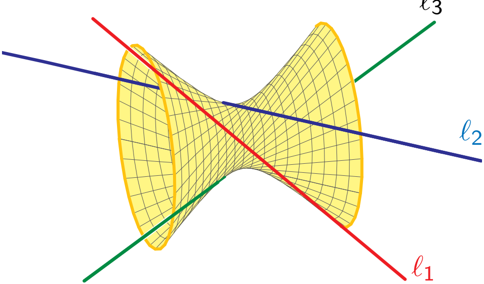
The Problem of Four Lines

What are the lines m_i meeting four general lines ℓ_1, ℓ_2, ℓ_3, and ℓ_4?

The Problem of Four Lines

What are the lines m_i meeting four general lines ℓ_1, ℓ_2, ℓ_3, and ℓ_4?

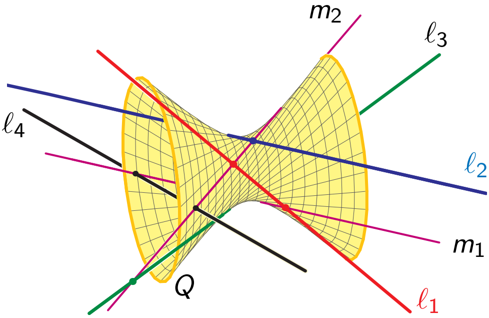
ℓ_1, ℓ_2, ℓ_3 lie on a unique hyperboloid Q of one sheet, and the lines meeting them form one ruling of Q.



The Problem of Four Lines

What are the lines m_i meeting four general lines ℓ_1, ℓ_2, ℓ_3, and ℓ_4?

ℓ_1, ℓ_2, ℓ_3 lie on a unique hyperboloid Q of one sheet, and the lines meeting them form one ruling of Q. The solutions m_i are the lines in that ruling passing through the points of intersection $\ell_4 \cap Q$.

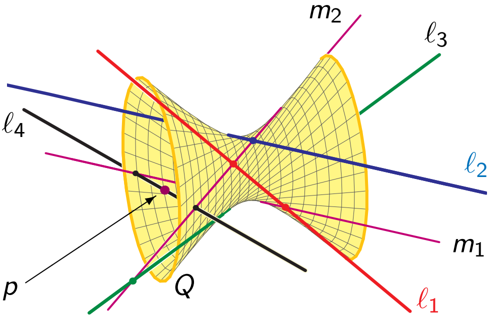


The Problem of Four Lines

What are the lines m_i meeting four general lines ℓ_1, ℓ_2, ℓ_3, and ℓ_4?

ℓ_1, ℓ_2, ℓ_3 lie on a unique hyperboloid Q of one sheet, and the lines meeting them form one ruling of Q. The solutions m_i are the lines in that ruling passing through the points of intersection $\ell_4 \cap Q$.

Rotating the line ℓ_4 180° around the point p interchanges the two solution lines m_1, m_2.

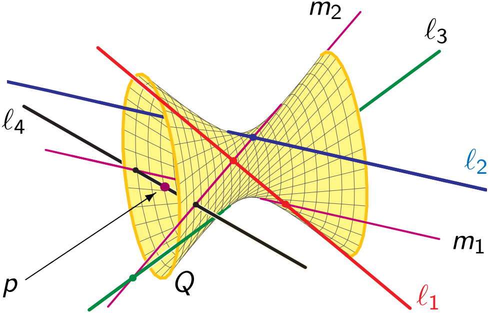


The Problem of Four Lines

What are the lines m_i meeting four general lines ℓ_1, ℓ_2, ℓ_3, and ℓ_4?

ℓ_1, ℓ_2, ℓ_3 lie on a unique hyperboloid Q of one sheet, and the lines meeting them form one ruling of Q. The solutions m_i are the lines in that ruling passing through the points of intersection $\ell_4 \cap Q$.

Rotating the line ℓ_4 180° around the point p interchanges the two solution lines m_1, m_2.



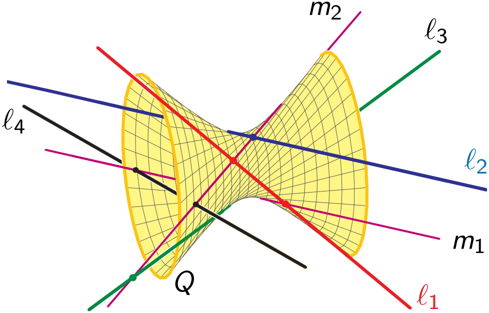
This shows that

The Galois group of the problem of four lines is the symmetric group $\mathcal{S}_2$.

Schubert Problems

The Schubert calculus is an algorithmic method of Schubert to solve a wide class of problems in enumerative geometry.

Schubert problems are problems from enumerative geometry involving linear subspaces of a vector space incident upon other linear spaces, such as the problem of four lines.



As there are many millions of computable Schubert problems, many with their own unique geometry, they provide a rich and convenient laboratory for studying Galois groups of geometric problems.

Schubert Galois Groups

c. 2003 Vakil's Method can show that a Schubert Galois group is at least alternating. All problems on $G(2,n)$ for $n \leq 16$ and on $G(3,n)$ for $n \leq 9$ are at least alternating.

Derksen and Vakil constructed enriched problems, from $G(4,8)$ up. These have Galois group $\mathcal{S}_n \subset \mathcal{S}_{\binom{n}{k}}$ (acting on k-subsets of $[n]$).

2009: With Leykin: Using numerical methods, many simple Schubert problems are full symmetric, including one with 17,589 solutions.

