Arboreal Galois Groups with Colliding Critical Points

Rob Benedetto

Amherst College

Wednesday, June 5, 2024

Motivation

A key goal of number theory: understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Too hard. So instead:

- Consider a tower of number fields $\cdots K_4 \,/\, K_3 \,/\, K_2 \,/\, K_1 \,/\, K_0$.
- Study the Galois groups $G_n := \mathrm{Gal}(K_n/K_0)$

Example: Fix a prime p, and let $K_n := \mathbb{Q}(\zeta_{p^n})$. Then $G_n := \mathrm{Gal}(K_n/K_0) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$

Example: Fix an elliptic curve $E/\mathbb{Q}$ and a prime ℓ. Let $K_n := \mathbb{Q}(E[\ell^n])$. Then $G_n := \mathrm{Gal}(K_n/K_0) \subseteq GL(2, \mathbb{Z}/\ell^n\mathbb{Z})$

Observation. In both cases, we have $f : X \to X$, and we adjoin iterated preimages of a rational point $P \in X(\mathbb{Q})$:

$$\cdots \xrightarrow{f} X \xrightarrow{f} X \xrightarrow{f} X \xrightarrow{f} X \xrightarrow{f} X$$

Notation

- K is a field, usually a number field
- $\overline{K}$ is the algebraic closure of K
- $f \in K(z)$ is a rational function of degree $d \geq 2$
- $d = \deg(f) = \max\{\deg p, \deg q\}$, where $f = \dfrac{p}{q}$.

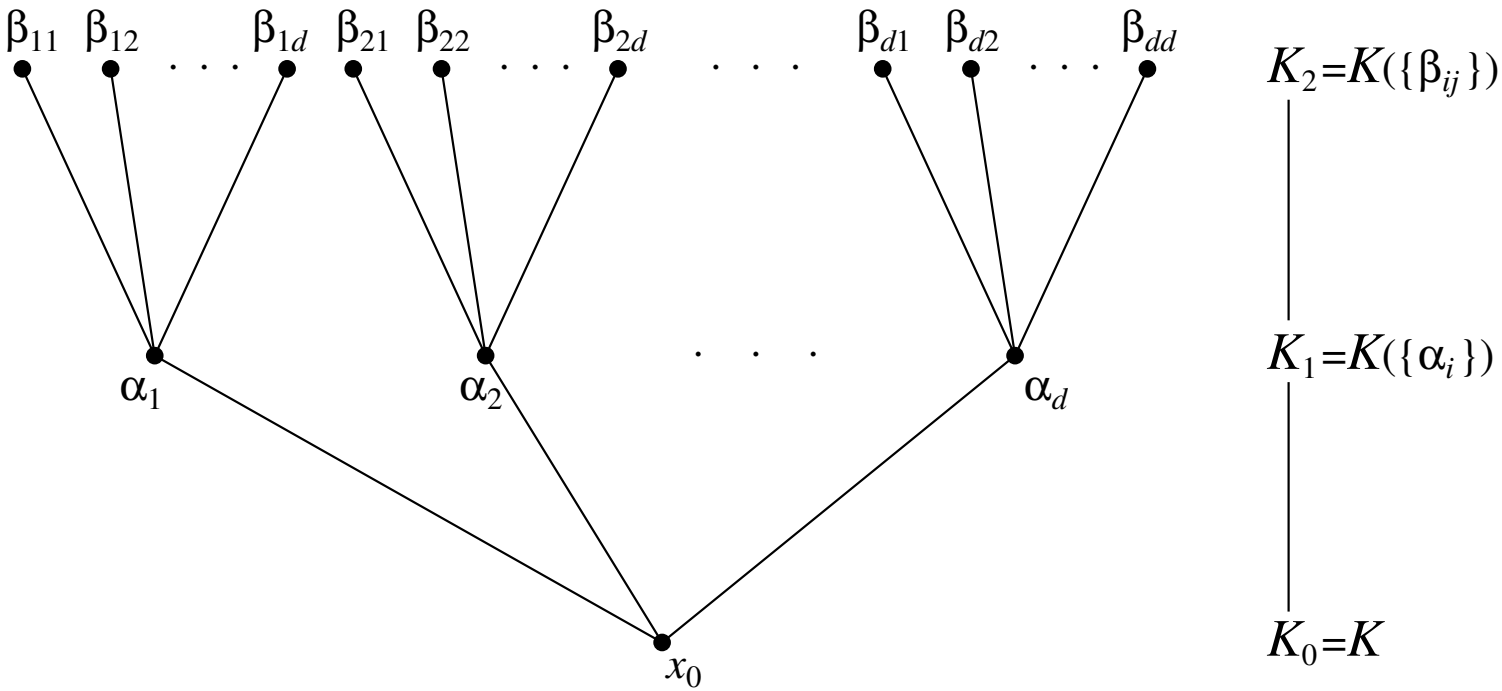
  Then $f : \mathbb{P}^1(\overline{K}) \to \mathbb{P}^1(\overline{K})$ is d-to-1 (counting multiplicity).
- $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n}$ is the n-th iterate of f
- $f^{-n}(x_0)$ is the set of roots of $f^n(z) = x_0$.

