Galois theory in several variables: a number theory perspective

Andrew Bridy (joint with Frank Sottile)

Yale University

September 1, 2020

A classic example

Let $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$.

For generic coefficients $a_n, \ldots, a_0$, $\mathrm{Gal}(f) \simeq S_n$. This means both

1. $\mathrm{Gal}(f/\mathbb{Q}(a_n, \ldots, a_1, a_0)) \simeq S_n$, and
2. for a generic enough choice of coefficients in $\mathbb{Q}$, $\mathrm{Gal}(f/\mathbb{Q}) \simeq S_n$.

The second claim follows from the first by Hilbert's Irreducibility Theorem (but defining "generic enough" is not always easy.)

What happens in several variables?

Galois group of a polynomial system

Let K be a characteristic 0 field with algebraic closure $\overline{K}$. Let $F = (f_1, \ldots, f_n)$ where each $f_i \in K[x_1, \ldots, x_n]$, and define

$$\begin{aligned} V(F) &:= V(f_1) \cap V(f_2) \cap \cdots \cap V(f_n) \\ &= \{x \in \overline{K}^n \mid f_1(x) = \cdots = f_n(x) = 0\}. \end{aligned}$$

Assume the $V(f_i)$ intersect transversely, so that $\dim V(F) = 0$. Define the splitting field Ω of F to be

$$\Omega := K(z_1, z_2, \ldots, z_n \mid z \in V(F)),$$

that is, Ω contains all coordinates of points in $V(F)$. Define

$$\mathrm{Gal}(F) := \mathrm{Gal}(\Omega/K).$$

Exercise: Ω is a Galois extension of K, i.e., the splitting field of a single univariate polynomial.

Examples

We compute the Galois group of $F = (x^2 - 2, y^3 - 2)$ over $\mathbb{Q}$. We have

$$V(F) = (\pm\sqrt{2}, \omega^i \sqrt[3]{2})$$

for ω a 3rd root of unity and $i \in \{0, 1, 2\}$. The splitting field is

$$\Omega = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \omega)$$

and $\mathrm{Gal}(F) = \mathrm{Gal}(\Omega/\mathbb{Q}) \simeq C_2 \times S_3$. A primitive element for Ω over $\mathbb{Q}$ is given by $\sqrt{2} + \sqrt[3]{2} + \omega$, which has minimal polynomial

$$g = x^{12} + 6x^{11} + 9x^{10} - 18x^9 - 48x^8 + 6x^7 + 17x^6 + 510x^5 + 1764x^4 + 1350x^3 + 573x^2 - 642x + 223.$$

The splitting field of g is Ω, and of course, $\mathrm{Gal}(g) \simeq C_2 \times S_3$.

Examples

Consider the system $F = (x^2 - a, y^3 - b)$ over $K = \mathbb{Q}(a, b)$, with

$$V(F) = (\pm\sqrt{a}, \omega^i \sqrt[3]{b}).$$

The splitting field is $\Omega = \mathbb{Q}(\sqrt{a}, \sqrt[3]{b}, \omega)$ and $\mathrm{Gal}(F) \simeq C_2 \times S_3$ again.

Had we taken $K = \mathbb{C}(a, b)$, the group would be $C_2 \times C_3$ instead, because $\mathbb{C}$ already contains a 3rd root of unity.

Examples

Consider again the system $F = (x^2 - a, y^3 - b)$, now over $K = \mathbb{C}(a, b)$. Let X be the variety cut out by $F = 0$ inside $\mathbb{P}^2_{x,y} \times \mathbb{P}^2_{a,b}$. There is an obvious projection

$$\mathbb{P}^2_{x,y} \times \mathbb{P}^2_{a,b} \to \mathbb{P}^2_{a,b}$$

onto the second component. Let π be its restriction to X.

Geometrically, there is a finite branched cover of complex varieties

$$\pi : X \to \mathbb{P}^2_{a,b}.$$

and the monodromy group of π is $C_2 \times C_3$.

