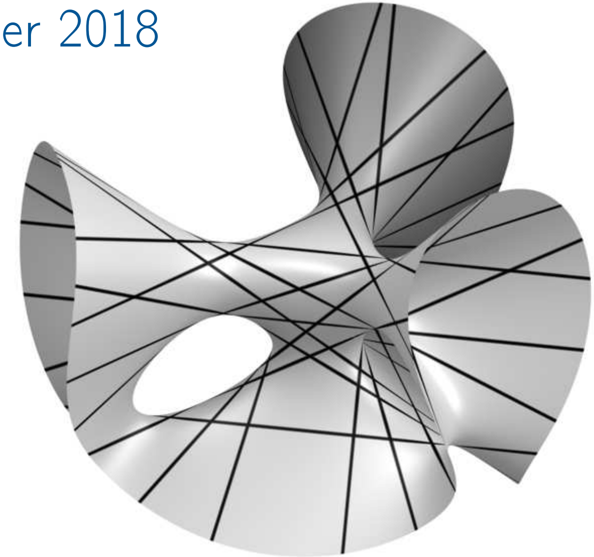
Galois groups for systems of polynomial equations

Algebraic Geometry Session
2018 CMS Winter meeting
10 December 2018



Frank Sottile

sottile@math.tamu.edu

With: Andrew Bridy and Thomas Yahl

Image of cubic surface courtesy of Oliver Labs

Multivariate Galois Theory

We all know that Galois theory arose from attempts first to solve, and then later to understand, the structure of the roots of a univariate polynomial

$$f(z) = 0 .$$

In enumerative geometry and in the applications of algebraic geometry, it is natural to consider the solutions to a system of multivariate polynomials,

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0 .$$

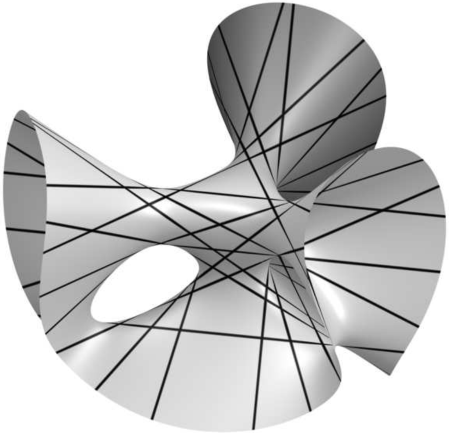
Galois theory likewise informs us about the structure of the solutions, but simply reducing to a univariate setting is often not helpful.

In this multivariate setting or in enumerative geometry, known (or discovered) structure constrains the Galois group and the problem arises to show that the group is as large as possible.

27 Lines on a Cubic Surface

Cayley & Salmon showed that 27 lines lie on a smooth cubic surface in $\mathbb{P}^3$. These lines have a very interesting configuration whose automorphism group is the Coxeter group E_8.

For a cubic defined over $\mathbb{Q}$, the lines are defined over a Galois extension K and Jordan observed that $\mathrm{Gal}(K/\mathbb{Q}) \subset E_8$.



Courtesy of Oliver Labs

Work in the 20th century showed that for a general cubic surface, the Galois group equals E_8.

This is also a monodromy group. Over the $\mathbb{P}^{19} \smallsetminus \Delta$ of smooth cubics the monodromy action on the lines is E_8.

It is also a Galois group of the extension of $\mathbb{C}[\mathbb{P}^{19}]$ to the field over which each line in the family is defined.

Schubert Galois Groups

The Schubert calculus studies problems of linear spaces that satisfy incidence conditions imposed by other linear spaces. It forms a rich laboratory for studying new phenomena in enumerative geometry.

$C.$ 2003 Derksen and Vakil discovered a Schubert problem with Galois group not the full symmetric group. Since then, some themes have emerged.

- Apparent Dichotomy. Known Schubert Galois groups are either the full symmetric group on the solutions or are imprimitive.

- Possible Classification. Discovery and constructions of families of Schubert problems with small Galois group suggests the possibility to classify such *enriched Schubert problems*.

- Inverse Galois Problem. If G is a Schubert Galois group, then so is $G \wr S_n$.

Bernstein's Theorem

An integer vector $\alpha \in \mathbb{Z}^n \rightsquigarrow$ a Laurent monomial $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

A finite subset $\mathcal{A} \subset \mathbb{Z}^n \rightsquigarrow$ a Laurent polynomial with support $\mathcal{A}$,

$$f \;=\; \sum_{\alpha \in \mathcal{A}} c_\alpha x^\alpha \qquad c_\alpha \in \mathbb{C}\,.$$

Write $\mathbb{C}^{\mathcal{A}}$ for the vector space of polynomials with support $\mathcal{A}$.

