An Arithmetic Basilica

Faseeh Ahmad, Robert L. Benedetto*,
Jen Cain, Greg Carroll, Lily Fang

Amherst College

Special Session on Arithmetic Dynamics
AMS Meeting at U Hawaii, Friday, March 22, 2019

Notation

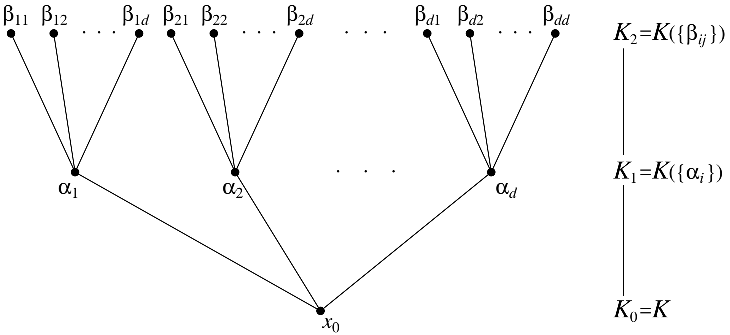
- K is a field, usually a number field
- $\overline{K}$ is the algebraic closure of K
- $f \in K[z]$ is a polynomial of degree $d \geq 2$
- $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n}$ is the n-th iterate of f
- $f^{-n}(x_0) = \left(f^n\right)^{-1}(x_0)$ is the set of n-th preimages of x_0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

$$\mathrm{Orb}_f^-(x_0) := \{x_0\} \cup f^{-1}(x_0) \cup f^{-2}(x_0) \cup \cdots$$

A Tower of Extension Fields

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

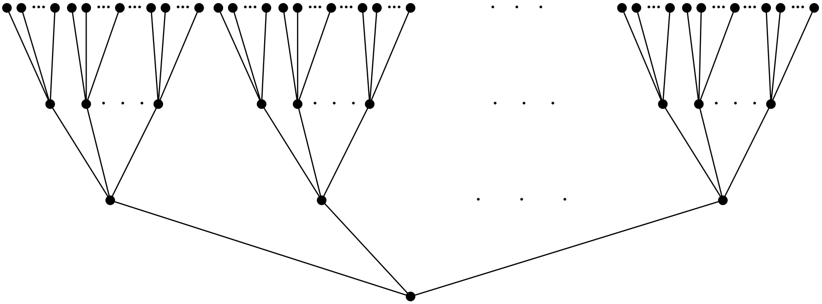


$K_\infty = \bigcup K_n$ and $G_\infty = \varprojlim G_n = \mathrm{Gal}(K_\infty/K)$

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: $g(z) = -2z^3 + 3z^2$

Note: Critical points are $0, 1, \infty$, and

$$0 \mapsto 0, \quad 1 \mapsto 1, \quad \infty \mapsto \infty$$

so g is PCF.

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

There is an (explicitly defined) infinite-index subgroup $E_\infty \subseteq \mathrm{Aut}(T_{3,\infty})$ with the following property.

Let K be a number field, let $x_0 \in K$, and let $K_\infty = K\Big(\bigcup_{n\geq 0} g^{-n}(x_0)\Big)$.
Then $G_\infty = \mathrm{Gal}(K_\infty/K)$ is a subgroup of E_∞.

Moreover, there infinitely many choices of $x_0 \in K$ for which $G_\infty \cong E_\infty$.

$f(z) = z^2 - 1$ Over Number Fields

Summer 2017 REU at Amherst with:

Faseeh Ahmad, Jen Cain, Greg Carroll, Lily Fang

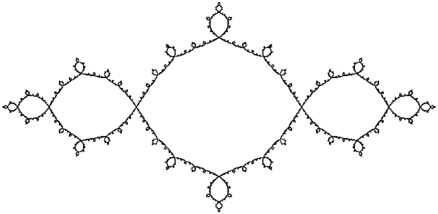
Recall: $f(z) = z^2 - 1$ is PCF, with $0 \mapsto -1 \mapsto 0$.

Question: Is there an analogous subgroup of $\mathrm{Aut}(T_{2,\infty})$ for f?

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

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

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



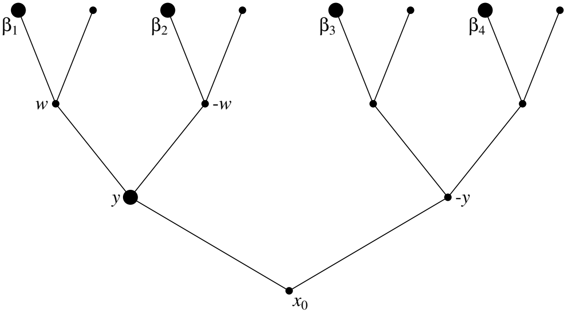
B_∞ is a certain well-understood self-similar subgroup of $\mathrm{Aut}(T_{2,\infty})$.

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

[Pink (2013) considers G_∞ over other function fields.]

What about over number fields?