2012: With Brooks and Martín del Campo: All Schubert problems on $G(2,n)$ are at least alternating.

2015: With White: All Schubert problems on $G(3,n)$ are 2-transitive.

2023: With Martín del Campo and Williams: Classified all Schubert problems on $G(4,8)$ and $G(4,9)$. Most (99.5%) are at least alternating.
Those that are not fall into three geometrically distinct families.

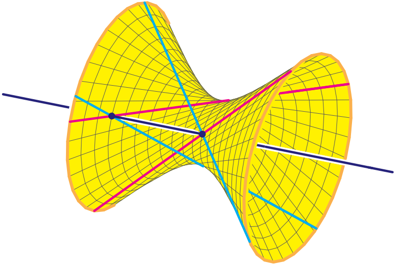
More recent

2022: With Williams and Li Ying: Constructed one of the families: Schubert problems A and B of degrees a and b may be composed to get a new problem with Galois group a subset of the wreath product $(\mathrm{Gal}_A)^b \rtimes \mathrm{Gal}_B$.

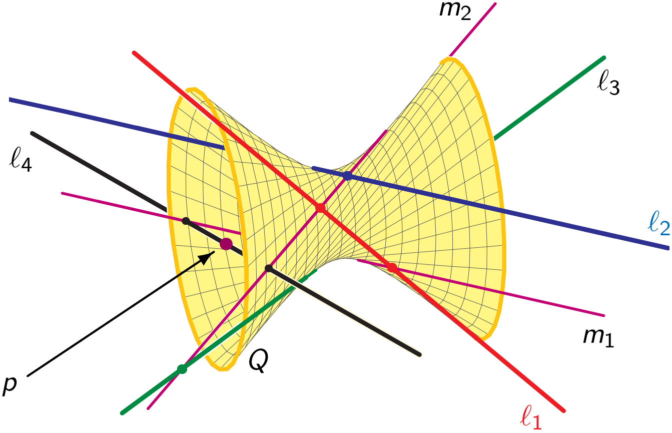
2025: With C.J. Bott: Composed Schubert problems on different Grassmannians to get a new problem on a flag manifold with full wreath product. (Analog of triangular.)

2025: Sophia Liao and Leonid Rybnikov: Used combinatorics to show that most simple Schubert problems on the Grassmannian are at least alternating.

2025: With C.J. Bott: Found many enriched problems on Lagrangian Grassmannians.
Some Galois groups:
D_{2m+3} (Fano problem) and $(\mathbb{Z}/2\mathbb{Z})^n$.



Thank You!



Derksen's example

Q: What 4-planes H in $\mathbb{C}^8$ that meet each of general 4-planes K_1, K_2, K_3, K_4 in a 2-dimensional subspace?

Auxiliary problem: There are four (h_1, h_2, h_3, h_4) 2-planes in $\mathbb{C}^8$ meeting each of K_1, K_2, K_3, K_4. Schematically, $\ydiagram{3}^{4} = 4$.

Fact: All solutions H to our problem have the form $H_{i,j} = \langle h_i, h_j \rangle$ for $1 \leq i < j \leq 4$. Schematically, $\ydiagram{2,2}^{4} = 6$.

It follows that the Galois group of $\ydiagram{2,2}^{4} = 6$ is equal to the Galois group of $\ydiagram{3}^{4} = 4$, which is known to be the symmetric group $\mathcal{S}_4$.

This problem $\ydiagram{2,2}^{4} = 6$ also has exceptional reality: If K_1, K_2, K_3, K_4 are real, then either two or six of the $H_{i,j}$ are real, and never four or zero.

Known Schubert Galois Groups

The three families:

(1) For $1 \leq k < n$, the problem of $2k$-planes in $\mathbb{C}^{2n}$ meeting 4 $\mathbb{C}^n$s in a $\mathbb{C}^k$ has Galois group $\mathcal{S}_n \subset \mathcal{S}_{\binom{n}{k}}$. Call this $\mathcal{G}\binom{n}{k}$.

(2) For Schubert problems λ on $G(k,n)$ and μ on $G(l,m)$, there is a new Schubert problem $\lambda \circ \mu$ on $G(k+l, n+m)$.
The number, $d(\lambda \circ \mu)$ of solutions is the product $d(\lambda) \cdot d(\mu)$ and

$$\mathrm{Gal}_{\lambda\circ\mu} \ \subseteq \ (\mathrm{Gal}_\mu)^{d(\lambda)} \rtimes \mathrm{Gal}_\lambda \,.$$

(3) There is a third, less-understood class.

All known Schubert Galois groups are iterated wreath products of the $\mathcal{G}\binom{n}{k}$.

Conjecture. These are the only Schubert Galois groups.

Hope. Enriched Schubert problems can be classified.

(2) is work with Williams and Ying, and involves interesting combinatorics.

Transitive Permutation Groups

A permutation group $H \subset \mathcal{S}_d$ has an action on $[d]$.
It is transitive if it has only one orbit on $[d]$.
It is t-transitive if it has only one orbit on $[d]^t \smallsetminus \Delta$
(the complement of the diagonal).

There are few highly ($t > 2$) transitive permutation groups.

H is *primitive* is it preserves no nontrivial partition of $[d]$.

Otherwise, H is *imprimitive*.

When H is imprimitive, $d = a \cdot b$ $(1 < a, b)$, so that $[d] = [a] \times [b]$.

Furthermore, the action of H preserves the fibration $[a] \times [b] \to [a]$.

Then H lies in the *wreath product* $(\mathcal{S}_b)^a \rtimes \mathcal{S}_a$.