Some recent results on arboreal Galois groups

Robert L. Benedetto

Amherst College

Brown Algebra Seminar
Monday, March 12, 2018

Notation

- K is a field, usually a number field
- $\overline{K}$ is the algebraic closure of K
- $\mathbb{P}^1(\overline{K}) = \overline{K} \cup \{\infty\}$ is the projective line over $\overline{K}$
- $f \in K(z)$ is a rational function of degree $d \geq 2$
- $d = \deg(f) = \max\{\deg a, \deg b\}$, where $f = \dfrac{a}{b}$.
  Then $f : \mathbb{P}^1(\overline{K}) \to \mathbb{P}^1(\overline{K})$ is d-to-1 (counting multiplicity).
- $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n}$ 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 $f^n(z) - x_0 = 0$.

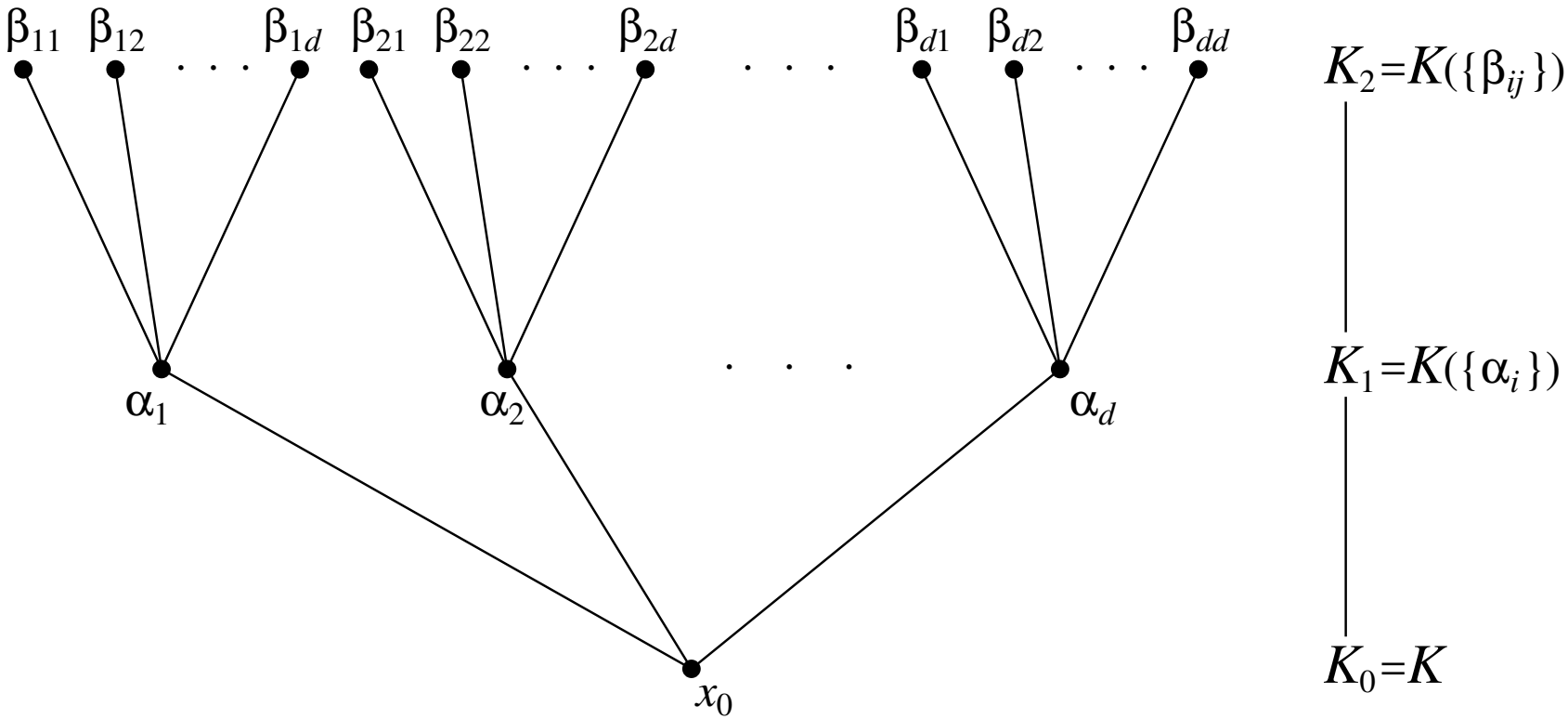
Goal: Given $x_0 \in \mathbb{P}^1(K)$, to understand the action of Galois on the backward orbit

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

A Tower of Extension Fields

Fix $f \in K(z)$ of degree $d \geq 2$, and fix $x_0 \in \mathbb{P}^1(K)$.