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

$$\mathrm{Orb}_f^-(x_0) := \{x_0\} \cup f^{-1}(x_0) \cup f^{-2}(x_0) \cup \cdots \subseteq \mathbb{P}^1(\overline{K})$$

A Tower of Extension Fields

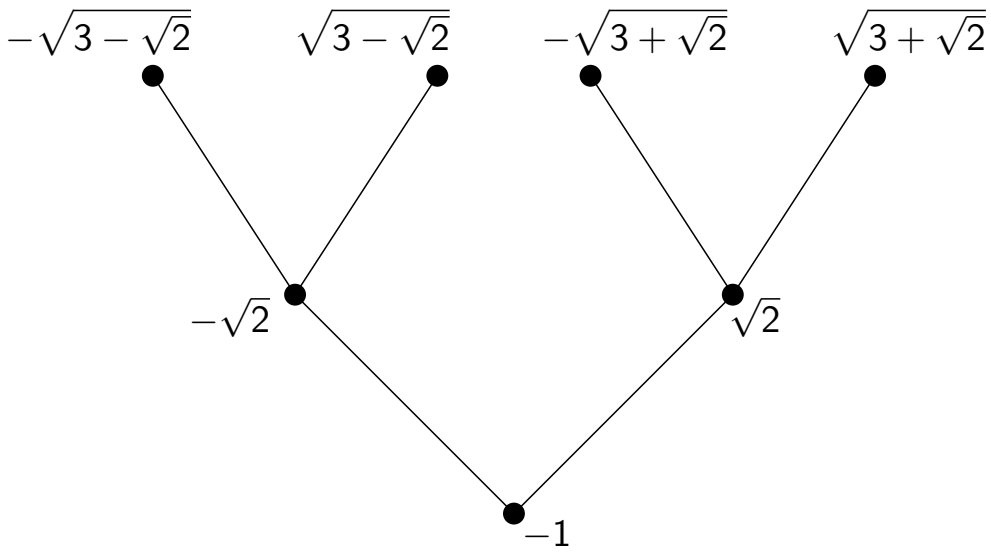
For each $n \geq 0$, let $K_n = K\left(f^{-n}(x_0)\right)$ and $G_n = \mathrm{Gal}(K_n/K)$.

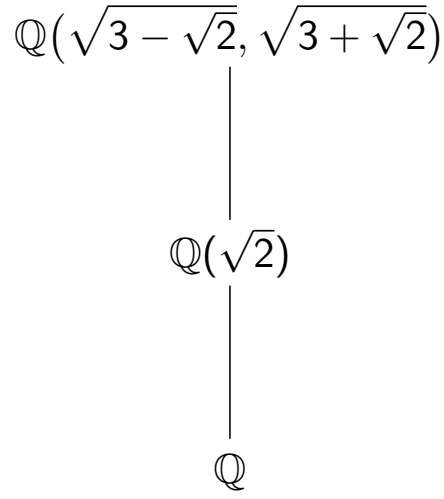


We call the groups G_n *arboreal Galois groups*. Note $G_n \subseteq \mathrm{Aut}(T_{d,n})$, where $T_{d,n}$ is a d-ary rooted tree of n levels.

