An Arboreal Basilica

Robert L. Benedetto

Amherst College

Arithmetic Dynamics Workshop
Northwestern U
Friday, May 18, 2018

Notation

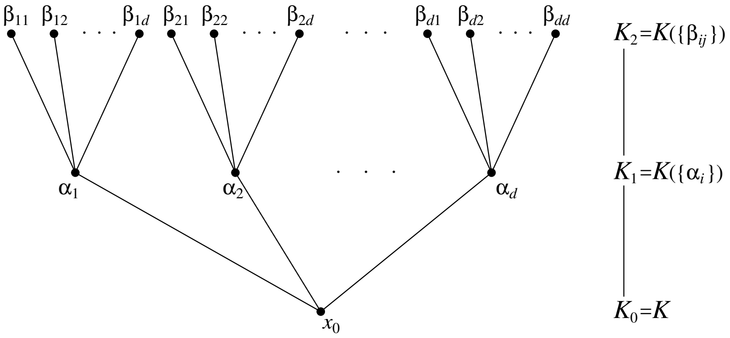
- K is a field, usually a number field
- $\overline{K}$ is the algebraic closure of K
- $f \in K[z]$ is a polynomial of degree $d \geq 2$
- $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n}$ is the n-th iterate of f
- $f^{-n}(x_0) = \left(f^n\right)^{-1}(x_0)$ is the set of n-th preimages of x_0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

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

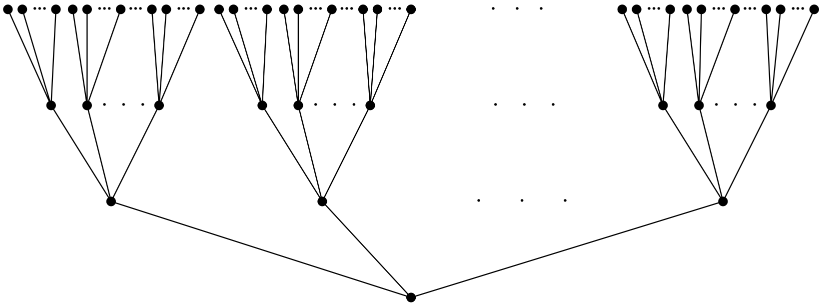


$K_\infty = \bigcup K_n$ and $G_\infty = \varprojlim G_n = \mathrm{Gal}(K_\infty/K)$

G_n and G_∞ are called *arboreal Galois groups*.

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

Let $T_n = T_{d,n}$ be a rooted d-ary tree with n levels, $T_\infty = \bigcup T_n$, and let $\mathrm{Aut}(T_n)$ and $\mathrm{Aut}(T_\infty)$ be their automorphism groups.



$\mathrm{Aut}(T_1) \cong S_d$, $\mathrm{Aut}(T_2) \cong S_d \wr S_d$, 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 $f^n(z) - x_0$,

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

Expectation: $[\mathrm{Aut}(T_n) : G_n]$ is bounded as $n \to \infty$, i.e., $[\mathrm{Aut}(T_\infty) : G_\infty] < \infty$, **unless** there is an obvious reason not.

One such "obvious" reason is that f **is PCF**:

Definition

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

A PCF Arboreal Galois Group: $f(z) = -2z^3 + 3z^2$

Note: besides being PCF, f has all critical points fixed, **and** for any $x \in \overline{K}$,

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

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

If $\sigma \in E_n$ fixes x, then σ 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 $n \geq 1$.

An Arboreal Conversation in Ann Arbor

A year ago at Sarah Koch's awesome Michigan Arithmetic Dynamics workshop:

Rafe Jones asked me:

"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 $\text{Disc}(f^2(z) - x)$ is a square, and not just that f is PCF?"

Summer 2017 REU at Amherst with:

Faseeh Ahmad, Jen Cain, Greg Carroll, Lily Fang

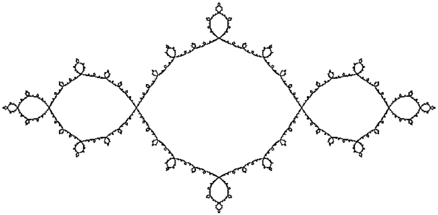
Recall: $g(z) = z^2 - 1$ is PCF, with $0 \mapsto -1 \mapsto 0$.