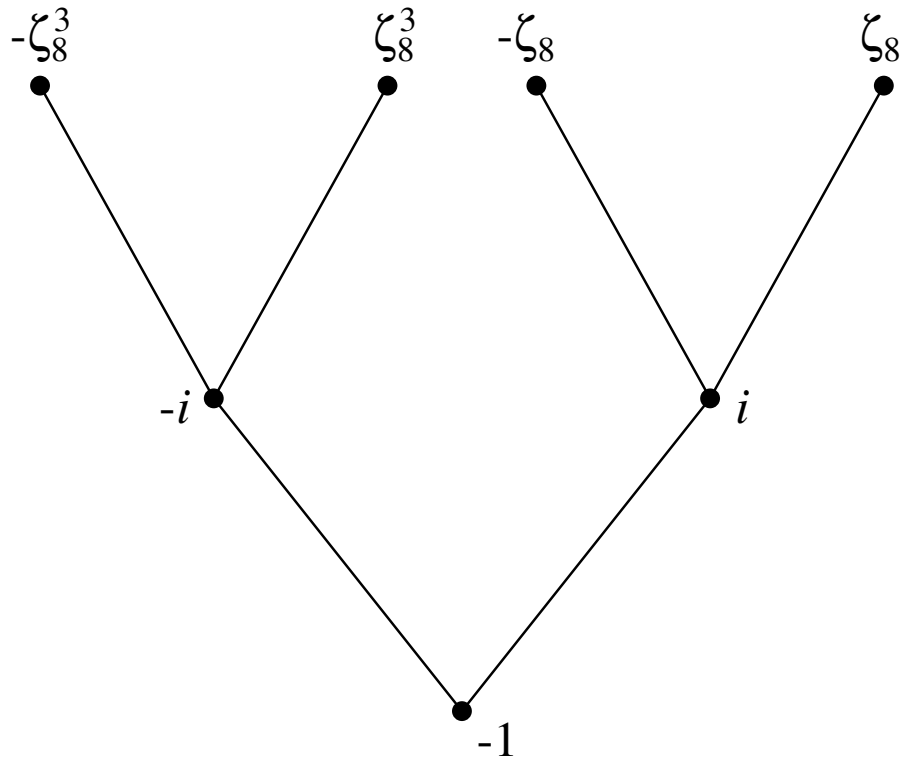
For each $n \geq 0$, let $K_n = K\left(f^{-n}(x_0)\right)$ and $G_n = \mathrm{Gal}(K_n/K)$.

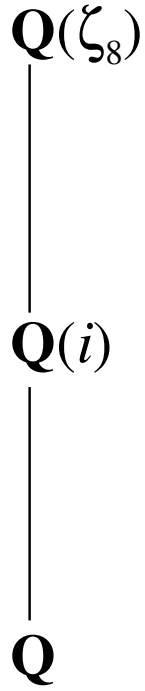


G_n is called an *arboreal Galois group*.