A Fairly Typical Example

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



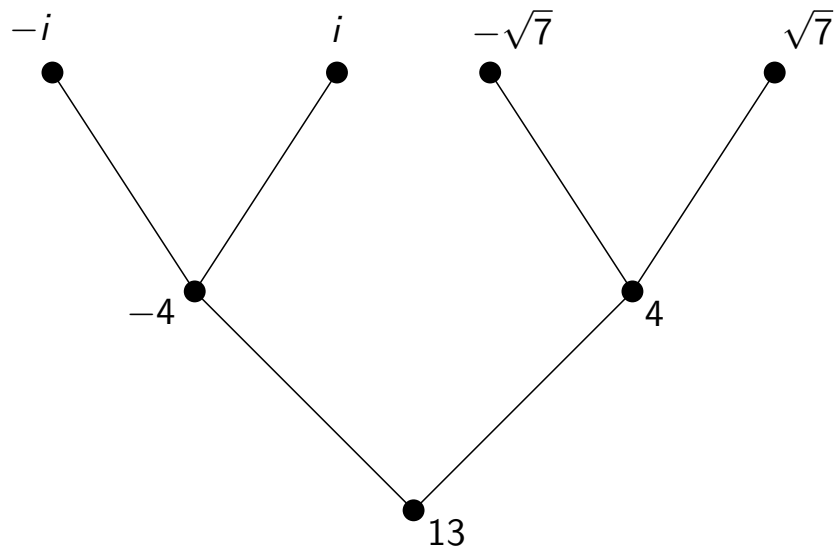


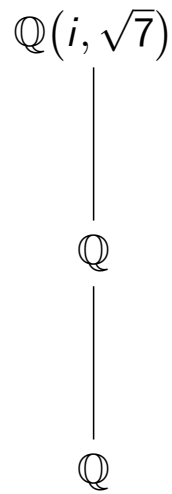
$G_1 \cong C_2$, and $G_2 \cong \mathrm{Aut}(T_{2,2}) \cong D_4$.
In general, $G_n \cong \mathrm{Aut}(T_{2,n})$ consists of all automorphisms of the n-level tree, for all $n \geq 1$.

FYI: For generic quadratic f, we have $G_n \cong \mathrm{Aut}(T_{2,n})$ for all $n \geq 1$.

Forcing a Smaller Galois Group

$K = \mathbb{Q}$, $f(z) = z^2 - 3$, and $x_0 = 13$.

