The Galois theory of orbits in arithmetic dynamics

organized by
Rafe Jones, Michelle Manes, and Joseph Silverman

Workshop Summary

1. Workshop goals

This workshop, held May 16–20, 2016, was devoted to the study of Galois properties of points in orbits of algebraic maps. The main topics for the workshop were:

- *Arboreal Galois Groups* of fields generated by points in backward orbits of finite algebraic maps.
- *Dynatomic Galois Groups* of fields generated by periodic points of finite algebraic maps.

Arboreal Galois groups sit naturally as subgroups of tree (or graph) automorphism groups, while dynatomic Galois groups are naturally subgroups of certain wreath products. A fundamental problem is to determine general conditions under which these dynamically generated Galois groups have finite index in the natural geometric groups that contain them. This is a dynamical analog of Serre's theorem on the size of the Galois groups generated by torsion points on elliptic curves. The goal of the workshop was to better understand these Galois groups over number fields and over function field in both the one-dimensional and higher dimensional settings. For the latter, an initial goal is to give a geometric characterization of those maps for which one does not expect a finite index theorem to hold, analogous to the case of CM elliptic curves.

Website: http://aimath.org/pastworkshops/galarithdyn.html.

2. Workshop talks

There were a total of nine talks over the five days of the workshop.

- Rafe Jones: The image of arboreal Galois representations
- Nigel Boston: Images of Frobenius unramified at $\mathfrak{p}$
- Joseph Silverman: Dynatomic polynomials, dynatomic representations, and dynatomic moduli spaces
- Mike Zieve: Statistics for dynamics over finite fields
- Rachel Pries: Degenerations of maps
- Wei Ho: Arithmetic statistics
- Bjorn Poonen: Bertini theorems over finite fields
- Tom Tucker: Surjectivity for arboreal representations under various conjectures
- Rob Benedetto: Components in nonarchimedean dynamics

3. Workshop problem list

The workshop generated many new problems in the field. The full workshop problem list is at http://aimpl.org/galarithdyn/.

4. Working group summaries

A total of eight working groups were formed over the five day workshop, with two disbanding relatively quickly when they realized that progress on their problems was unlikely. (Members of those groups joined other working groups for the rest of the week.) We provide summaries of the progress made by each of the other six working groups during the workshop.

4.1. Conjugacy invariants The group focused on Question 2.1 (http://aimpl.org/galarithdyn/2/): The group started by studying whether Pink's generating function Φ_w is a rational function for every $w = \rho(Frob_p)$. It then shifted to studying the following problem. Let $\phi(z) \in \mathbb{F}_p[z]$ be a polynomial of degree at least 2 defined over a finite field. For each $n \geq 1$, factor $\phi^n(z)$ as $\phi^n(z) = f_{n,1}(z)f_{n,2}(z)\cdots f_{n,k_n}(z)$ with polynomials ordered to satisfy $\deg f_{n,i} \leq \deg f_{n,i+1}$. Define the degree sequence $D_n = (\deg f_{n,1}, \deg f_{n,2}, \ldots, \deg f_{n,k_n})$. The factorization of ϕ^{n+1} is composed of the factors of the various $f_{n,i}\big(\phi(z)\big)$, so viewing the elements of D_n as vertices, we can connect the $f_{n,i}$-vertex in D_n to the vertices in D_{n+1} coming from the factorization of $f_{n,i}\big(\phi(z)\big)$. The group concentrated especially on quadratic polynomials, so each D_n vertex connects to either one or two vertices in D_{n+1}. Depending on properties of ϕ and p, one can color the vertices of D_n so that the splitting is modeled by a Markov process. The group spent a lot of time studying a particular example in which the vertices had four possible colors. Fairly extensive computer simulations indicated that the abstract Markov process explains to some order of approximation the actual tree coming from iteration of ϕ, but there appears to be more going on than just the Markov process. This suggests that the distribution of D_{n+1} depends on more than the distribution of the colored vertices in the previous level D_n. Work in studying this and other examples is ongoing, as is a computation of the exact limit distribution predicted by the (rather complicated) Markov process.

