The inverse problem for arboreal Galois representations of index two

Andrea Ferraguti

Joint Mathematics Meeting 2020

18/1/2020

Quadratic arboreal Galois representations

Let K be a field of characteristic not 2, and let $f \in K[x]$ be a monic, quadratic polynomial with $f^{(n)}$ separable for every $n \geq 1$. We set $f^{(0)} := x$ by convention.

The set $T(f) \subseteq K^{\text{sep}}$ of the roots of all the $f^{(n)}$'s has a natural structure of infinite, regular, rooted binary tree.

The absolute Galois group $G_K := \operatorname{Gal}(K^{\text{sep}}/K)$ acts on $T(f)$ via its natural Galois action, yielding a continuous map of profinite groups $\rho_f \colon G_K \to \operatorname{Aut}(T(f))$.

Definition

Such map is called the arboreal Galois representation attached to f.

Open Problem

How does one compute $\operatorname{Im}(\rho_f)$? Or at least, how does one understand whether $[\operatorname{Aut}(T(f)) : \operatorname{Im}(\rho_f)] < \infty$ or not?

Surjective representations

Let $f = (x-a)^2 - b \in K[x]$. The adjusted post-critical orbit of f is the sequence defined by: $c_1 := -f(a), \quad c_n := f^{(n)}(a), n \geq 2$.

Throughout the talk, I will always assume that every $f^{(n)}$ is separable, i.e. that $c_n \neq 0$ for every n.

Let $\langle c_1, \ldots, c_n \rangle$ be the $\mathbb{F}_2$-vector space generated by $c_1, \ldots, c_n$ inside $K^\times / K^{\times 2}$.

Theorem (Stoll, 1992)

The arboreal representation $\rho_f \colon G_K \to \mathrm{Aut}(T(f))$ *is surjective if and only if* $\dim\langle c_1, \ldots, c_n \rangle = n$ *for every* n.
This holds, for example, for $x^2 + a \in \mathbb{Q}[x]$ *if* $a \equiv 1 \bmod 4$.

Theorem (F., Micheli, 2019)

Let k *be a field of characteristic not 2 and* t *be transcendental over* k. *Then the polynomial* $f = x^2 + t \in k(t)[x]$ *has surjective representation.*

Which representations have maximal image?

Stoll's theorem implies that linear relations (modulo squares) among the elements of the adjusted post-critical orbit decrease the size of the image of the representation.

Question

What type of linear relations in the post-critical orbit ensure that $\mathrm{Im}(\rho_f)$ is a maximal subgroup of $\Omega_\infty := \mathrm{Aut}(T(f))$?

Notice that Ω_∞ is a pro-2-group. Hence, its maximal subgroups are exactly those of index two, i.e. they are kernels of maps $\Omega_\infty \to \mathbb{F}_2$.

Understanding maximal subgroups of Ω_∞

Since $\Omega_\infty = \varprojlim_{n\geq 1} \underbrace{\mathbb{F}_2 \wr \ldots \wr \mathbb{F}_2}_{n \text{ times}}$, every $\sigma \in \Omega_\infty$ has an expression of the form $(\sigma_1, \ldots, \sigma_n, \ldots)$ where $\sigma_n \in \mathbb{F}_2^{2^{n-1}}$.

For every $n \geq 1$ there is a homomorphism $\phi_n \colon \Omega_\infty \to \mathbb{F}_2$ that sends σ to the sum of the coordinates of σ_n.

We let $\widehat{\phi} \coloneqq \prod_n \phi_n \colon \Omega_\infty \to \prod_{n\geq 1} \mathbb{F}_2$. One can check that $\ker \widehat{\phi} = [\Omega_\infty, \Omega_\infty]$. Hence, the dual group $\Omega_\infty^\vee \coloneqq \hom(\Omega_\infty, \mathbb{Q}_2/\mathbb{Z}_2)$ is spanned by all the ϕ_n's.

Proposition

There exists a bijection

$$\bigoplus_{n\geq 1} \mathbb{F}_2 \setminus \{\underline{0}\} \xrightarrow{\sim} \{\textit{maximal subgroups of } \Omega_\infty\}$$

$$\underline{a} = (a_n)_{n\geq 1} \mapsto M_{\underline{a}}$$

where $M_{\underline{a}} = \ker \sum_{n\geq 1} a_n \phi_n$.

Understanding maximal subgroups of Ω_∞

Let K be a field of characteristic not 2 and $f \in K[x]$ be monic, quadratic with adjusted post-critical orbit $\{c_n\}_{n\geq 1}$ and arboreal representation ρ_f.