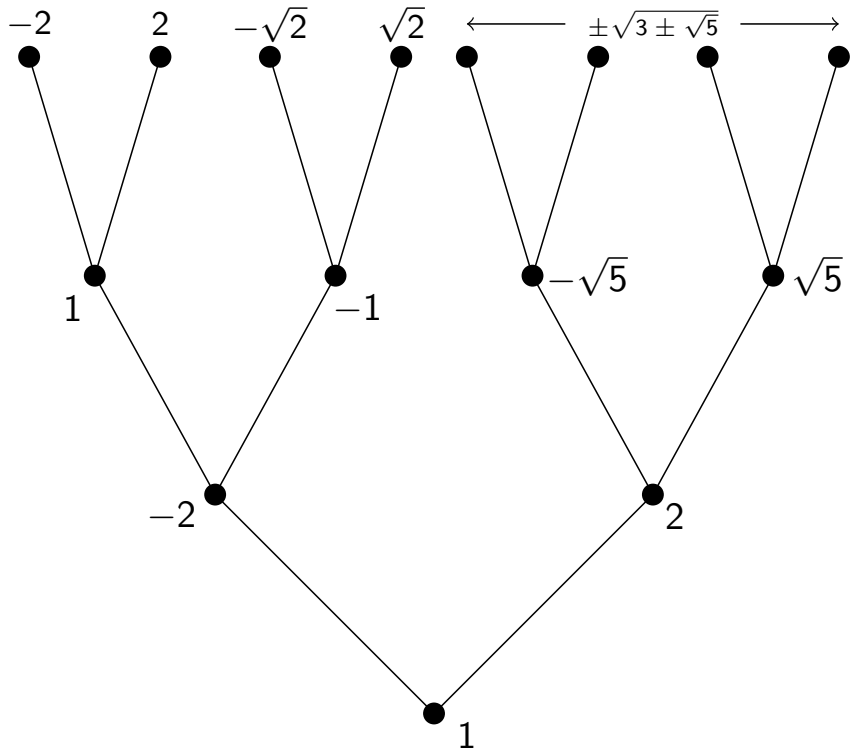


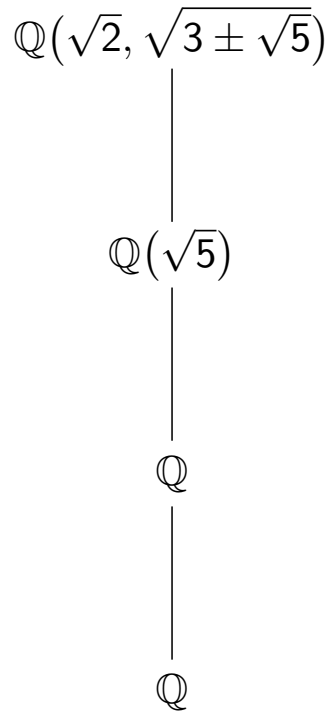


$G_1 \cong \{1\}$, and $G_2 \cong C_2 \times C_2$, so $[\mathrm{Aut}(T_{2,2}) : G_2] = 2$
But after that, the Galois group grows as much as possible:
$[\mathrm{Aut}(T_{2,n}) : G_n] = 2$. (I think!)

Even Smaller

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

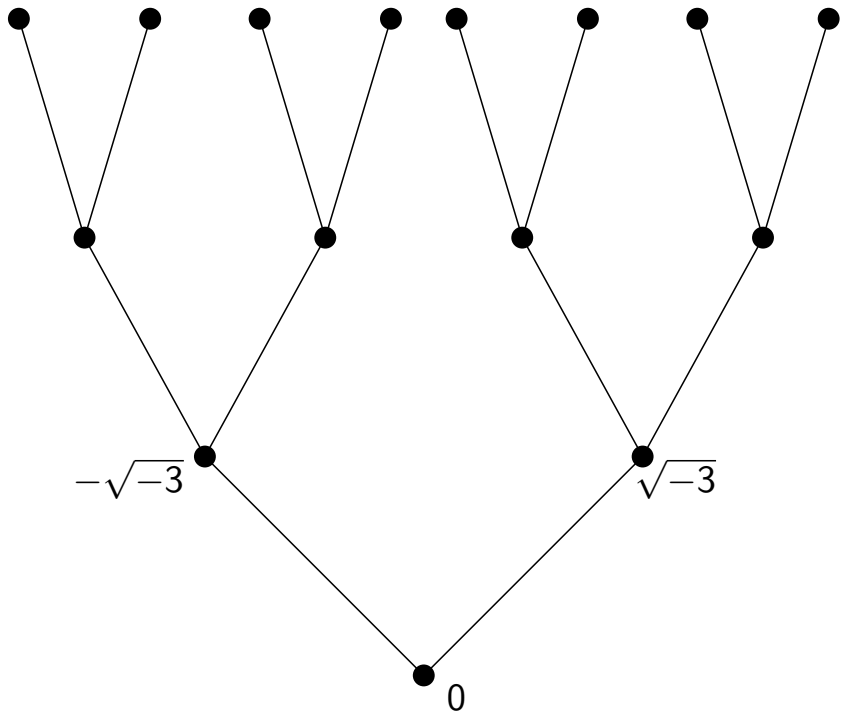


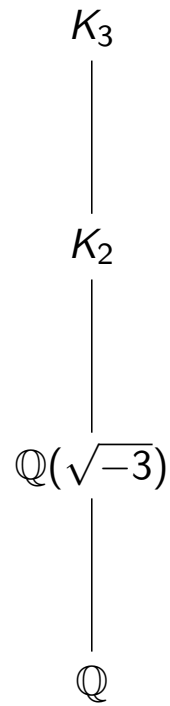


$G_1 \cong \{1\}$, and $G_2 \cong C_2$, so $[\mathrm{Aut}(T_{2,2}) : G_2] = 4$.
After that, $[\mathrm{Aut}(T_{2,n}) : G_n] \to \infty$. The issue: $x_0 = 1$ is periodic.