A Misleadingly Simple Example

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

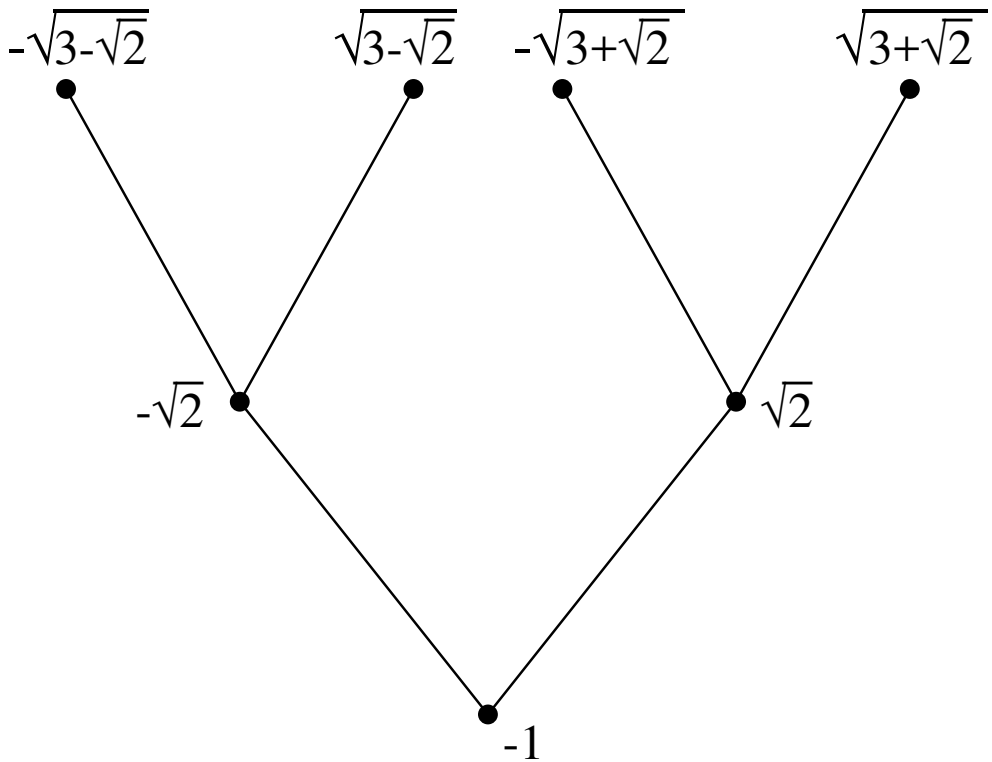


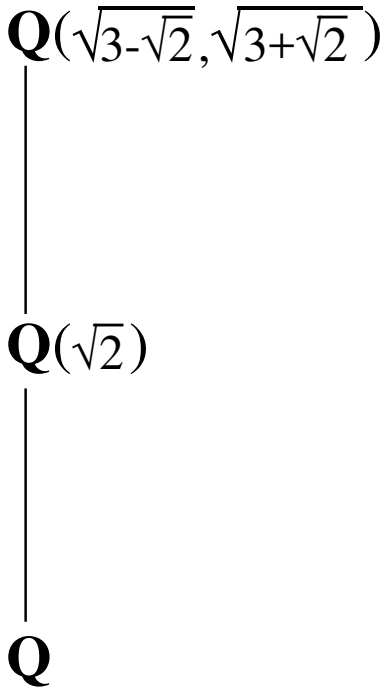


$G_1 \cong C_2$, and $G_2 \cong C_2 \times C_2$.
In general, $G_n \cong (\mathbb{Z}/2^{n+1}\mathbb{Z})^\times \cong C_2 \times C_{2^{n-1}}$

A More Complicated Example

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

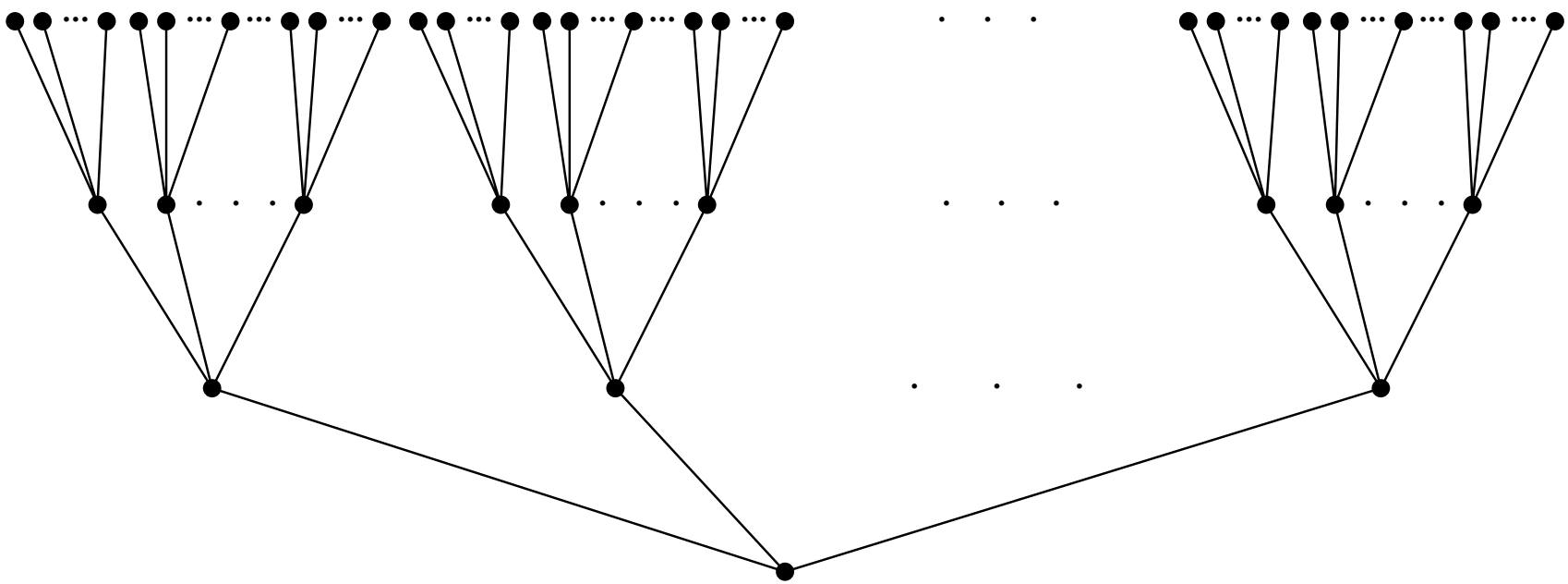




$G_1 \cong C_2$, and $G_2 \cong D_4$. In general, G_n consists of all automorphisms of the n-level tree.

