~~Computing arboreal Galois groups of some PCF polynomials~~ Arboreal Galois groups and Odoni's Conjecture

Robert L. Benedetto*
Jamie Juul

Amherst College

A Showcase of Number Theory at Liberal Arts College
JMM San Diego, Thursday, January 11, 2018

Notation

- K is a field, usually a number field
- $\overline{K}$ is the algebraic closure of K
- $f \in K[z]$ is a polynomial of degree $d \geq 2$
- $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n}$ is the n-th iterate of f
- $f^{-n}(x_0) = \left(f^n\right)^{-1}(x_0)$ is the set of n-th preimages of x_0 under f. That is, the set of roots of $f^n(z) - x_0 = 0$.

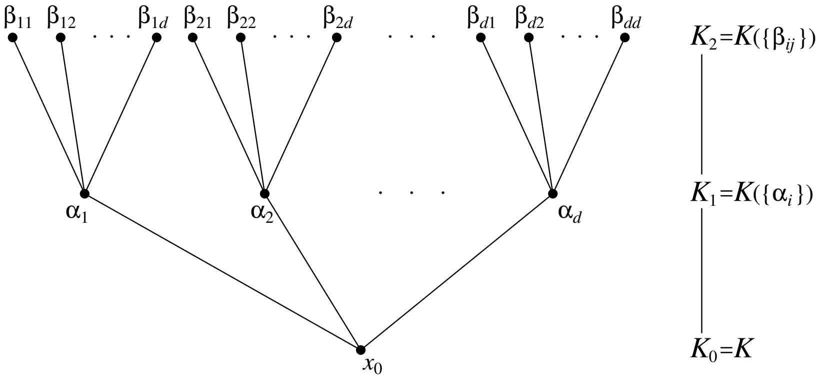
Goal: Given $x_0 \in K$, to understand the action of Galois on the backward orbit

$$\{x_0\} \cup f^{-1}(x_0) \cup f^{-2}(x_0) \cup \cdots$$

A Tower of Extension Fields

Fix $f \in K[z]$ of degree $d \geq 2$, and fix $x_0 \in K$.

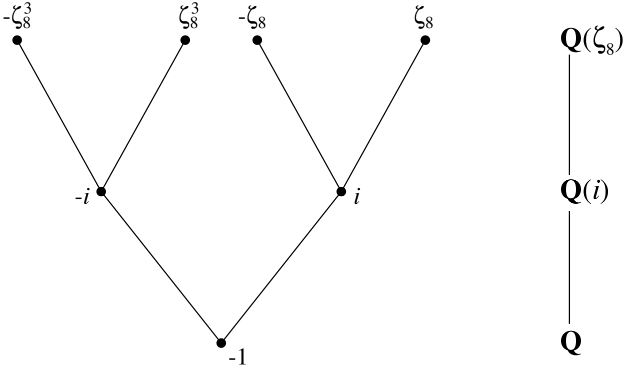
For each $n \geq 0$, let $K_n = K\big(f^{-n}(x_0)\big)$ and $G_n = \mathrm{Gal}(K_n/K)$.



G_n is called an *arboreal Galois group*.

A Misleadingly Simple Example

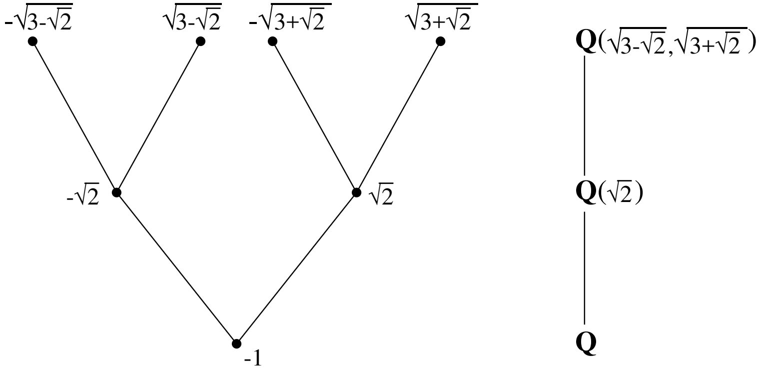
$K = \mathbb{Q}$, $f(z) = z^2$, and $x_0 = -1$.