Another Hiccup That Can Arise

$K = \mathbb{Q}$, $f(z) = z^2 + 3$, and $x_0 = 0$.





Fact. $G_n \cong \mathrm{Aut}(T_{2,n})$ for $n = 1, 2$, but $[\mathrm{Aut}(T_{2,3}) : G_3] = 2$.

And then $[\mathrm{Aut}(T_{2,n}) : G_n] = 2$ for $n \geq 3$. (We think.)

Discriminants

Recall if $P(z) = a_d z^d + \cdots + a_0 = a_d \prod_{i=1}^{d}(z - \alpha_i) \in K[z]$, the *discriminant* of P is

$$\Delta(P) = a_d^{2d-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 \in K.$$

So $\sqrt{\Delta(P)} = a_d^{d-1} \prod_{i<j}(\alpha_i - \alpha_j) \in L = K(\alpha_1, \ldots, \alpha_d)$, and

$$\boxed{\sqrt{\Delta(P)} \in K \Leftrightarrow \begin{array}{l}\text{all } \sigma \in \mathrm{Gal}(L/K) \text{ are even} \\ \text{permutations of } \{\alpha_1, \ldots, \alpha_d\}\end{array}}$$

There are iterative formulas for $\Delta_n := \Delta(f^n(z) - x_0)$ of the form

$$\Delta_n = (\text{fudge factor}) \cdot \Delta_{n-1}^d \prod \left(f^n(\gamma) - x_0\right)$$

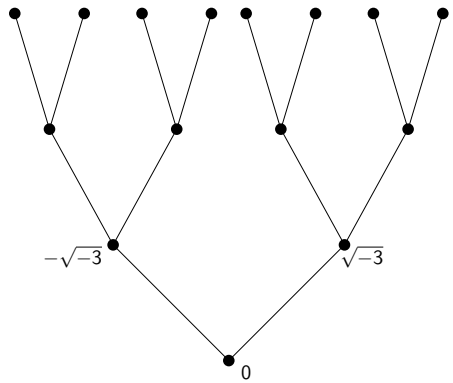
where the product is over all critical points γ of f.

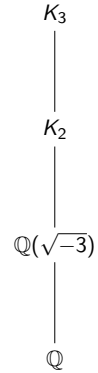
(E.g. Aitken-Hajir-Maire 2005; Jones-Manes 2012)

Moral. To understand the *backward* orbit of x_0, it helps to understand the *forward* orbits of the critical points.

Example Revisited

$K = \mathbb{Q}$, $f(z) = z^2 + 3$, and $x_0 = 0$.





Recall. $G_n \cong \mathrm{Aut}(T_{2,n})$ for $n = 1, 2$, but $[\mathrm{Aut}(T_{2,3}) : G_3] = 2$.

Here's why:

1. The critical orbits are $\infty \mapsto \infty \mapsto \infty \mapsto \cdots$ and
$$0 \mapsto 3 \mapsto 12 \mapsto 147 \mapsto 21612 \mapsto \cdots$$
2. So the discriminant formulas give
$$\Delta_1 = -3 \cdot \square, \quad \Delta_2 = 3 \cdot \square, \quad \Delta_3 = 3 \cdot \square, \quad \Delta_4 = 3 \cdot 1801 \cdot \square$$

Key Point: $\sqrt{\Delta_3} \in K_2$.

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

Recall: $K_n = K\left(f^{-n}(x_0)\right)$ and $G_n = \mathrm{Gal}(K_n/K)$.

$T_{d,n}$ is a d-ary rooted tree with n levels, so $G_n \subseteq \mathrm{Aut}(T_{d,n})$.

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

One "obvious" reason is if x_0 is periodic. Another is if f **is PCF**:

Definition

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

That is, for every critical point $\gamma \in \mathbb{P}^1(\overline{K})$ of f, there are integers $n > m \geq 0$ such that $f^n(\gamma) = f^m(\gamma)$.

