Computing arboreal Galois groups of some cubic polynomials

Robert L. Benedetto

Amherst College

Mathematical Congress of the Americas, Montreal
Special Session on Arithmetic Dynamics
Wednesday, July 26, 2017

Notation

- K is a field, usually a number field
- $\overline{K}$ is the algebraic closure of K
- $\phi \in K(z)$ is a rational function of degree $d \geq 2$

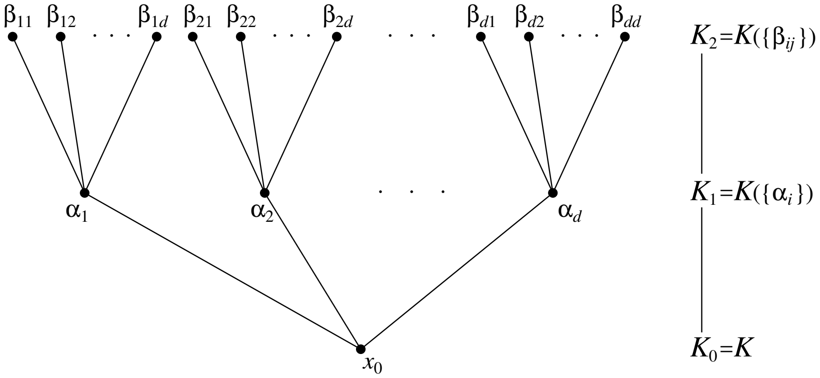
Goal: Given $x_0 \in \mathbb{P}^1(K)$, to understand the action of Galois on the backward orbit

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

A Tower of Extension Fields

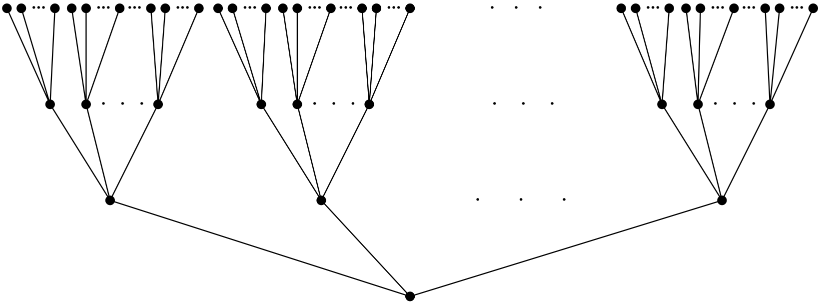
Fix $\phi \in K(z)$ of degree $d \geq 2$, and fix $x_0 \in \mathbb{P}^1(K)$.

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



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

Let T_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 $\phi^n(z) - x_0$,

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

Question: How big a subgoup 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 $\mathrm{Aut}(T_\infty) = \varprojlim \mathrm{Aut}(T_n)$.

When is $[\mathrm{Aut}(T_\infty) : G_\infty]$ "obviously" infinite?

- If the root point x_0 is periodic.
- If there is a critical point in the backward orbit of x_0.
- If $\phi = \psi^n$ for some $\psi \in K(z)$ and $n \geq 2$.
- If ϕ is an endomorphism of an algebraic group (or a quotient).
  Examples:
  - $\phi(z) = z^d$ is an endomorphism of the multiplicative group $\overline{K}^\times$.
  - ϕ is Chebyshev, e.g. $\phi(z) = z^2 - 2$. (Semi-conjugate to z^d.)
  - ϕ is Lattès. (Semi-conjugate to elliptic curve endomorphism.)

When is $[\mathrm{Aut}(T_\infty) : G_\infty]$ "obviously" infinite? (Cont'd)

- If $\phi(h(z)) = \phi(z)$ for some nontrivial $h \in \mathrm{PGL}(2, \overline{K})$, and if $\deg \phi \geq 3$.

  Example: $\phi(z) = z^d + c$ with $d \geq 3$, and $h(z) = \zeta_d z$.

  After the first level we have $\zeta_d \in K_1$.

  At each successive branch, we pick up only C_d, not S_d.

  Thus, $G_n \subseteq [C_d]^{\wr n}$.
  (Well, slightly more complicated at first level if $\zeta_d \notin K_0$.)

- Certain funny coincidences occur in critical points' orbits: e.g. ϕ has only two critical points c_1 and c_2, and $\phi^n(c_1) = \phi^n(c_2)$ for some $n \geq 2$. [Observed by Richard Pink.]

- ϕ is **postcritically finite**.

PCF maps

Definition

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

Why does PCF imply infinite index?

Let N be the length of the longest critical orbit.
Then each discriminant $\Delta_n = \mathrm{Disc}(\phi^n(z) - x_0)$
turns out to be a product of finitely many factors (mostly powers of $\Delta_1, \ldots, \Delta_N$).