T_n and $\mathrm{Aut}(T_n)$

Let $T_n = T_{d,n}$ be a rooted d-ary tree with n levels,
and let $\mathrm{Aut}(T_n)$ 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 $\mathrm{Aut}(T_n)$?

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

$$G_n \text{ is isomorphic to a subgroup of } \mathrm{Aut}(T_n).$$

Question: How big a subgroup of $\mathrm{Aut}(T_n)$?

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

More precisely, our expectation is that the index $[\mathrm{Aut}(T_n) : G_n]$ is bounded as $n \to \infty$.

That is, $G_\infty = \varprojlim G_n$ has finite index in $\mathrm{Aut}(T_\infty) = \varprojlim \mathrm{Aut}(T_n)$.

Some reasons $[\mathrm{Aut}(T_\infty) : G_\infty] = \infty$ "obviously"

- If the root point $x_0 \in \mathbb{P}^1(K)$ is periodic.
- If there is a critical point in the backward orbit of x_0.
- If $f = g \circ h$ for some $g, h \in K(z)$, both of degree ≥ 2.
- If f is an endomorphism of an algebraic group (or a quotient): **Examples**:
  - $f(z) = z^d$ is an endomorphism of $\mathbb{G}_m$.
  - f is Chebyshev, e.g. $f(z) = z^2 - 2$. (Semi-conjugate to z^d.)
  - f is Lattès. (Semi-conjugate to elliptic curve endomorphism.)
- If $f(h(z)) = f(z)$ for some nontrivial $h \in \mathrm{PGL}(2, \overline{K})$, and if $\deg f \geq 3$. **E.g.:** $f(z) = z^d + c$ with $d \geq 3$, and $h(z) = \zeta_d z$.
- Certain funny coincidences occur in critical points' orbits: e.g. f has only two critical points c_1 and c_2, and $f^n(c_1) = f^n(c_2)$ for some $n \geq 2$. [Observed by Richard Pink.]
- f is **postcritically finite**.

PCF maps

Definition

$f(z)$ is **postcritically finite**, or **PCF**, if every critical point of f has finite forward orbit.

Example. $f(z) = z^2 - 1$.
The only critical point is $c = 0$, and $0 \mapsto -1 \mapsto 0$.

Example. $f(z) = z^2 + i$. The only critical point is $c = 0$, and

$$0 \mapsto \ i \ \mapsto \ i - 1 \ \mapsto \ -i \ \mapsto \ i - 1.$$

Why does PCF imply infinite index?

It's because of the iterated discriminants $\Delta_n = \mathrm{Disc}(f^n(z) - x_0)$.

Once we get to some level M of the tower, K_M already contains $\sqrt{\Delta_n}$ for every $n \geq M$.

So $\mathrm{Gal}(K_n/K_M)$ acts only by even permutations for $n \geq M$.

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 finite index results assuming each $f^n(z) - x_0$ is irreducible over K.
- Pink (2013), Juul (2014), Juul-Kürlberg-Madhu-Tucker (2015) prove $G_\infty = \mathrm{Aut}(T_\infty)$ 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.

A certain PCF cubic

2016 joint work with
Xander Faber, Ben Hutz, Jamie Juul, and Yu Yasufuku:

Consider the following map: $f(z) = -2z^3 + 3z^2$.

Critical points are $0, 1, \infty$; all three are fixed.

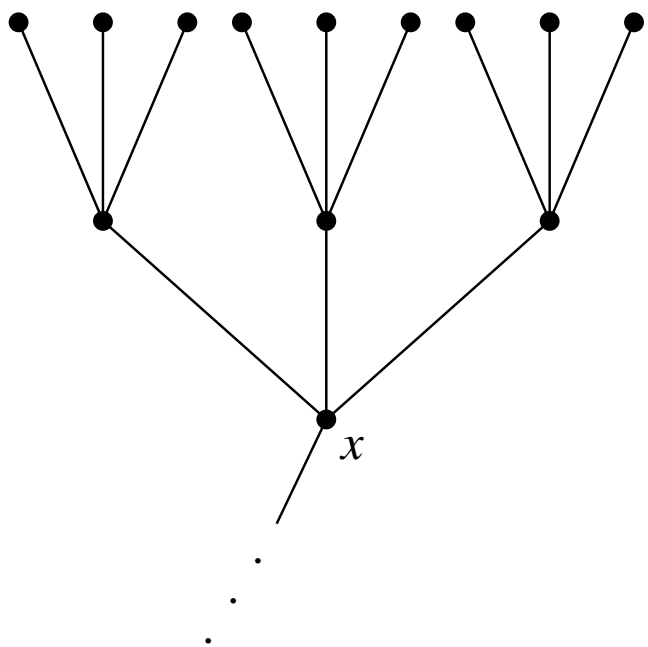
In addition, direct computation shows:

For any $x \in \overline{K}$,

$$\mathrm{Disc}\big(f^2(z) - x\big) = \left[2^{16} \cdot 3^9 \cdot x^2(x-1)^2\right]^2 \in \big(K(x)^\times\big)^2.$$