$G_1 \cong C_2$, and $G_2 \cong C_2 \times C_2$. In general, $G_n \cong (\mathbb{Z}/2^{n+1}\mathbb{Z})^\times$

A More Complicated Example

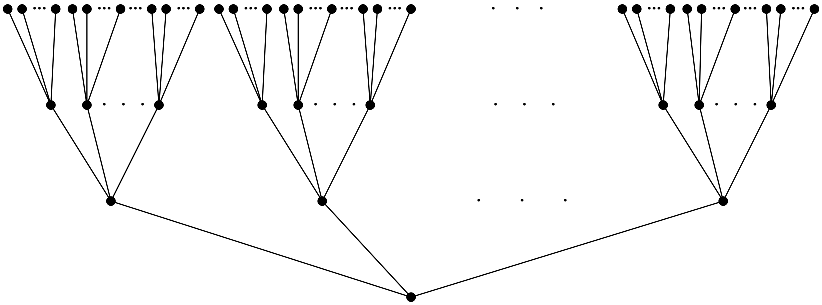
$K = \mathbb{Q}$, $f(z) = z^2 - 3$, and $x_0 = -1$.



$G_1 \cong C_2$, and $G_2 \cong D_4$. In general, G_n consists of (all?) automorphisms of the n-level tree.

$T_{d,n}$ and Aut($T_{d,n}$)

Let $T_n = T_{d,n}$ be a rooted d-ary tree with n levels, and let Aut(T_n) be its automorphism group.



$\mathrm{Aut}(T_1) \cong S_d$, $\mathrm{Aut}(T_2) \cong S_d \wr S_d$, and $\mathrm{Aut}(T_n) \cong [S_d]^{\wr n}$.

Note: $\left|\mathrm{Aut}(T_n)\right| = (d!)^{1+d+d^2+\cdots+d^{n-1}}$

How big is G_n in $\mathrm{Aut}(T_{d,n})$?

Because each $\sigma \in G_n$ is completely determined by its action on the roots of $f^n(z) - x_0$,

$$G_n \text{ is isomorphic to a subgroup of } \mathrm{Aut}(T_{d,n}).$$

Question: How big a subgroup of $\mathrm{Aut}(T_{d,n})$?

Expected answer: It should be (essentially) all of $\mathrm{Aut}(T_{d,n})$, unless there is an obvious reason why it can't be.

Note: There is a long list of "obvious" reasons why $[\mathrm{Aut}(T_{d,n}) : G_n]$ would be unbounded as $n \to \infty$, e.g. that f is **postcritically finite**.

Conjecture (Odoni, 1985)

For every degree $d \geq 2$, there is a polynomial $f(x) \in \mathbb{Q}[z]$ of degree d and $x_0 \in \mathbb{Q}$ such that $G_n \cong \mathrm{Aut}(T_{d,n})$ for all $n \geq 0$.

Some past results

- Odoni (1985) proves $G_n \cong \mathrm{Aut}(T_{d,n})$ for a generic polynomial of degree d, and for a specific degree 2 polynomial over $\mathbb{Q}$.
- Stoll (1992) extends Odoni's method to infinitely many degree 2 polynomials over $\mathbb{Q}$.
- Jones (early 2000s) proves various bounded index results assuming each $f^n(z) - x_0$ is irreducible over K.
- Pink (2013), Juul (2014), Juul-Kürlberg-Madhu-Tucker (2015) prove $G_n \cong \mathrm{Aut}(T_{d,n})$ results when K is a function field, under various restrictions on f and x_0.
- Gratton-Nguyen-Tucker (2013) and Bridy-Tucker (2017) prove bounded index for non-PCF quadratic and cubic $f \in K[x]$ under various restrictions on f; for number fields, conditional on *abc*-conjecture for K or Vojta Conjecture.
- Looper (2016) proves Odoni's Conjecture over $\mathbb{Q}$ for **prime** degree $d = p$, using $f(z) = z^p + kpz^{p-1} - kp$ and $x_0 = 0$.

Arbitrary Degree

Theorem (RB, Juul, 2018)

For any $d \geq 2$, there is a polynomial $f \in \mathbb{Q}[z]$ of degree d and a point $x_0 \in \mathbb{Q}$ such that $G_n \cong \mathrm{Aut}(T_{d,n})$, where

$$K_n = \mathbb{Q}\big(f^{-n}(x_0)\big), \quad \textit{and} \quad G_n = \mathrm{Gal}(K_n/\mathbb{Q}).$$

We use $x_0 = \dfrac{b}{a}$, and $f \in \mathbb{Q}[z]$ of the form either

$$f(z) = az^d - bz^{d-1} \quad \text{or} \quad f(z) = a^2z^d - b^2z^{d-2}.$$

Either way, we have $x_0 \mapsto 0 \mapsto 0$.