4.2. Dynatomic modular curves The group focused on Question 4.2 (http://aimpl.org/galarithdyn/4/): What are the primes of bad reduction for the dynatomic modular curve $X_1^{\text{dyn}}(N)$, and why?

The dynatomic modular curve is defined as the smooth completion of the vanishing of the N^{th} dynatomic polynomial $\Phi_n(x,c)$. We have a natural map to $\mathbb{P}^1$ from this curve:

$$X_1^{\text{dyn}}(N) \to \mathbb{P}^1, \qquad (x,c) \mapsto c.$$

From Morton, we know that if $X_1^{\text{dyn}}(N)$ has bad reduction at p, then two branch points collide modulo p. The working group has a simpler proof of this statement than the one in Morton's paper.

The group's primary goal was to understand the branching behavior of this map. In particular, they looked at Morton's polynomials $\delta_n(c)$ whose roots are branch points of the map $X_1^{\text{dyn}}(N) \to \mathbb{P}^1$. Their goal was to combine data about the cycle structure of monodromy around these branch points. That means they have to understand both:

- Branching over $\mathbb{C}$. The group made significant headway in this direction, using a combinatorial description of which cycles collide via known results about external rays and the Mandelbrot set.

- How close branch points are p-adically, and what happens when they collide modulo p. This is future work.

4.3. Critical point relations The group focused on Question 6.1 (http://aimpl.org/galarithdyn/6/): Which sorts of critical orbit relations force infinite index for the image of Galois in the arboreal case?

In degree 2, we have two critical orbit relations that force the image of Galois to have infinite index: When the map is PCF (in fact this holds in every degree), and when the map has a *Pink obstruction*, which is defined when the critical points γ_1 and γ_2 satisfy $\phi^n(\gamma_1) = \phi^n(\gamma_2)$ for some $n \geq 1$.

The group made significant progress on many fronts:

- In the geometric case, $G_\infty = Gal(\phi^\infty(x) - t/\mathbb{C}(t))$, the index of G_∞ in $Aut(T_\infty)$ is either one or infinite. We know that in the arithmetic case (where we specialize to $t = 0$, for example) it is possible to have finite index without having surjectivity. This result says that such non-full finite index happens only due to "arithmetic accidents" involving the choice of base point.
- Let γ_1, γ_2 be the critical points of a cubic polynomial ϕ. If $\phi^n(\gamma_1) = \phi^n(\gamma_2)$ for some $n > 0$, then the image of Galois has infinite index.
- If all of critical points of ϕ have odd ramification index, then the image of Galois has infinite index.

Most importantly, the group extended a key lemma of Pink's from degree 2 rational functions to arbitrary degree polynomials, and they are on track to extend the result to rational maps:

Let K be a field of characteristic not equal to 2, and $\phi \in K(z)$. Then Galois group of $\phi^n(z) - t$ over $K(t)$ is generated by inertia elements for each post-crticial point of ϕ, and moreover the action of these inertial elements on $Aut(T_\infty)$ can be described recursively.

The lemma is used to project the Galois group G_∞ into $Aut(T_\infty)^{\mathrm{ab}} = (\mathbb{Z}/2\mathbb{Z})^N$. If the index is infinite in the abelianization, then it is infinite in the whole group. The group also found an example which they believe should have infinite index, but for which their current techniques do not work. It is a quartic polynomial with three finite critical points satisfying $\phi^2(\gamma_1) = \phi^2(\gamma_2) = \phi^2(\gamma_3)$.

For future work, the group conjectures a stronger rigidity property than the "index one or infinity" result mentioned above: either the arboreal representation is surjective, or the Hausdorff dimension of G_∞ is strictly between 0 and 1. They hope to explicitly calculate this dimension.

4.4. Find more arboreal Galois representations, Group A The group focused on Question 10.1 (http://aimpl.org/galarithdyn/10/): Find examples of polynomials or rational maps $d \geq 3$ for which we can compute explicitly the arboreal Galois representation up to finite index over various fields. This group also wanted to find new techniques to compute the image of Galois, avoiding using ramification. However, they gave up on that secondary goal and focused on the first one.