$f(z) = -2z^3 + 3z^2$, with root point x_0

For any x in the preimage tree of x_0, consider this subtree:



We have $\mathrm{Disc}\left(f^2(z) - x\right) \in \left(K(x)^\times\right)^2$. Hence,

$$\mathrm{Gal}\left(K\left(f^{-2}(x)\right)/K(x)\right) \subseteq \mathrm{Aut}(T_2) \cap A_9.$$

Computing G_n for $f(z) = -2z^3 + 3z^2$

Let E_n be the subgroup of $\mathrm{Aut}(T_n)$ carved out by the condition

$$\text{If } \sigma \in E_n \text{ fixes } x, \text{ then } \sigma \text{ is even on } f^{-2}(x).$$

Theorem (RB, Faber, Hutz, Juul, Yasufuku; 2016)

Let K be a number field.
Let $\mathfrak{p}|2$ and $\mathfrak{q}|3$ be primes of K, and suppose that

- $v_{\mathfrak{q}}(x_0) = 1$, *and*
- **either** $v_{\mathfrak{p}}(x_0) = \pm 1$ **or** $v_{\mathfrak{p}}(1 - x_0) = 1$.

Then the preimage tree of x_0 under $f(z) = -2z^3 + 3z^2$ has $G_n \cong E_n$ for all $n \geq 1$.

Example. Let $K = \mathbb{Q}$, and

$$x_0 \in \left\{3, \pm 6, \pm\frac{3}{2}, 15, -21, \pm 30, \pm\frac{15}{2}, \dots\right\}.$$

A local ramification lemma for $f(z) = -2z^3 + 3z^2$

Lemma

For all $n \geq 0$ and all $y \in f^{-n}(x_0)$, in the field extension $K(y)/K$, the prime $\mathfrak{p}$ ramifies to degree divisible by 2^n, and the prime $\mathfrak{q}$ ramifies to degree divisible by 3^n.

In particular, since $K(y) \subseteq K_n$, the Galois group G_n has order divisible by 6^n.

Sketch of Proof: For $\mathfrak{q}$ (recall: $\mathfrak{q}|3$),

$$f(z) = -2z^3 + 3z^2 \equiv z^3 \pmod{\mathfrak{q}}$$

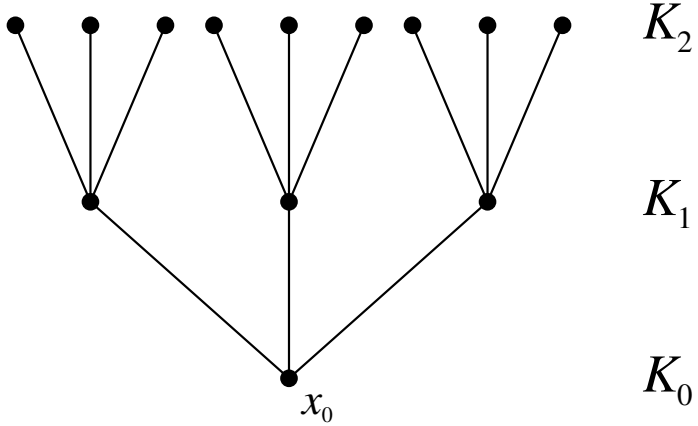
$$\text{so} \qquad f^n(z) \equiv z^{3^n} \pmod{\mathfrak{q}}.$$

Since $v_{\mathfrak{q}}(x_0) = 1$, we must have $v_{\mathfrak{q}}(y) = 1/3^n$.
The proof for $\mathfrak{p}$ and 2^n is similar. "QED"