Why? Because that would force $\sqrt{\Delta_n} \in K_{n-1}$ for all $n \geq N$, and hence (at least) an extra factor of 2 in the index $[\mathrm{Aut}(T_{d,n}) : G_n]$ for all $n \geq N$.

Colliding Critical Points

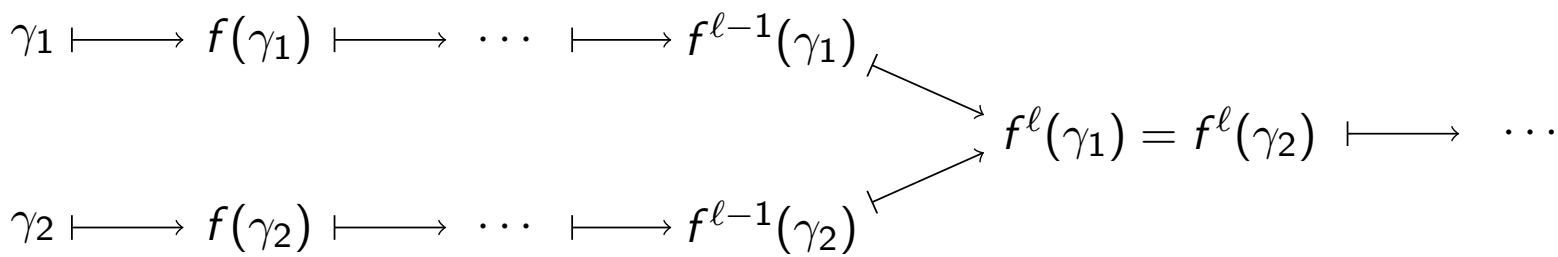
Another "obvious" reason $[\mathrm{Aut}(T_{d,n}) : G_n]$ could be unbounded:

Definition

Let $\gamma_1, \gamma_2 \in \mathbb{P}^1(\overline{K})$ be critical points of $f \in K(z)$, and let $\ell \geq 1$ be an integer.

We say that γ_1 and γ_2 *collide* (at ℓ iterations) if

$$f^\ell(\gamma_1) = f^\ell(\gamma_2), \text{ but } f^i(\gamma_1) \neq f^i(\gamma_2) \text{ for } 0 \leq i < \ell.$$



Pink (2013, unpublished) observed that if f has only two critical points, and if these critical points collide at $\ell \geq 1$ iterations,

then $[\mathrm{Aut}(T_{d,n}) : G_n]$ is unbounded.

Quadratic rational maps with colliding critical points

[Assume char $K \neq 2$.] Fix $\ell \geq 2$.

Let $f \in K(z)$ be a **rational function** of degree $\deg f = 2$ whose two critical points γ_1, γ_2 collide at the ℓ-th iteration.

(The moduli space of such maps is one-dimensional.)

Then for $n \geq \ell$, any $\sigma \in G_n = \mathrm{Gal}(K_n/K)$ acts as an **even permutation** on the 2^n points of $f^{-n}(x_0)$, since

$$\boxed{\Delta_n = \square(\Delta_{n-1})^2\big(f^n(\gamma_1) - x_0\big)\big(f^n(\gamma_2) - x_0\big) \text{ is a square for } n \geq \ell.}$$