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

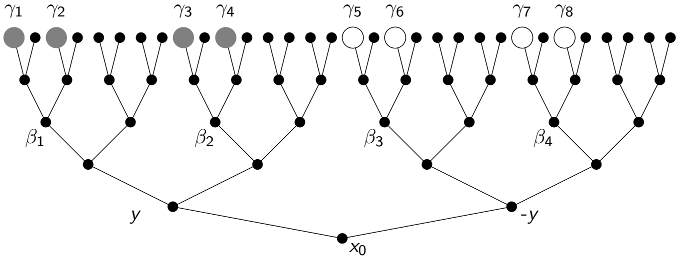


$\beta_1^2 \beta_2^2 = (w+1)(-w+1) = 1 - w^2 = -y$, so

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

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.

More arboreal restrictions for $f(z) = z^2 - 1$



$$\left(\frac{\gamma_1\gamma_2\gamma_3\gamma_4}{\gamma_5\gamma_6\gamma_7\gamma_8}\right)^4 = \left(\frac{\beta_1\beta_2}{\beta_3\beta_4}\right)^2 = \frac{-y}{y} = -1.$$

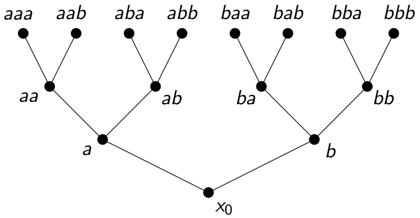
So K_5 contains ζ_8, and for $n \geq 6$,
G_n has to act the same on ζ_8 for *every* T_5 subtree of T_n.

And so on.

How do we describe this?

Labeling and Parity

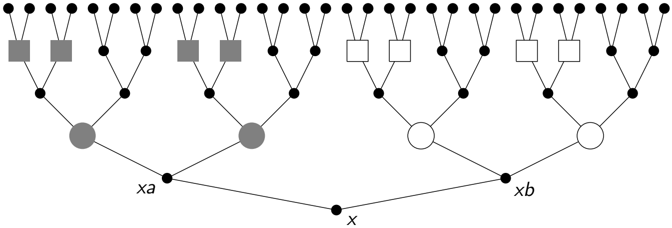
Label each node of $T_{2,n}$ at m-th level by a word in $\{a, b\}^m$:



For $\sigma \in \mathrm{Aut}(T_{2,n})$ and a node x of $T_{2,n}$ define the *parity* $\mathrm{Par}(\sigma, x)$ of σ at x to be

$$\mathrm{Par}(\sigma, x) := \begin{cases} 0 & \text{if } \sigma(xa) = \sigma(x)a \text{ and } \sigma(xb) = \sigma(x)b \\ 1 & \text{if } \sigma(xa) = \sigma(x)b \text{ and } \sigma(xb) = \sigma(x)a \end{cases}$$

Describing the Basilica



For any node x in the tree, labelled $x \in \{a, b\}^m$, define

$$P(\sigma, x) := (-1)^{\mathrm{Par}(\sigma,x)} + 2 \sum_{t \in \{a,b\}} \left[Q(\sigma, xbt) - Q(\sigma, xat) \right],$$

where $Q(\sigma, x) := \sum_{i \geq 0} 2^i \sum_{s_1,\ldots,s_i \in \{a,b\}} \mathrm{Par}(\sigma, xas_1as_2 \cdots as_i) \in \mathbb{Z}_2.$

Note: $P(\sigma, x) \in 1 + 2\mathbb{Z}_2 = \mathbb{Z}_2^\times \cong \mathrm{Gal}\left(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}\right)$

The Arithmetic Basilica

Write $T_\infty := T_{2,\infty}$, with root node x_0. Define
$M_\infty := \{\sigma \in \mathrm{Aut}(T_\infty) \big| P(\sigma, x) = P(\sigma, x_0) \text{ for all nodes } x \text{ of } T_\infty\}$.

Theorem

1. *M_∞ is a subgroup of* $\mathrm{Aut}(T_{2,\infty})$
2. $P : M_\infty \to \mathbb{Z}_2^\times$ *by* $\sigma \mapsto P(\sigma, x_0)$
   is a surjective group homomorphism with kernel B_∞.

That is, $$\{e\} \longrightarrow B_\infty \longrightarrow M_\infty \xrightarrow{P} \mathbb{Z}_2^\times \longrightarrow \{1\}$$

For each $n \geq 1$, let B_n, M_n be the restrictions of B_∞, M_∞ to T_n.

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}
$\lvert B_n \rvert$	2^1	2^3	2^6	2^{12}	2^{23}	2^{45}	2^{88}	2^{174}

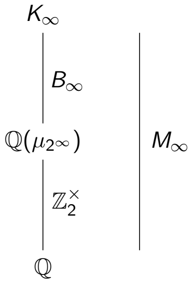
The Expectation/Hope for $f(z) = z^2 - 1$

$$\{e\} \longrightarrow B_\infty \longrightarrow M_\infty \xrightarrow{P} \mathbb{Z}_2^\times \longrightarrow \{1\}$$

Over any field K, we have $K\left(\mu_{2^\infty}\right) \subseteq K_\infty$.

Over $K = \mathbb{C}(t)$ with $x_0 = t$, we have $G_\infty \cong B_\infty$.

So over $\mathbb{Q}$, we should expect:



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

Theorem (Ahmad, RB, Cain, Carroll, Fang; 2017? 2019?)

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

- $K_n = K\big(f^{-n}(x_0)\big)$, *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 $G_{2n} \cong M_{2n}$

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!