$G_2 \cong E_2$

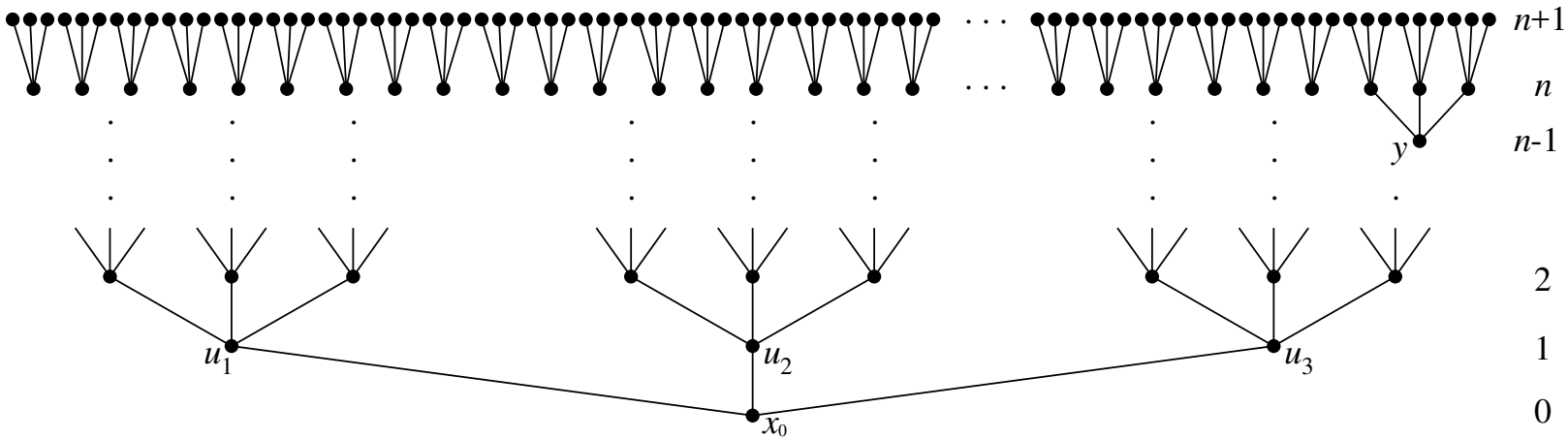
Since $E_1 = S_3$ has order 6, the lemma gives $G_1 \cong E_1$.

But $|E_2| = 2^3 \cdot 3^4 = 648$, while the lemma only tells us that $|G_2|$ is divisible by 36.



- Still, we know $\mathrm{Gal}(K_2/K_1)$ has order divisible by 6.
- So by Cauchy's Theorem, G_2 has elements σ, τ fixing K_1 and of orders 2 and 3.
- Some playing shows we can get all 648 elements of E_2

For $n \geq 2$, $G_n \cong E_n$ implies $G_{n+1} \cong E_{n+1}$



There are four n-high trees here: above x_0, u_1, u_2, and u_3.

Strategically pick elements from each copy of E_n and combine various commutators of them to produce $\lambda \in G_{n+1}$ that acts as:

- two 2-cycles on $f^{-2}(y)$, and
- the identity everywhere else.

Now take products of conjugates of λ to produce all of E_{n+1}.

A PCF quadratic polynomial: $g(z) = z^2 - 1$

Does the existence of a special group E_n in the BFHJY Theorem about $f(z) = -2z^3 + 3z^2$ rely on the special fact that $\mathrm{Disc}(f^2(z) - x)$ is a square, and not just that f is PCF?

Summer 2017 REU at Amherst with:

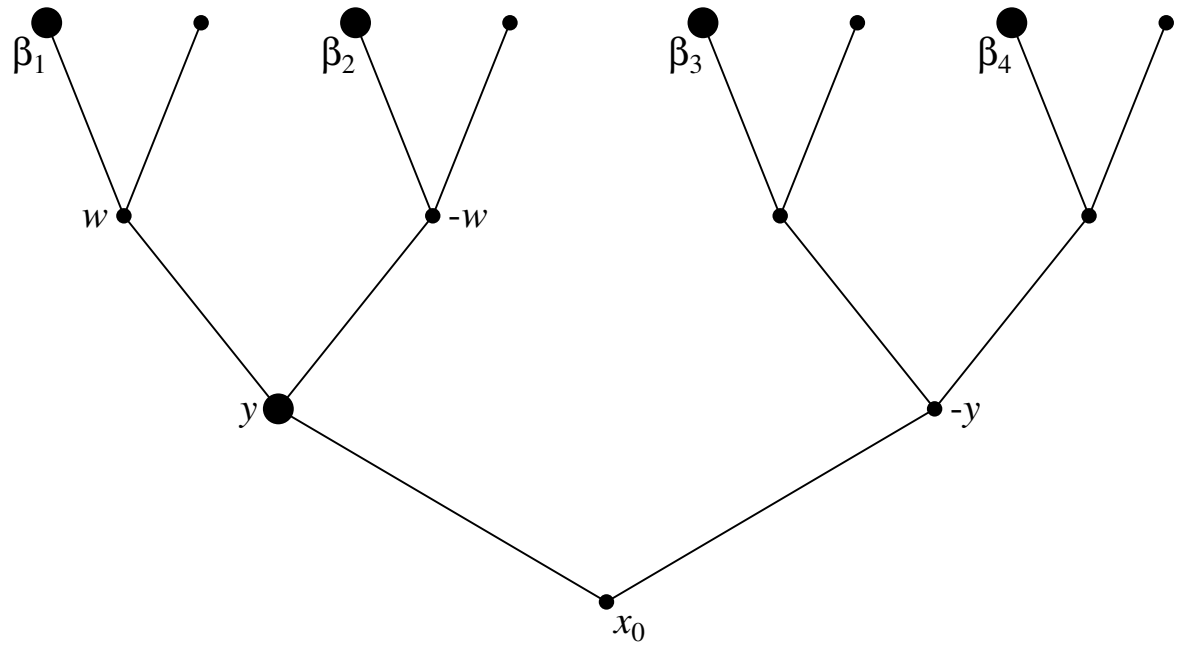
Faseeh Ahmad, Jen Cain, Greg Carroll, Lily Fang

Recall: $g(z) = z^2 - 1$ is PCF, with $0 \mapsto -1 \mapsto 0$.

