The Galois theory of orbits in arithmetic dynamics

The American Institute of Mathematics

The following compilation of participant contributions is only intended as a lead-in to the AIM workshop "The Galois theory of orbits in arithmetic dynamics." This material is not for public distribution.

Corrections and new material are welcomed and can be sent to `workshops@aimath.org`

Version: Fri May 13 13:18:30 2016

Table of Contents

Chapter A: Participant Contributions

A.1 Benedetto, Rob

I'd like to understand better arboreal representations over finite fields, thinking in terms of local contributions at primes of good reduction over number fields and function fields. In particular, I'd like to get a better understanding of the good reduction case before turning to the bad reduction case, to properly frame questions about Galois actions on p-adic dynamical systems of bad reduction.

A.2 Boston, Nigel

I am interested in the arboreal Galois representations associated to Galois actions on iterates of polynomials, in particular quadratics. I am most curious about the images of Frobenius elements at unramified primes. I am also curious about how this all interacts with the Markov processes introduced by Rafe Jones and me and refined by Vefa Goksel, Shixiang Xia, and me.

A.3 Faber, Xander

The work of Odoni, Stoll, Jones, and others has connected the Galois groups of iterated pre-images of a point x_0 under a polynomial $f \in [z]$ on one hand, with the density of prime divisors appearing in the f-orbit of x_0 on the other. Much of this work only applies to polynomials that are not postcritically finite. I am interested in finding extensions of these ideas to the postcritically finite setting because of the application to the density of primes p for which Newton's method succeeds p-adically. For references on the latter topic, see the following articles:

R. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon, and T. Tucker. "Periods of rational maps modulo primes." Mathematische Annalen. 355 (2013), 637–660.

X. Faber and A. Towsley. "Newton's method over global height fields." Journal de Theorie des Nombres de Bordeaux. 26 (2014), 347–362.

X. Faber and J.F. Voloch "On the number of places of convergence of Newton's method over number fields." Journal de Theorie des Nombres de Bordeaux. 23 (2011), 387–401.

A.4 Hamblen, Spencer

In general, I'm interested in the structure of the Galois groups of fields obtained from adjoining preimages, and am currently working on questions of wild ramification (and deep ramification) in these fields.

I have also previously worked with deformation rings of Galois representations, and I would be interested in finding applications for this work in arithmetic dynamics.

A.5 Hindes, Wade

In what follows, K is a global field and $\phi \in K(x)$. For $n \geq 1$, we let $K_n(\phi)$ be the field obtained by adjoining all solutions of $\phi^n(x) = 0$ to K. With some mild separability assumptions, $K_n(\phi)/K$ is Galois and $K_{n-1}(\phi) \subseteq K_n(\phi)$. Hence, we may define the inverse limit

$$G_K(\phi) = \varprojlim \mathrm{Gal}(K_n(\phi)/K) \tag{1}$$

with respect to the restriction maps. It is known that $G_K(\phi)$ is naturally a subgroup of $\mathrm{Aut}(T)$, the automorphism group of a $\deg(\phi)$-ary rooted tree; see [RJSurvey]. Below is a list of possible problems to address about $G_K(\phi)$:

A. Stoll/Odoni problem: Let $c \in \mathbb{Q}$ and let $\phi_c(x) = x^2 + c$. Prove that $G_K(\phi_c) \cong \mathrm{Aut}(T)$ outside of a thin (or density zero) subset of c's.
B. Let $\phi(x) = x^3 + ax + b$ be a cubic polynomial. Find an arithmetic condition on the critical orbits of ϕ ensuring that the subextensions $K_n(\phi)/K_{n-1}(\phi)$ are maximal; compare to the results in [**?**, Theorem 25] and [**?**, Lemma 1.6].
C. What type of subgroups $G_K(\phi) \leq \mathrm{Aut}(T)$ arise from PCF maps? This problem is partially understood for quadratic polynomials, though the family $\phi(x) = (x-c)^2 + c - 1$ for rational values of c remains elusive [**?**, §4]: the case $\phi(x) = (x+1)^2 - 2$ (corresponding to $c = -1$) is particularly interesting, as it generates extensions unramified at all odd primes. As for higher degree examples, consider $\phi(x) = x^3 - \frac{3}{4}x - \frac{3}{4}$.
D. Let $K/k(t)$ be a function field. Show that for every $\phi \in K(x)\ k(x)$, the superelliptic curve $C_{\ell,m}(\phi) : Y^\ell = \phi^m(x)$ is non-isotrivial for some pair $\ell \geq 2$ and $m \geq 1$ (perhaps using the residue formula in [**?**, §5]); for how this property relates to Galois theory, see [Me].