Lemma

Let $\underline{a} = (a_n)_{n\geq 1} \in \bigoplus_{n\geq 1} \mathbb{F}_2$. *Then* $\mathrm{Im}(\rho_f) \subseteq M_{\underline{a}} \iff \prod_{n\geq 1} c_n^{a_n} \in K^2$.

Stoll's theorem follows immediately!

Corollary

If f is post-critically finite or $K^\times/K^{\times 2}$ is finite dimensional, then $[\Omega_\infty : \mathrm{Im}(\rho_f)] = \infty$.

Representations with (transitive) maximal image

Theorem (F., Pagano, Casazza)

Let $\underline{a}=(a_n)_{n\geq 1}\in\bigoplus_{n\geq 1}\mathbb{F}_2$ *be such that* $\underline{a}\neq\underline{0},(1,0,\ldots,0,\ldots)$. *Let* $f\in K[x]$ *be irreducible.*
Then $\mathrm{Im}(\rho_f)=M_{\underline{a}}$ *if and only if*

$$\prod_{i\geq 1}c_i^{a_i}\in(K^\times)^2,\quad \prod_{i\geq 1}c_i^{b_i}\notin K^2 \text{ for every } \underline{b}=(b_n)_{n\geq 1}\in\bigoplus_{i\geq 1}\mathbb{F}_2 \text{ with } \underline{b}\neq\underline{0},\underline{a}$$

and one of the following two conditions is satisfied:

a) $a_1=1$;

b) $a_1=0$ *and* $h\left(c_1,\ldots,c_{n-1},\sqrt{\prod_{i\geq 1}c_i^{a_i}}\right)$ *is linearly independent from* $\{c_1,\ldots,c_{n-1},c_{n+1},c_{n+2},\ldots\}$ *in* $K^\times/K^{\times 2}$, *where* $h(X_1,\ldots,X_{n-1},Y)\in\mathbb{Z}[X_1,\ldots,X_{n-1},Y]$ *depends only on* $\underline{a}$, *and* n *is the largest index with* $a_n=1$.

If one of these conditions is sastisfied, then f *is stable, i.e.* $f^{(n)}$ *is irreducible for every* n.

A sketch of the proof

The idea is study, for a non-zero $\underline{a} = (a_n)_{n\geq 1} \in \bigoplus_{n\geq 1} \mathbb{F}_2$, the maximal subgroups of $M_{\underline{a}}$.

The most delicate step of the proof is to show that if $\varphi\colon M_{\underline{a}}^{\mathrm{ab}} \to \Omega_\infty^{\mathrm{ab}}$ is the natural map, then $|\ker \phi| = 2$.

This is done by first noticing that $\ker \varphi = [\Omega_\infty, \Omega_\infty]/[M_{\underline{a}}, M_{\underline{a}}]$, and then proving that elements of $\ker \varphi$ can be represented as elements in $I_{\Omega_\infty}\mathbb{F}_2^{2^{n-1}}/I_{\Omega_\infty}^2\mathbb{F}_2^{2^{n-1}}$, for n the largest integer such that $a_n = 1$.

One then uses this fact to prove the following:

- If $a_1 = 1$, then the maximal subgroups of $M_{\underline{a}}$ all arise as intersections of the maximal subgroups of Ω_∞ with $M_{\underline{a}}$.
- If $a_0 = 0$, then there is an additional character $M_{\underline{a}} \to \mathbb{F}_2$ which maps $\sigma = (\sigma_n)_{n\geq 1}$ to $\sum_{n\geq 2} a_n \widetilde{\phi}_n(\sigma)$, where $\widetilde{\phi}_n(\sigma)$ is the sum of the first half of the coordinates of σ_n.

Finally, one computes the function $h(X_1, \ldots, X_{n-1}, Y) \in \mathbb{Z}[X_1, \ldots, X_{n-1}, Y]$ in terms of $\underline{a}$.

Representations with (non-transitive) maximal image

Theorem (F., Pagano, Casazza)

We have that $\mathrm{Im}(\rho_f) = M_{(1,0,\ldots,0,\ldots)}$ *if and only if* $f = (x-a)^2 - u^2$ *for some* $a, u \in K$ *and*

$$\{c_1 \pm u, c_2 \pm u, \ldots, c_n \pm u, \ldots\} \text{ is linearly independent in } K^\times/(K^\times)^2.$$

If these conditions hold, then $f = g_1 g_2$ *in* $K[x]$*, where* g_1, g_2 *are* f*-stable linear polynomials, i.e.* $g_i \circ f^{(n)}$ *is irreducible for every* $i \in \{1,2\}$ *and every* $n \geq 1$*.*

Examples over the rationals

Let $f := x^2 + t \in \mathbb{Q}(t)[x]$. Then $\mathrm{Im}(\rho_f) = \Omega_\infty$. Are there any specializations of f whose representations have maximal image?