Question: Is there an analogous subgroup of $\mathrm{Aut}(T_n)$ for g, where $T_n = T_{2,n}$ is a binary rooted tree?

Answer: Yes! But it's more complicated to describe.

A curious identity for $g(z) = z^2 - 1$



$\beta_1^2\beta_2^2 = (w+1)(-w+1) = 1 - w^2 = -y$, so

$$\left(\frac{\beta_1\beta_2\beta_3\beta_4}{y}\right)^2 = \frac{(-y)(y)}{y^2} = -1.$$

So K_3 contains ζ_4, and for $n \geq 4$,
G_n has to act the same on ζ_4 for *every* T_3 subtree of T_n.

The arboreal group for $g(z) = z^2 - 1$

Thus, G_4 must be contained in a certain subgroup of $\mathrm{Aut}(T_4)$ of index $2^{3-1} = 4$,
and G_5 must be contained in a certain subgroup of $\mathrm{Aut}(T_5)$ of index $2^{7-1} = 64$.

But then there is *another* relation forcing K_5 to contain ζ_8, and hence for $n \geq 6$, for G_n to act the same on ζ_8 for every T_5 subtree of T_n.

Similarly for T_7 and ζ_{16}, and in general for T_{2n-1} and ζ_{2^n}.

For each $n \geq 1$, let M_n be the subgroup of $\mathrm{Aut}(T_n)$ carved out by the above conditions.

n	1	2	3	4	5	6	7	8
$\lvert\mathrm{Aut}(T_n)\rvert$	2^1	2^3	2^7	2^{15}	2^{31}	2^{63}	2^{127}	2^{255}
$\lvert M_n\rvert$	2^1	2^3	2^7	2^{13}	2^{25}	2^{47}	2^{91}	2^{177}

The arboreal Galois group for $g(z) = z^2 - 1$

n	1	2	3	4	5	6	7	8
$\lvert \mathrm{Aut}(T_n) \rvert$	2^1	2^3	2^7	2^{15}	2^{31}	2^{63}	2^{127}	2^{255}
$\lvert M_n \rvert$	2^1	2^3	2^7	2^{13}	2^{25}	2^{47}	2^{91}	2^{177}

Theorem (Ahmad, RB, Cain, Carroll, Fang; 2017)

Let K be a number field, let $g(z) = z^2 - 1$, and let $x_0 \in K$. For each $n \geq 1$, let

- $K_n = K\left(g^{-n}(x_0)\right)$, *and*
- $G_n = \mathrm{Gal}(K_n/K)$.

Then

1. *G_n is isomorphic to a subgroup of M_n, and*
2. *if $\left[K_0\left(\sqrt{x_0}, \sqrt{x_0+1}, \zeta_8\right) : K_0\right] = 16$, then $G_n \cong M_n$.*

Note: The $\left[K_0\left(\sqrt{x_0}, \sqrt{x_0+1}, \zeta_8\right) : K_0\right] = 16$ condition is equivalent to saying $[K_5 : K] = |M_5|$.

Odoni's Conjecture

Conjecture (Odoni, 1985)

Let K be a Hilbertian field. [E.g. number field or function field.] Then for every degree $d \geq 2$, there is a monic polynomial $f(z) \in K[z]$ of degree d and $x_0 \in K$ such that

$$G_n \cong \mathrm{Aut}(T_{d,n}) \quad \textit{for all} \quad n \geq 0.$$

Theorem (Looper, 2016)

Let $d = p$ be a prime. Then there is an integer $k \in \mathbb{Z}$ such that for $x_0 = 0$ and

$$f(z) = z^p + kpz^{p-1} - kp \in \mathbb{Q}[z],$$

we have $G_n \cong \mathrm{Aut}(T_{d,n})$ for all $n \geq 0$.

Odoni's Conjecture: VERY recent results

Theorem (Kadets, two weeks ago)

Let $d \geq 20$ be even. Then there is a (not necessarily monic) $f \in \mathbb{Q}[z]$ of degree d such that $G_n \cong \mathrm{Aut}(T_{d,n})$ for all $n \geq 0$.

Theorem (Specter, 10 days ago)

Let K be a number field, and let $d \geq 2$. Then there is a monic polynomial $f \in \mathbb{Q}[z]$ of degree d such that

$$\mathrm{Gal}(K(f^{-n}(0))/K) \cong \mathrm{Aut}(T_{d,n})$$

for all $n \geq 0$.

But anyhow...