Their example was the cubic polynomial $\phi(z) = -2z^3 + 3z^2$. This is a PCF function; in fact it is a conservative polynomial (one where all critical points are fixed). It is a conjugate of the Newton map $z^3 - z$. The group looked at the preimage tree over 3 (computing the arithmetic Galois representation) and over the transcendental t (computing the geometric Galois representation).

Letting $G_n = Gal(\phi^n(z) - t/\bar{Q}(t))$, the group showed that $G_1 \cong S_3$ and that

$$G_n \subseteq (G_{n-1} \wr S_3) \cap \ker(\text{Even}_2),$$

where Even_2 is the map $sgn : S_9 \to \{\pm 1\}$. They conjecture that this is an equality, which they verified for $t = 3$ and $n \leq 4$. From this, they can conclude that

$$\text{Hausdorff dimension}(G_\infty) \leq 1 - \frac{1}{3}\left(\frac{\log 2}{\log 6}\right) \approx 0.871.$$

They have conjectural generators for G_n, which will be provably generators using the Critical Orbits group's extension of Pink's lemma.

For future work, they plan to look at families of conservative rational functions of the form

$$\phi(z) = \frac{(d-2)z^d + dz}{dz^{d-1} + d - 2}.$$

4.5. Find more arboreal Galois representations, Group B The group also focused on Question 10.1 (http://aimpl.org/galarithdyn/10/). Their focus was on polynomial functions of the form $x^p + c$ for $p > 3$ prime. In particular, let ζ_p be a primitive p^{th} root of unity, and define

$$\phi_p(z) = z^p + 1 - \zeta_p.$$

The group proved the following theorem. Let G_∞ be the Galois group associated to the arboreal representation of ϕ_p over the base point ζ_p. Then $G_\infty \leq [C_p]^\infty$ has finite index in $Aut(T_\infty)$.

Their proof relies on their ability to show that a conjugated version of these maps has every iterate Eisenstein, and that they have primitive prime divisors for the forward orbit of the unique finite critical point.

For $p = 3$, they are able to show surjectivity of the Galois representation. This provides the first known example of a function of degree $d \geq 3$ with surjective arboreal representation in its natural geometric overgroup. (A longstanding conjecture of Odoni's posits that there exists in every degree a function whose arboreal representation is the full automorphism group of the tree. This result is roughly in that direction, though here the geometric overgroup is an iterated wreath product of cyclic groups rather than the full automorphism group of the tree.) The group is working on extending the surjectivity result for primes $p \geq 4$.

4.6. Wild ramification This group focused on Question 12.1 (http://aimpl.org/galarithdyn/12/): Study Galois representations over local fields of residue characteristic p dividing the degree of ϕ (or with $p < \deg \phi$). In particular, they studied the function $\phi(x) = x^2 - c$ for $c \in K$ with K a finite extension of Q_2. Their goal was to understand the image of G_∞ in $Aut(T_\infty)$.

Their finding: The image of Galois always has infinite index in the automorphism group of the tree, and the Hausdorff dimension of the image depends on the 2-adic valuation $v_2(c)$. They were able to prove:

- If $v_2(c) < -4$, then $K_\infty = K_1$, so $G_\infty \subseteq \mathbb{Z}/2\mathbb{Z}$.
- If $v_2(c) = -4$, then $G_\infty \subseteq (\mathbb{Z}/2\mathbb{Z})^2$, but the inertia subgroup satisfies $I \subseteq \mathbb{Z}/2\mathbb{Z}$.
- Let $v_n = -2^{n+1}/(2^n - 1)$. If $v_2(c) < v_n$, then $K_\infty = K_n$.

- If $v_n < v_2(c) < v_{n+1}$, then $K_\infty = K(\alpha)$ for any choice of $\alpha \in \phi^{-n}(0)$. In this case, $G_\infty = I \subseteq (\mathbb{Z}/2\mathbb{Z})^{n+1}$.
- At $v_2(c) = -2$, there is infinite ramification. In fact, the inertia subgroup satisfies $I = (\mathbb{Z}/2\mathbb{Z})^\infty$ and $G_\infty/I = \mathbb{Z}_2$.
- For $v_2(c) > -2$, there is infinite wild ramification. It is no longer true that $K_\infty = K(\alpha)$ for a single $\alpha \in \bar{K}$.