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

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

$g(z) = z^2 - 1$ over function fields

Let $K = \mathbb{C}(t)$, $g(z) = z^2 - 1$, and $x_0 = t$. The associated arboreal Galois group $G_\infty = \mathrm{Gal}(K_\infty/K)$ is called the **Basilica group** B.



g is a double cover $\mathbb{P}^1(\mathbb{C}) \smallsetminus \{\infty, 0, -1, 1\} \to \mathbb{P}^1(\mathbb{C}) \smallsetminus \{\infty, 0, -1\}$

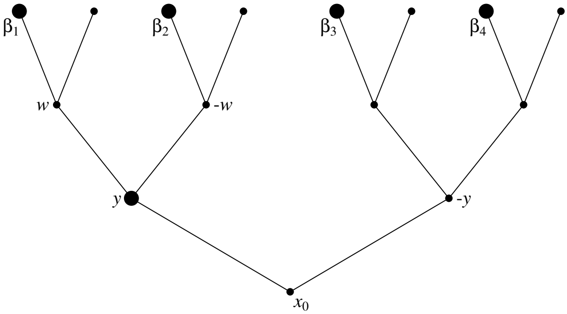
B is a certain well-understood self-similar subgroup of $\mathrm{Aut}(T_{2,\infty})$.

However, $G_\infty \cong B$ relies on the fact that $\mathbb{C}$ is algebraically closed.

Pink (2013) considers G_∞ over other function fields; in general, they are bigger.

So what about number fields?

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



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

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

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 restrictions 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 Arithmetic Basilica Group

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}

More precisely:

- $M_n = \mathrm{Aut}(T_n)$ for $n = 1, 2, 3$.
- $M_n = \left(M_{n-1} \wr S_2\right) \cap H_2$ for $n = 4, 5$,
  where H_2 specifies same action on ζ_4 above x_0 and both preimages of x_0.
- $M_n = \left((M_{n-1}) \wr S_2\right) \cap H_2 \cap H_3$ for $n = 6, 7$,
  where H_3 specifies same action on ζ_8 above x_0 and both preimages of x_0.
- $M_n = \left(M_{n-1} \wr S_2\right) \cap H_2 \cap H_3 \cap H_4$ for $n = 8, 9$,
  where H_4 specifies same action on ζ_{16} above x_0 and both preimages of x_0.

etc.

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

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 $[K_5 : K] = |M_5|$.

Sketch of the proof that $G_n \cong M_n$: Start

Levels 1,2,3:

Direct computation shows $\Delta_n(x) = \mathrm{Disc}(f^n(z) - x) = a_n^2 b_n$, where

$$a_n \in K(x) \quad \text{and} \quad b_n = \begin{cases} 1 + x & \text{if } n = 1, \\ -x & \text{if } n \geq 2 \text{ is even}, \\ -(1 + x) & \text{if } n \geq 3 \text{ is odd}. \end{cases}$$

Our hypothesis gives $[K(\sqrt{x_0}, \sqrt{x_0 + 1}, \sqrt{-1}) : K] = 8$, so we can choose the parities of $\sigma \in G_3 \subseteq \mathrm{Aut}(T_3)$ at levels $n = 1, 2, 3$ independently.

As a result, $G_n \cong M_n \cong \mathrm{Aut}(T_n)$ for $n = 1, 2, 3$.

Also: $\sqrt{-1} \notin K_2$, but $\sqrt{-1} \in K_3$.

Sketch of the proof that $G_n \cong M_n$: Overall Strategy

Inductively prove, for $n \geq 2$:

- K_{2n-1} contains all the 2^n-roots of unity, but K_{2n-2} does not.
- K_{2n-1} contains a 2^n-root of $x_0 + 1$, but K_{2n-2} does not.
- K_{2n} contains a 2^n-root of $-x_0$, but K_{2n-1} does not.
- $G_{2n-1} \cong M_{2n-1}$ and $G_{2n} \cong M_{2n}$

Key Tool: For any $y \in \overline{K}$ and $a, b \in g^{-2}(y)$ with $g(b) = -g(a)$, we have $(ab)^2 = -y$.

Sketch of the proof that $G_n \cong M_n$: Another tool

How do we show K_n does NOT contain certain roots?

Example: Proving K_3 does not contain $\sqrt[4]{-x_0}$:

Let $H = \mathrm{Gal}(K_3/K_1(i))$.

By hypothesis, $\sqrt{-x_0} \notin K_1(i) = K(i, \sqrt{x_0+1})$.

Thus, if $\sqrt[4]{-x_0} \in K_3$, then H has a quotient isomorphic to $\mathbb{Z}/4$.

Hence $H^{\mathrm{ab}} = H/\mathrm{Comm}(H)$ has a quotient isomorphic to $\mathbb{Z}/4$.

Analyze the action of H on T_3 to show that:

$$\text{for all } \sigma \in H, \quad \sigma^2 \in \mathrm{Comm}(H).$$

Contradiction!