Theorem. (Bernstein) *Let $\mathcal{A}_1, \ldots, \mathcal{A}_n \subset \mathbb{Z}^n$ be finite sets. For general $(f_1, \ldots, f_n) \in \mathbb{C}^{\mathcal{A}_1} \oplus \cdots \oplus \mathbb{C}^{\mathcal{A}_n}$, the number of solutions to*

$$f_1(x) \;=\; f_2(x) \;=\; \cdots \;=\; f_n(x) \;=\; 0$$

in $(\mathbb{C}^\times)^n$ is the mixed volume of conv$(\mathcal{A}_1), \ldots,$ conv$(\mathcal{A}_n)$.

Question. What does Galois theory have to say about systems of sparse polynomials?

Obstructions to Full Symmetric

While we expect that for typical supports $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$, the generic system will have Galois group $\mathrm{Gal}_{\mathcal{A}_\bullet}$ the full symmetric group $S_{MV(\mathcal{A}_\bullet)}$, there are two obvious ways for this to fail.

I) $n = 1$. $f(x) = g(x^a) = 0$ with $a > 1$.

II) $n = 2$. $f(x, y) = g(y) = 0$.

In both cases, the solutions form a fibration over roots of g.
The Galois group must preserve this fibration, which implies that

$$\mathrm{Gal} \;\subset\; S_a \wr S_b\,,$$

where $b = \deg(g)$ and $a = \deg(f(x, \text{root of } g))$.

Note that the expectation is the Observed Dichotomy, $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is either full symmetric or imprimitive.

Obstructions, Continued

Suppose that $0 \in \mathcal{A}_i$ and write F for $f_1, \dots, f_n$.

I) $\mathbb{Z}\{\mathcal{A}_1, \dots, \mathcal{A}_n\} = \Lambda \subsetneq \mathbb{Z}^n$. Then there is a homomorphism

$$\varphi_{\mathcal{A}_\bullet} \colon (\mathbb{C}^\times)^n \twoheadrightarrow (\mathbb{C}^\times)^n \qquad \text{with} \quad \ker \varphi_{\mathcal{A}_\bullet} = \mathrm{Hom}(\mathbb{Z}^n/\Lambda, \mathbb{C}^\times)$$

s.t. $F(x) = G(\varphi_{\mathcal{A}_\bullet}(x))$ with the support of G spanning $\mathbb{Z}^n$.

II) After reordering, $\exists k$ with $\mathrm{rk}\mathbb{Z}\{\mathcal{A}_1, \dots, \mathcal{A}_k\} = k$, and changing coordinates, $(\mathbb{C}^\times)^n = (\mathbb{C}^\times)^k \times (\mathbb{C}^\times)^{n-k}$, $x = (y; z)$ with

$$F(x) \;=\; G(y), H(y; z)$$

support G is $\mathcal{A}_1, \dots, \mathcal{A}_k$ and support H is $\mathcal{A}_{k+1}, \dots, \mathcal{A}_n$.

Theorem. (Esterov '18) *If I or II do not hold, then* $Gal_{\mathcal{A}_\bullet} = S_{MV(\mathcal{A}_\bullet)}$.

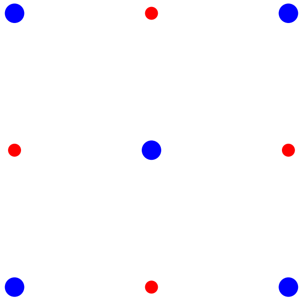
Corollary. *This enables the complete classification of when general polynomial systems with support* $\mathcal{A}_\bullet$ *are solvable in radicals.*

Why this is called research....

Until Friday, Andrew Bridy and I had a 'proof' of a conjecture of Esterov when $n = 2$:

Broken Conjecture. *Suppose that $\mathcal{B}_1, \ldots, \mathcal{B}_n \subset \mathbb{Z}^n$ do not satisfy I or II, and $\lambda\colon \mathbb{Z}^n \xrightarrow{\sim} \Lambda \subsetneq \mathbb{Z}^n$, and $\mathcal{A}_i = \lambda(\mathcal{B}_i)$.*
Then Gal$_{\mathcal{A}_\bullet} = \ker \varphi_{\mathcal{A}_\bullet} \wr S_{MV(\mathcal{B}_\bullet)}$.

Example. (Esterov-Lang)
$\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{A}$
Gal$_{\mathcal{A}_\bullet} = (\mathbb{Z}/2\mathbb{Z} \wr S_4) \cap A_8$.

$\mathcal{A} =$ 

Obstruction. No edge of conv$\mathcal{A}$ is primitive, and the edges are 'dependent' modulo $\mathbb{Z}\mathcal{A}$.

Our proof does work with some mild hypotheses.