Bibliography

[Boston-Jones] N. Boston and Rafe Jones. The image of an arboreal Galois representation, *Pure and Applied Mathematics Quarterly* 5.1 (Special Issue: in honor of Jean-Pierre Serre, Part 2 of 2) (2009): 213-225.

[xdc] S. Hamblen, R. Jones, and K. Madhu. The density of primes in orbits of $z^d + c$, *Int. Math. Res. Not.* 7 (2015): 1924-1958.

[Me] W. Hindes. Average Zsigmondy set, dynamical Galois Groups, and the Kodaira-Spencer Map, preprint arXiv:1603.04459

[RJSurvey] R. Jones, Galois representations from pre-image trees: an arboreal survey, *Pub. Math. Besançon* (2013): 107-136.

[Voloch] M. Kim, D. Thakur, and J. Voloch. Diophantine approximation and deformation, *Bulletin de la Société Mathématique de France* 128.4 (2000): 585-598.

[Stoll-Galois] M. Stoll. Galois groups over $\mathbb{Q}$ of some iterated polynomials, *Arch. Math.* 59 (1992): 239-244.

A.6 Hutz, Benjamin

I interested in number theoretical and computational aspects of dynamical systems. I am particularly interested in higher dimensional cases. My main focus at this workshop is to learn more about the techniques used to study the Galois theory of orbits and catch-up on what is currently known. During the workshop I am especially interested in working on the higher dimensional case where 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.

A.7 Jones, Rafe

I am interested in several topics associated with the arboreal representation attached to a rational function and a point, that is, the Galois action on iterated preimages of the point under the function.

1) I would like to see a plausible conjecture put forward of the classes of cubic (or higher degree) rational functions for which one does not expect the arboreal representation to have finite index in the automorphism group of the tree of preimages. I would also like to see some classes of higher-degree maps for which one expects an analogous finite-index statement to fail.

2) I am interested in results giving a readily-verifiable criterion for a cubic polynomial (or higher degree) with integer coefficients to have a finite-index arboreal representation, assuming if necessary that all iterates are irreducible.

3) I am interested in questions revolving around the computation of arithmetic iterated monodromy groups, especially for PCF maps. In particular, the constant field sub-extensions of the associated extensions are very poorly understood, even for the simplest examples.

4) I am interested in exploring a question posed by Umberto Zannier, which one could call "unlikely arboreal intersections": given rational functions f and g over a number field K and a,b in K, let K(f,a) (resp. K(g,b)) denote the field obtained by adjoining all iterated preimages of a under f (resp. b under g). Suppose that the intersection of K(f,a) and K(g,b) is an infinite extension of K. What can one say about the relationship of f and g? In particular, if K(f,a) = K(g,b), must f and g have a common iterate?

I am also interested in the dynatomic Galois problem. Morton has given some sufficient conditions for these Galois groups to be as large as possible, but the conditions fail to hold in many cases. It would be very interesting to have additional sufficient conditions. It would also be interesting to find special classes of rational functions for which these groups can never be as large as possible.

A.8 Krumm, David

I am interested in studying basic properties of some curves corresponding to dynatomic polynomials. Let $\Phi_n(c,x) \in \mathbb{Q}[c,x]$ be the n-th dynatomic polynomial of the quadratic polynomial x^2+c. Viewing $\Phi_n(c,x)$ as a polynomial in the variable x with coefficients in the function field $\mathbb{Q}(c)$, let N be a splitting field for Φ_n and let G be the Galois group of the extension $N/\mathbb{Q}(c)$. Let X be the curve with function field N. For every subgroup H of G we may consider the curve X/H. I would like to address the following problems:

A. Give an explicit description of all maximal subgroups of G.
B. For every maximal subgroup M of G, compute the genus of the curve X/M.
C. With M as above, find an efficient procedure to determine an affine plane model of the curve X/M.