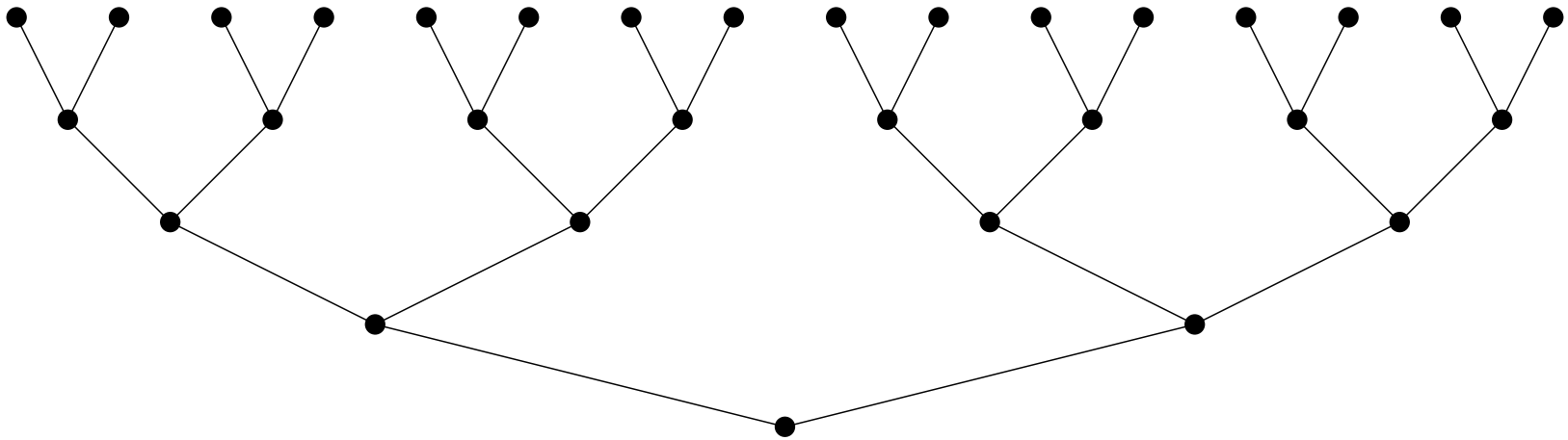
But this parity restriction applies ℓ levels above **every** node of $T_{2,n}$.

Let $M_{\ell,n}$ be the subgroup of $\mathrm{Aut}(T_{2,n})$ carved out by this (repeated) parity restriction.

So $G_n \subseteq M_{\ell,n}$.

Special Case: $d = 2$ and $\ell = 2$

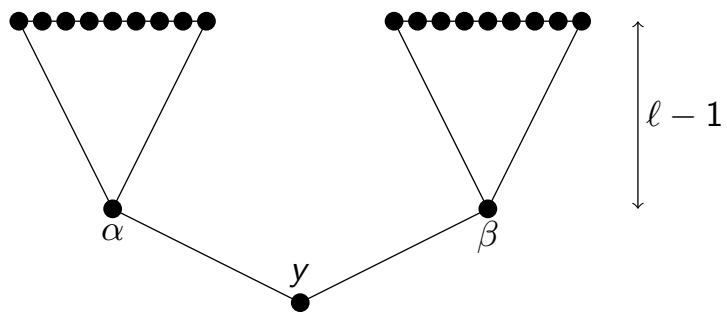
$$G_n = \mathrm{Gal}(K_n/K) \subseteq M_{\ell,n} \subseteq \mathrm{Aut}(T_{2,n})$$



$M_{\ell,n}$ is the subgroup of $\mathrm{Aut}(T_{2,n})$ determined by:

For each node y of the tree, each $\sigma \in M_{\ell,n}$ acts as an even permutation of the 2^ℓ nodes lying ℓ levels above y.

Odd Cousins (at level $\ell \geq 2$). [Joint with Anna Dietrich]



Fix a node y in the tree. We say σ

- acts *positively* above y if σ is even above both α and β.
- acts *negatively* above y if σ is odd above both α and β.

Definition

If $\sigma \in M_{\ell,n}$ acts negatively above an odd number of nodes at level $n - \ell$, we say σ is an **odd-cousins map** at level n.

Colliding critical points for $\deg(f) = 2$

$$K_n = K(f^{-n}(x_0)), \qquad G_n = \mathrm{Gal}(K_n/K), \qquad M_{\ell,n} \subseteq \mathrm{Aut}(T_{2,n})$$

Theorem (RB, Dietrich, 2023)

Let $f \in K(z)$ with $\deg(f) = 2$ such that the two critical points of f collide at the ℓ-th iterate, where $\ell \geq 2$. Then $G_n \subseteq M_{\ell,n}$.
Moreover:
Assume $x_0 \in K$ is not periodic and not postcritical.
There are $\kappa_n \in K$, given by explicit expressions involving f and x_0, such that the following are equivalent:

1. *$G_n = M_{\ell,n}$ for all $n \geq 1$.*
2. *No product $\kappa_{i_1} \cdots \kappa_{i_m}$ (for $i_1 < \cdots < i_m$) is a square in K.*

Idea: For $n \geq \ell$, κ_n is a square in K if and only if there are no odd cousins maps in $\mathrm{Gal}(K_n/K)$.