The monodromy group equals the Galois group of the function field extension $K(X)/\mathbb{C}(a, b)$ (Harris). This geometric picture can be invoked over $\mathbb{Q}$, but it produces a constant field extension (C_3 vs. S_3).

A note on specialization

For $F = (x^2 - a, y^3 - b)$, the Galois group over $\mathbb{Q}(a, b)$ is preserved if we specialize the coefficients to some $a \in \mathbb{Q}$ and $b \in \mathbb{Q}$ and take the Galois group over $\mathbb{Q}$, for "most" specializations. This is a consequence of Hilbert's Irreducibility Theorem.

If we take the Galois group over $\mathbb{C}(a, b)$, we cannot hope to specialize to $a \in \mathbb{C}$, $b \in \mathbb{C}$ and preserve the Galois group. However, we can introduce a parameter t and specialize to $a, b \in \mathbb{C}(t)$, again preserving the group under most specializations.

Galois extensions $K/\mathbb{Q}$ are analogous to Galois extensions $K/\mathbb{C}(t)$, which correspond to Galois covers of $\mathbb{P}^1(\mathbb{C})$.

Polynomial systems with given support

Any n-tuple $a = (a_1, \ldots, a_n) \in \mathbb{N}^n$ corresponds to the monomial

$$x^a = x_1^{a_1} \ldots x_n^{a_n} \in \mathbb{C}[x_1, \ldots, x_n].$$

In this way a finite set $A_1 \subseteq \mathbb{N}^n$ corresponds to a space of polynomials

$$\mathbb{C}^{A_1} = \left\{ \sum_{a \in A_1} c_a x^a : c_a \in \mathbb{C} \right\}.$$

An n-tuple of supports $A = (A_1, \ldots, A_n)$ corresponds to

$$\mathbb{C}^A = \mathbb{C}^{A_1} \oplus \cdots \oplus \mathbb{C}^{A_n},$$

which is the space of all systems $(f_1, \ldots, f_n)$ of n polynomials in n variables with support A.

Mixed volume

Let $K_1, \ldots, K_n$ be convex bodies in $\mathbb{R}^n$, equipped with Minkowski sum

$$K_1 + K_2 = \{x + y : x \in K_1 \text{ and } y \in K_2\}.$$

The *mixed volume* $V(K_1, \ldots, K_n)$ is the unique real-valued function on n-tuples of convex bodies that is

- symmetric,
- multilinear with respect to Minkowski sum, and
- normalized so that $V(K_1, K_1, \ldots, K_1) = n!\text{Vol}(K_1)$.

For $n = 2$,

$$V(K_1, K_2) = \text{Vol}(K_1 + K_2) - \text{Vol}(K_1) - \text{Vol}(K_2),$$

and this formula extends appropriately to $n \geq 3$.

The Bernstein-Kouchnirenko theorem

Let $A = (A_1, \ldots, A_n)$ and let $F = (f_1, \ldots, f_n) \in \mathbb{C}^A$.

The Bernstein-Kouchnirenko theorem predicts the generic number of solutions of the system $F(x) = 0$ in $(\mathbb{C}^*)^n$.

Theorem (Bernstein-Kouchnirenko)

There is an algebraic set $B_A \subsetneq \mathbb{C}^A$ such that, for all $F \in \mathbb{C}^A \setminus B_A$, the number of isolated solutions in $(\mathbb{C}^*)^n$ of $F(x) = 0$ equals the mixed volume of the convex hulls of the A_i.

The Bernstein-Kouchnirenko theorem

The system

$$a_0 + a_1 x + a_2 y + a_3 xy = 0$$
$$b_0 + b_1 x^2 y + b_2 x y^2 = 0$$

generically has 4 solutions in $(\mathbb{C}^*)^2$. It corresponds to the tuples

$$A_1 = \{(0,0),(0,1),(1,0),(1,1)\}$$
$$A_2 = \{(0,0),(2,1),(1,2)\}$$

Using our formula for mixed volume in dimension 2, it is easy to show that $V(N_1, N_2) = 4$, where N_i is the convex hull of A_i.