Theorem (RB, Juul, 2018)

Let K be a number field and let $d \geq 2$. If either

- *$[K : \mathbb{Q}]$ is odd (e.g. $K = \mathbb{Q}$), or*
- *d is even,*

then there is a monic polynomial $f \in K[z]$ of degree d and a point $x_0 \in K$ such that $G_n \cong \mathrm{Aut}(T_{d,n})$, where

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

For d odd, we use $f(z) = z^d - b^2 z^{d-2}$, where $b = x_0$.

$$\text{So } x_0 \mapsto 0 \mapsto 0.$$

For d even, we use $f(z) = z^d - bz^{d-1}$, where $b = \dfrac{x_0^d}{x_0^{d-1} + 1}$.

$$\text{So } x_0 \mapsto b \mapsto 0 \mapsto 0.$$

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 $n \geq 0$,

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

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 $f(z) = z^d - b^{d-m}z^m$, with $f^2(x_0) = f^3(x_0) = 0$.

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

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

Step 2. Use Step 1 and the particular dynamics of f to show that the inertia group $I_{n+1}(\mathfrak{p}) \subseteq G_{n+1}$ contains a transposition.

Step 3. For $\alpha \in f^{-n}(x_0)$, show $\mathrm{Gal}\left(\mathbb{Q}\left(f^{-1}(\alpha)\right)/\mathbb{Q}(\alpha)\right) \cong S_d$

The result is now immediate by group theory.

Step 1: For each n, a new prime $\mathfrak{p}$ 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 a certain finite set S of primes: bad primes, primes dividing d, etc.)

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

On the other hand, since

$$x_0 \mapsto 0 \mapsto 0 \quad \text{or} \quad x_0 \mapsto b \mapsto 0 \mapsto 0,$$

no $\mathfrak{q}$ that ramified in some previous K_ℓ can ramify in K_{n+1}. So $\mathfrak{p}$ is a **newly** ramified prime.

Step 2: The inertia group $I(\mathfrak{p}) \subseteq G_{n+1}$ contains a transposition

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

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.

So σ transposes those two, and leaves all the rest fixed.

Step 3: $G = \mathrm{Gal}\left(K\left(f^{-1}(\alpha)\right)/K(\alpha)\right) \cong S_d$

$f(z) = z^d - b^{d-m}z^m$ and x_0 with primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ such that:

- $v_{\mathfrak{p}_1}(b) \geq v_{\mathfrak{p}_1}(x_0) = 1$, and
- $v_{\mathfrak{p}_2}(b) \leq v_{\mathfrak{p}_2}(x_0) < 0$.

$f^{n+1}(z) - x_0$ is Eisenstein at $\mathfrak{p}_1$. 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 $K_{\mathfrak{p}_2}$ that is totally ramified at $\mathfrak{p}_2$.
So $f(z) - \alpha$ has a degree m irreducible factor over $K(\alpha)_{\mathfrak{P}_2}$.

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

Step 3 Cont'd: $G = \mathrm{Gal}\left(K\left(f^{-1}(\alpha)\right)/K(\alpha)\right) \cong S_d$

$f(z) = z^d - b^{d-m}z^m$ and x_0 with primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ such that:

- $v_{\mathfrak{p}_1}(b) \geq v_{\mathfrak{p}_1}(x_0) = 1$, and
- $v_{\mathfrak{p}_2}(b) \leq v_{\mathfrak{p}_2}(x_0) < 0$.

Using ramification above $\mathfrak{p}_1$ and $\mathfrak{p}_2$, we've shown:

1. G acts transitively on $f^{-1}(\alpha)$, and
2. G has a subgroup H that acts transitively on $\{\beta_1, \ldots, \beta_m\} \subseteq f^{-1}(\alpha)$.

Also, by Step 2, G contains a transposition.

Using the facts that $\gcd(m, d) = 1$ and $m > d/2$, it is a group theory exercise to prove $G = S_d$.

Summary of Results

Theorem (RB, Faber, Hutz, Juul, Yasufuku; 2016)

Let K be a number field, let $f(z) = -2z^3 + 3z^2$, and let $x_0 \in K$. Assuming mild restrictions on x_0, we have $G_n \cong E_n \subsetneq \mathrm{Aut}(T_{3,n})$.

Theorem (Ahmad, RB, Cain, Carroll, Fang; 2017)

Let K be a number field, let $g(z) = z^2 - 1$, and let $x_0 \in K$. Assuming mild restrictions on x_0, we have $G_n \cong M_n \subsetneq \mathrm{Aut}(T_{2,n})$.

Theorem (RB, Juul, 2018)

Let K be a number field and let $d \geq 2$. Assuming moderate restrictions on d and K (including all $d \geq 2$ for $K = \mathbb{Q}$), there is a monic polynomial $f \in K[z]$ of degree d and a point $x_0 \in K$ such that $G_n \cong \mathrm{Aut}(T_{d,n})$.