Proposition

There are exactly 5 maximal subgroups of Ω_∞ that can appear as $\mathrm{Im}(\rho_{f_{t_0}})$ for infinitely many $t_0 \in \mathbb{Q}$. These correspond to the vectors:

$$v_1 = (1,1,0,\ldots,0,\ldots), \quad v_2 = (0,1,0,\ldots,0,\ldots), \quad v_3 = (1,0,1,0,\ldots,0,\ldots),$$

$$v_4 = (0,1,1,0,\ldots,0\ldots), \quad v_5 = (1,0,\ldots,0,\ldots).$$

Theorem (F., Pagano, Casazza)

Let $u \in 2\mathbb{Z} \setminus \{0\}$. The the following hold:

1. *if $t_0 = -1 - u^2$, then $\mathrm{Im}(\rho_{f_{t_0}}) = M_{v_1}$;*
2. *if $t_0 = \frac{1}{u^2-1}$, then $\mathrm{Im}(\rho_{f_{t_0}}) = M_{v_2}$.*

Examples over the rationals

Conjecture (Vojta)

Let $d \in \mathbb{Z}_{\geq 5}$ and $g \in \mathbb{Q}[x]$ a polynomial of degree d with non-zero discriminant. Then there exist constants $C_1(d), C_2(d)$ such that if $x_0, y_0 \in \mathbb{Q}$ satisfy $y_0^2 = f(x_0)$, then:

$$h(x_0) \leq C_1 \cdot h(f) + C_2.$$

Theorem (F., Pagano, Casazza)

Assume Vojta's conjecture, and let $i \in \{3, 4, 5\}$. Then there exists an infinite, thin set $E_i \subseteq \mathbb{Q}$ such that for all but finitely many $t_0 \in E_i$ we have $\operatorname{Im}(\rho_{f_{t_0}}) = M_{v_i}$.

Remark

If $g_1 = x^2 - 1 - t^2$, $g_2 = x^2 + \frac{1}{t^2-1}$ and $g_5 = x^2 - t^2$ are seen as polynomials with coefficients in $\mathbb{Q}(t)$, then $\operatorname{Im}(\rho_{g_i}) = M_{v_i}$.
On the other hand, there are no polynomials $\psi = x^2 + h(t) \in \mathbb{Q}(t)$ with $\operatorname{Im}(\rho_\psi) \in \{M_{v_3}, M_{v_4}\}$.

A reconstruction theorem

Finally, one can ask if any two maximal subgroups $M_{\underline{a}}$ and $M_{\underline{b}}$ are isomorphic whenever $\underline{a} \neq \underline{b}$.

Theorem (F., Pagano, Casazza)

If $\underline{a}, \underline{b} \in \bigoplus_{n \geq 1} \mathbb{F}_2$ are distinct vectors (possibly null), then $M_{\underline{a}}$ and $M_{\underline{b}}$ are non-isomorphic as topological groups.

The proof makes use of the following object.

Definition

Let G be a topological group and S a set of topological generators. The graph of commutativity of (G, S) has the elements of S as nodes, and two nodes g, h are connected if and only if $gh \neq hg$.

The proof method

The proof is quite involved. First, we studied in deep the descending central series of each $M_{\underline{a}}$, i.e. the sequence defined by

$$M_{\underline{a}}^{(0)} := M_{\underline{a}}, \quad M_{\underline{a}}^{(n)} := [M_{\underline{a}}, M_{\underline{a}}^{(n-1)}]$$

These subgroups are defined in terms of certain maximal subgroups of $\Omega_\infty^{(n)}$, for a suitable n.

Next, one defines the following invariant of a graph Γ with at least two vertices:

$$d_\Gamma := \min_{g\in\Gamma} \max_{g'\in\Gamma\setminus\{g\}} \mathrm{dist}_\Gamma(g,g').$$

The final step is to show that if $\underline{a} \neq \underline{b}$, then there exist $n \geq 0$ and sets of topological generators S, S' for $M_{\underline{a}}^{(n)}, M_{\underline{b}}^{(n)}$ such that if Γ, Γ' are the graphs of commutativity of $(M_{\underline{a}}^{(n)}, S), (M_{\underline{b}}^{(n)}, S')$ then $d_\Gamma \neq d_{\Gamma'}$.

Thank you for your attention!