A solution to these problems would afford a better understanding of how the Galois group of the polynomial $\Phi_n(c,x)$ changes as c varies over all rational numbers.

A.9 Looper, Nicole

One of my main interests is to work on finite index theorems for arboreal representations attached to polynomials over number fields. Especially in cases where much work has been done (e.g., stable non-PCF quadratics) it would be nice to establish what the best possible

statements are of what is known using techniques that we are aware of. Beyond that, I would also like to work on developing alternate approaches to these problems–ones outside of the route using Stoll's lemma and height bounds of integral points on curves. The scarcity of known methods seems to be the main limitation in moving forward, which is why I think it is important to try to diversify in this regard.

I would also be interested in working on Odoni's conjecture, namely, that for every $d \geq 2$, there exists a monic polynomial in $\mathbf{Z}[x]$ of degree d whose arboreal Galois representation has index 1.

A.10 Nguyen, Khoa

Let K be a number field and let $f(x) \in K(x)$ be a rational function of degree at least 2. I am interested in studying the field K_f obtained by adjoining all preperiodic points of f into K. For instance, if f is a polynomial that is not conjugate to the power map or $\pm$Chebyshev, can we prove that K_f is "significantly different" from the cyclotomic extension of K? More generally, if f and g have "distinct dynamical behaviors", can we say that K_f and K_g are "very different". During the workshop, I will be clearer about this.

A.11 Obus, Andrew

My main field of expertise is branched covers of curves in positive and mixed characteristic, particularly involving wild ramification. I have not written any papers on dynamics, but I find the subject of arboreal Galois representations very interesting. I would be especially interested in low-characteristic analogs of results currently requiring characteristic zero or large characteristic, such as Theorem 3.1 in Jones's "arboreal survey."

A.12 Pries, Rachel

My main research topics are about moduli spaces of curves and abelian varieties and Galois theory of curves. I am especially curious about the interplay between automorphisms of curves and arithmetic structures on their Jacobians. Most of my work is about curves in positive characteristic but more recently I have been working on projects about rational points on curves over function fields and number fields. I am looking forward to learning more about arithmetic dynamics and collaborating on open research problems with the group.

A.13 Rubinstein-Salzedo, Simon

There are several invariants of arithmetical interest associated to a number field, such as the Galois group, the set of ramified primes, the class number, and so on. I am interested in understanding when there exists a number field that has several simultaneous invariants. For example, is there a number field with Galois group A_{10} that is unramified away from $\{2, 3, 5, \infty\}$? If so, how many? Unlike the classical inverse Galois problem, this family of questions is still very interesting when the Galois group is a symmetric or alternating group.

There are several sources of such interesting number fields, where it is possible to say something nontrivial about several simultaneous invariants, for example coming from modular forms or specializations of branched covers. Dynamical systems also provide interesting examples of number fields. Preimage fields of PCF morphisms are particularly interesting, since they provide infinite towers of number fields which are unramified away from a finite set of primes. We can also say something about the Galois groups, as they are subgroups of iterated wreath products.

I do not know of any systematic study of other arithmetic invariants associated to preimage fields of dynamical systems. In the case of class groups, this question has an Iwasawa-theoretic flavor. For example, if $K = \mathbb{Q}(\zeta_p)$ and $\phi(x) = x^p$ and $K_n = K(\phi^{-n}(1))$, then the K_n's form the cyclotomic $\mathbb{Z}_p$-tower of K, and Iwasawa theory studies the p-part of the class number of K_n. Is it possible to do Iwasawa theory more generally for PCF morphisms?

I have not devoted significant effort to this last problem, but if other people at the workshop are interested, I would love to work on it.

A.14 Silverman, Joseph

I am interested in all aspects of the Galois theory of fields generated by special points of dynamical systems. Recently Michelle Manes and I have been investigating rational maps of P^2 having non-trivial automorphism groups. These maps, with their added structure, might provide good first candidates for studying dynatomic and arboreal representations in dimension greater than one. Here's a question: (Maybe easy? I haven't spent time thinking about it.) Let $f : P^2 \to P^2$ be a dominant rational map of degree 2 that is algebraically stable and such that $Aut(f)$ is isomorphic to the orthogonal group $O(2)$. What can one say about its arboreal representations?