Bézout's Theorem predicts 6 solutions, 2 of which are generically at ∞.

Reduced and irreducible supports

Let $A = (A_1, \ldots, A_n)$ be a prescribed support. We say A is

- *reduced* if the A_i do not lie in a proper sublattice of $\mathbb{Z}^n$ and
- *irreducible* if no k of the A_i lie in a k-dimensional sublattice of $\mathbb{Z}^n$,

up to translating any number of the A_i.

A is non-reduced iff there is a non-invertible map $\psi : \mathbb{Z}^n \to \mathbb{Z}^n$ such that $A \subseteq \psi(\mathbb{Z}^n)$, after translation if necessary.

Galois group of a polynomial system

Let $A = (A_1, \ldots, A_n)$ be a support and let $F \in \mathbb{C}^A$.

Let V be the mixed volume of the convex hulls of the A_i.

Theorem (Esterov)

1. *If A is reduced and irreducible, then $Gal(F) \simeq S_V$.*
2. *If $Gal(F) < S_V$, then $Gal(F)$ is imprimitive.*

In Esterov's setting, $\mathrm{Gal}(F)$ is a monodromy group. We can also take it to be a Galois group as we have described, with the coefficients of the f_i as indeterminates.

The non-reduced case

Suppose A is non-reduced with corresponding polynomial system F. We may choose $\psi : \mathbb{Z}^n \to \mathbb{Z}^n$ and $B \subseteq \mathbb{Z}^n$ so that $A = \psi(B)$ for B reduced. Let G be the system with support B. There is an embedding

$$\mathrm{Gal}(F) \hookrightarrow \operatorname{coker} \psi \wr \mathrm{Gal}(G).$$

Conjecture (Esterov)

If A is irreducible, this embedding is an isomorphism.

Unfortunately, this conjecture is false in general, though true if $n = 1$.

See Esterov-Lang for a complete accounting in the case $A_1 = A_2 = \cdots = A_n$. In full generality, not much is known.

The univariate non-reduced case

Let

$$f(x) = \sum_{i \in A} a_i x^i \in \mathbb{C}(\{a_i : i \in A\})[x].$$

with $\deg f = n$. Let $d = \gcd(A)$, so f decomposes as

$$f = g \circ x^d$$

and g has no further decomposition.

Theorem (Esterov-Lang, B.-Sottile)

$Gal(f) \simeq C_d \wr S_{n/d}$

Esterov-Lang prove this as a special case of their general argument, which uses toric geometry and topology.
Bridy-Sottile's argument is purely algebraic, and should to some extent carry over to positive characteristic.

The univariate non-reduced case

Let $f = g \circ x^d$, and let $z_1, \ldots, z_k$ be the roots of g.

The roots of f break up into k blocks of size d. The ith block consists of the roots of $x^d - z_i$, and

$$\mathrm{Gal}(x^d - z_i) \simeq C_d$$

for each i. The group $C_d \wr S_k$ consists of all permutations of the kd roots of f that respect the block structure and act cyclically within each block, so it is the largest possible Galois group of f.

To show $\mathrm{Gal}(f) \simeq C_d \wr S_k$, we use specializations of f to $\mathbb{C}(t)$.

The univariate non-reduced case

Let L be the splitting field of g, so $\mathrm{Gal}(L) \simeq S_k$. Let M_i be the splitting field of $x^d = z_i$, and let M be the splitting field of f, so that

$$M = M_1 M_2 \cdots M_k.$$

The hard part of the argument is to show that the M_i are disjoint over L, in the sense that