Discriminants of iterates

Recall: the discriminant of a polynomial $f(z) = Az^d + \cdots$ with roots $\alpha_1, \ldots, \alpha_d$ is

$$\begin{aligned} \mathrm{Disc}(f) = \Delta(f) &= a^{2d-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{d(d-1)/2} d^d A^{d-1} \prod_{f'(\beta)=0} f(\beta). \end{aligned}$$

Let $C = (-1)^{d(d-1)/2} d^d A^{d-1}$. Then for any $n \geq 0$,

$$\Delta\left(f^{n+1}(z) - x_0\right) = C^{d^n} \left[\Delta\left(f^n(z) - x_0\right)\right]^d \prod_{f'(\beta)=0} \left(f^{n+1}(\beta) - x_0\right).$$

Moral: To get a prime $\mathfrak{p}$ to ramify in K_{n+1} but not in K_n, want
$f^{n+1}(\text{crit.pt.}) \equiv x_0 \pmod{\mathfrak{p}}$, but
$f^{\ell}(\text{crit.pt.}) \not\equiv x_0 \pmod{\mathfrak{p}}$ for $1 \leq \ell \leq n$.

Outline of the proof that $G_n \cong \mathrm{Aut}(T_n)$

Recall $f(z) = a^{d-m}z^d - b^{d-m}z^m$ with $x_0 = \dfrac{b}{a}$.

We proceed by induction on $n \geq 0$. Assuming it's true for n:

Step 1. Show that there is a prime $p \nmid ab$ that ramifies in K_{n+1}, but not in K_n. (Use forward orbit of critical point(s) modulo p.)

Step 2. For $\alpha \in f^{-n}(x_0)$, show $\mathrm{Gal}\left(\mathbb{Q}\big(f^{-1}(\alpha)\big)/\mathbb{Q}(\alpha)\right) \cong S_d$

Step 3. Use Step 1 and the particular dynamics of f to show that the inertia group $I_{n+1}(p) \subseteq G_{n+1}$ contains a transposition.

The result is now immediate by group theory.

Step 1: For each n, a new prime $p \nmid ab$ ramifies in K_{n+1}

Use a strategically chosen modulus N so that
$$\prod_{f'(\beta)=0} \left(f^{n+1}(\beta) - x_0\right) \text{ is never a square modulo } N.$$
(After adjusting for contributions from bad primes.)

Thus, for every n, there is a prime $p \nmid ab$ that ramifies in K_{n+1}.

On the other hand, since $x_0 \mapsto 0 \mapsto 0$, no p' that ramified in some previous K_ℓ can ramify in K_{n+1}. So p is a **newly** ramified prime.

Step 2: $G = \mathrm{Gal}\left(\mathbb{Q}(f^{-1}(\alpha))/\mathbb{Q}(\alpha)\right) \cong S_d$

$$f(z) = p_2^{d-m} z^d - p_1^{d-m} z^m \quad \text{and} \quad x_0 = \frac{p_1}{p_2}.$$

$f^{n+1}(z) - x_0$ is Eisenstein at p_1. So for $\alpha \in f^{-n}(x_0)$,
$f(z) - \alpha$ is Eisenstein at $\mathfrak{p}_1$; so irreducible over $\mathbb{Q}(\alpha)$.

So G acts transitively on $f^{-1}(\alpha)$

$f^{n+1}(z) - x_0$ has a degree-m^{n+1} factor over $\mathbb{Q}_{p_2}$ that is totally ramified at p_2.
So $f(z) - \alpha$ has a degree m irreducible factor over $\mathbb{Q}(\alpha)_{\mathfrak{p}_2}$.

So G contains a subgroup that acts transitively on an m-element subset of $f^{-1}(\alpha)$.

By Step 3 (to come), G contains a transposition. Assuming $(m, d) = 1$ and $m > d/2$, can prove $G = S_d$.

Step 3: The inertia group $I(p) \subseteq G_{n+1}$ contains a transposition

Since p ramifies in K_{n+1} but not in K_n, there must be some nontrivial $\sigma \in \mathrm{Gal}(K_{n+1}/K_n) \cap I_{n+1}(p)$.

σ permutes those $\alpha \in f^{-(n+1)}(x_0)$ that are critical points mod $\mathfrak{p}$.

Now use simple facts about the critical orbits of f to show that there are only two such α.

Recap: the Main Theorem

Theorem (RB, Juul, 2018)

For any $d \geq 2$, there is a polynomial $f \in \mathbb{Q}[z]$ of degree d and a point $x_0 \in \mathbb{Q}$ such that $G_n \cong \mathrm{Aut}(T_{d,n})$, where

$$K_n = \mathbb{Q}\big(f^{-n}(x_0)\big), \quad \textit{and} \quad G_n = \mathrm{Gal}(K_n/\mathbb{Q}).$$

Thank you!