The following is highly speculative: Let $f_c(x) = x^2 + c$, fix a basepoint b, let T_n be the binary tree based at b obtained from the first n-fold backward iterates of b. (For simplicity, assume T_n contains no critical points.) Write $W_n = Aut(T_n)$ for the tree automorphism group, and let $W_n \to W_{n-1}$ be the natural map restricting the action to the subtree T_{n-1}.

Question (1): What are the irreducible representations of W_n, and do at least some of them they fit together in an interesting and natural way? (There are many papers in the literature that discuss representations of wreath products.)

Question (2) Assuming that they do, fix a compatible system of (irreducible complex) representations $R_n : W_n \to GL(C)$ in the sense that the R_n's commute with the maps $W_n \to W_{n-1}$. There are now many Sato-Tate type questions that one might ask. For example, take b and c in a finite field F_p, then we can look at the characteristic polynomial of $R_n(Frob_p)$. Of course, we should really include b and c in the labeling, say

$$P(b, c, p, n; X) = char\ poly\ of\ R_n(Frob_p)$$

for $f_c(x)$ and basepoint b.

With an appropriate normalization (how?), take the inverse limit as $n \to \infty$, then what is the distribution of the resulting polyomials as b and/or c range over F_p, say as $p \to \infty$, or alternatively for b and c in F_{p^k} with $k \to \infty$? (Alternatively, take modular representations into $GL(Z/\ell^m Z)$ and then let $m \to \infty$ to get ℓ-adic represenations, instead of using complex representations?)

A.15 Thompson, Bianca

I have been working with Rob Benedetto and Jamie Juul on the following; Looking over a finite field, consider a quadratic polynomial $z^2 + c$. If we look at the pull back of a point that is not periodic do we eventually get 'enough' extensions in a row up one of the branches in the backward orbit tree.

A.16 Tucker, Tom

Here is a general question I would like to know the answer to:

Let K be a number field. Let f be a polynomial with coefficients in K, $\deg f > 1$. Let G denote the inverse limit of the Galois groups of the splitting field of $f^n(x)$ over K. Let G' denote the inverse limits of the Galois groups of the splitting fields of $f^n(x) - t$ over $K(t)$. Suppose that 0 is not periodic under f.

Can anyone come up with an example where G *does not* have finite index in G'? I'm wondering if in particular it might be possible to find a PCF example.

A.17 Walton, Laura

I am particularly interested in problems on forward orbits and functional graphs in dynamics over finite fields, and inverse orbits/arboreal representations in the local fields case. I would like to learn more about these topics, as well as work on problems in these fields. I would also like to learn more about dynamics over global fields.

A.18 Yasufuku, Yu

I am interested in exploring the conditions when the dynamical Galois groups for higher-dimensional self-maps are smaller than expected. For example, does the ambiant variety of the map matter? The construction of the towers of Galois groups is local in the sense that one just takes preimages of a point by iterates. But the condition might depend on the ambient space on which the self-map is defined as a (quasi)-finite morphism (or even without ramification?). Another approach might be looking for a suitable family of self-maps parametrized by B, where B is a curve or a low-dimensional variety, so that the problem reduces to finding rational points on B. It is also presumably constructive to think about more maps for which one can prove a generalization of Stoll's and Jones' criterion. For some or all of the above, I think it is worthwhile to explore connections with standard conjectures in Diophantine geometry. A natural candidate is the (Bombieri)–Lang conjecture (though this would be ineffective). In any case, it would be interesting if we can say something about (some) polynomial maps $[F(X, Y, Z) : G(X, Y, Z) : Z^d]$ on $\mathbb{P}^2$.

A.19 Zieve, Michael

I am interested in all uses of Galois-theoretic methods in dynamics. One question I find particularly intriguing is understanding the rational functions $f(x)$ with coefficients in a number field K which have many periodic points in infinitely many residue fields of K. For instance, Trevor Hyde and I noticed that $(x-1)^n/(x+1)^n$ has many periodic points mod p for infinitely many primes p. If n is even then this doesn't fit into either of the standard sources of examples, namely coordinate projections of group homomorphisms or functions which are bijections mod p for infinitely many primes p. I would like to know whether there is another large source of examples which contains this one, and whether there are further examples. Galois-theoretic methods seem natural to address this topic.