Thus, 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 $G_\infty = \mathrm{Aut}(T_\infty)$ for a generic polynomial of degree d.
  Also proves $G_\infty = \mathrm{Aut}(T_\infty)$ for a specific degree 2 polyomial 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 $\phi^n(z) - x_0$ 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 ϕ and x_0.
- Bush-Hindes-Looper (2016) prove $[[C_p]^{\wr\infty} : G_\infty] < \infty$ for infinitely many $\phi(z) = z^p + c$ examples over $\mathbb{Q}$. (Including some with $G_\infty = [C_p]^{\wr\infty}$.)

A certain PCF cubic

For the rest of this talk: $\phi(z) = -2z^3 + 3z^2$.

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

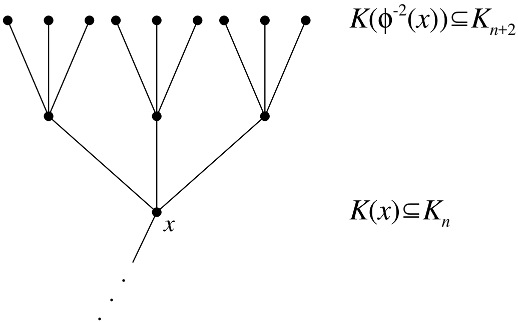
Note: Newton's method for finding the roots of $g(z) = z^3 - z$ requires iterating $\psi(z) = \dfrac{2z^3}{3z^2 - 1}$, which is conjugate to $\phi(z)$. (via $z \mapsto 1/(1-2z)$)

$\phi(z) = -2z^3 + 3z^2$

Direct computation shows: for any $x \in \overline{K}$,

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

So for any x in the preimage tree of x_0, the extension $K\left(\phi^{-2}(x)\right)/K(x)$ has Galois group contained in $\mathrm{Aut}(T_2) \cap A_9$.

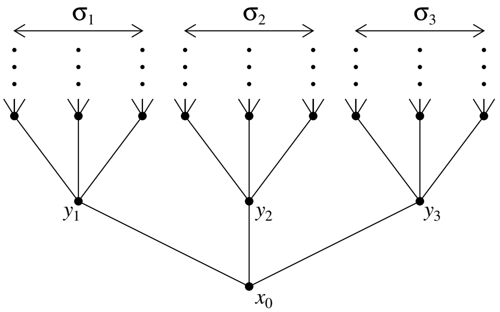


Thus, $G_n \subseteq E_n$, where E_n is the following group:

Let $E_1 = S_3 \quad (\cong \mathrm{Aut}(T_1))$, and $E_2 = \mathrm{Aut}(T_2) \cap A_9$.

For $n \geq 1$: Let $E_{n+1} = \big(E_n \wr S_3\big) \cap \big(A_9 \text{ at level } 2\big)$

That is, to pick an element of E_{n+1}, first choose elements $\sigma_1, \sigma_2, \sigma_3 \in E_n$ to act on the subtrees above y_1, y_2, y_3:



Then choose $\tau \in S_3$ at the bottom, to permute $\{y_1, y_2, y_3\}$, **while ensuring the automorphism is even at level 2**.

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

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 $\phi(z) = -2z^3 + 3z^2$ 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

Lemma

For all $n \geq 0$ and all $y \in \phi^{-n}(x_0)$, 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: $\mathfrak{q}|3$),

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

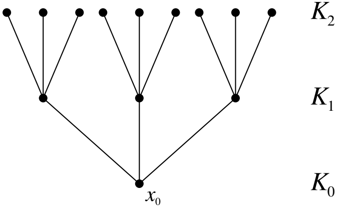
$$\text{so} \qquad \phi^n(z) \equiv z^{3^n} \pmod{\mathfrak{q}}.$$

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"

$G_2 \cong E_2$

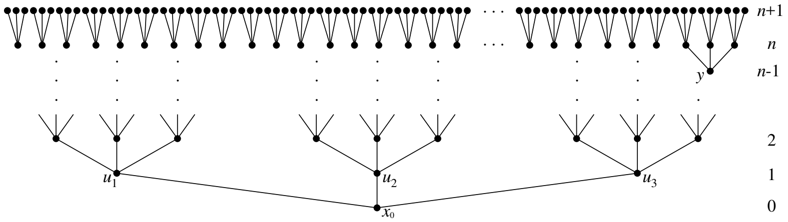
Since $E_1 = S_3$ has order 6, the lemma gives $G_1 \cong E_1$.

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 $\phi^{-2}(y)$, and
- the identity everywhere else.

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

Summary

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

Let K be a number field, let $\phi(z) = -2z^3 + 3z^2$, and let $x_0 \in K$ satisfy certain simple conditions at 2 and 3.

Then the preimage tree of x_0 under ϕ has $G_n \cong E_n$ for all $n \geq 1$, where E_n is a certain subgroup of $\mathrm{Aut}(T_n)$, with

$$|E_n| = 2^{3^{n-1}} \cdot 3^{(3^n-1)/2}, \qquad |\mathrm{Aut}(T_n)| = 6^{(3^n-1)/2},$$

$$\textit{so index is} \quad [\mathrm{Aut}(T_n) : E_n] = 2^{(3^{n-1}-1)/2}.$$

Thank you!