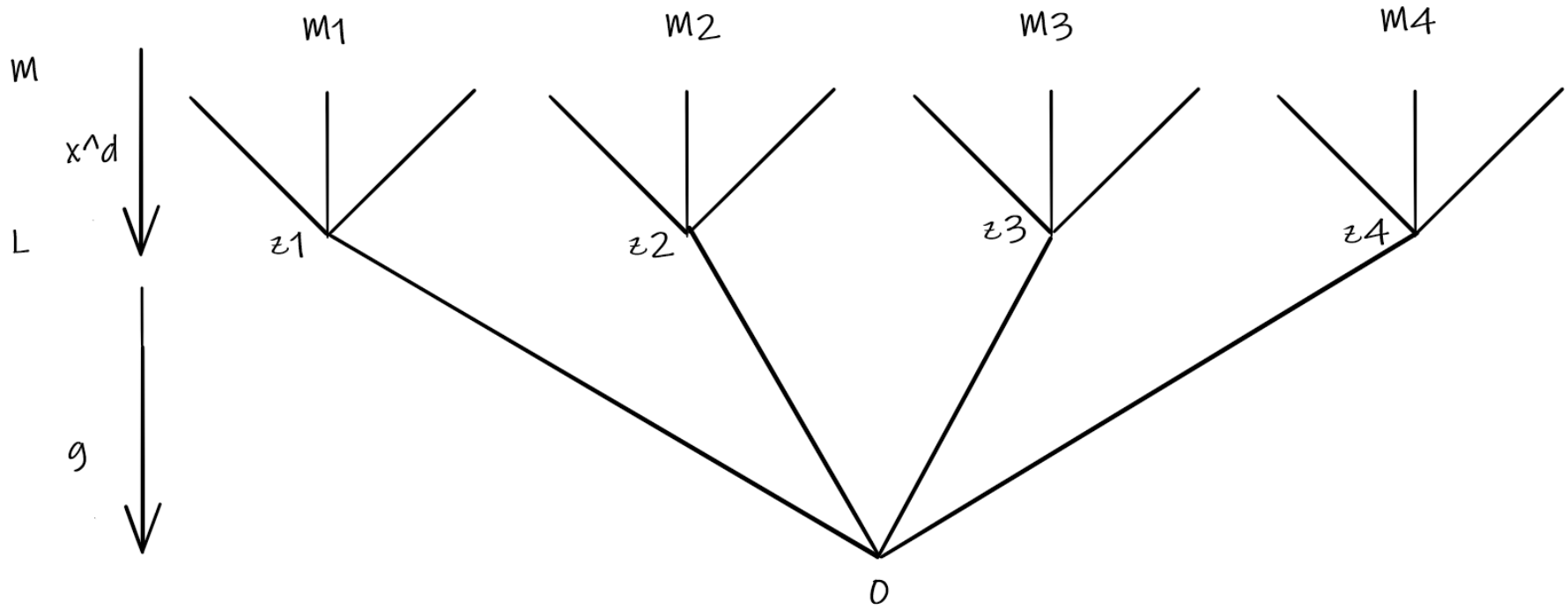
$$M_i \cap \prod_{j \neq i} M_j = L.$$

This is done by specializing to find primes $\mathfrak{p}_i$ of L that ramify in M_i and not in any other M_j. With this at hand,

$$\mathrm{Gal}(M/L) \simeq \prod_{i=1}^{k} \mathrm{Gal}(M_i/L) \simeq C_d \times \ldots C_d,$$

which finishes the argument.

The univariate non-reduced case



This is the diagram of fields for $d = 3$ and $\deg g = 4$. The generic Galois group $C_3 \wr S_4$ acts by automorphisms on this tree.

Further questions

- How much carries over to positive characteristic?
- Can we prove probabilistic statements for Galois groups of random polynomial systems over $\mathbb{Q}$?
- How does $\mathrm{Gal}(F)$ relate to splitting and ramification of primes in several variables? Is there a Dedekind-Kummer theorem or a Chebotarev density theorem about factorizations mod p?
- What is the correct formulation of the inverse Galois problem for systems of complex polynomials with generic coefficients?
- Is the multivariate approach useful for attacking univariate Galois problems by adding more variables?

Galois theory in several variables: a number theory perspective

Andrew Bridy (joint with Frank Sottile)

Yale University

September 1, 2020