Cross ratios

Definition

The **cross ratio** of $a, b, c, d \in \mathbb{P}^1(\overline{K})$ is

$$\mathrm{CR}(a, b, c, d) := \frac{(a-b)(c-d)}{(a-c)(b-d)}$$

- Invariant under coordinate change:

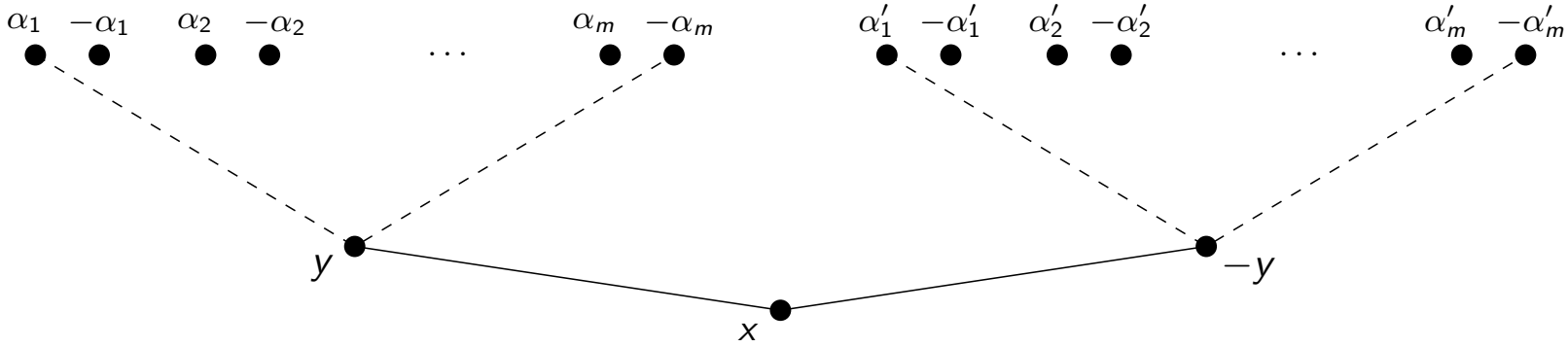
  $$\mathrm{CR}(\eta(a), \eta(b), \eta(c), \eta(d)) = \mathrm{CR}(a, b, c, d)$$

  for a linear fractional transformation $\eta \in \mathrm{PGL}(2, \overline{K})$
- $\mathrm{CR}(a, 0, \infty, 1) = a$
- $\mathrm{CR}(a, b, c, d) \in \overline{K} \smallsetminus \{0, 1\} \Leftrightarrow a, b, c, d$ all distinct

---

So we can move the two critical points of our map f to 0 and ∞, to get $f(z) = \dfrac{Az^2 + B}{z^2 + C}$.

Cross ratios and κ_n



With $f(z) = \frac{Az^2+B}{z^2+C}$ and $0, \infty$ colliding at ℓ-th iterate,

$$\left(\prod_{i=1}^{m} \alpha_i + \prod_{i=1}^{m} \alpha'_i\right)^2 = 4q_{\ell-1} \cdot \mathrm{CR}\left(x, f(0), f^\ell(\infty), f(\infty)\right),$$

where $q_{\ell-1} := (-C)^{2^{\ell-2}} \prod_{i=2}^{\ell-1} \left(\frac{f(\infty)-f^i(\infty)}{f(\infty)-f^i(0)}\right)^{2^{\ell-i-1}} \in K^\times$

So use

$$\kappa_n := \begin{cases} \Delta(f^n - x_0) & \text{if } 1 \le n \le \ell - 1, \\ (*)\,\mathrm{CR}(x_0, f(\gamma_1), f^\ell(\gamma_2), f(\gamma_2)) & \text{if } n = \ell. \\ \mathrm{CR}(x_0, f^{n-\ell+1}(\gamma_1), f^n(\gamma_2), f(\gamma_2)) & \text{if } n \ge \ell + 1, \end{cases}$$

Cubic polynomials with colliding critical points [REU 2022]

Let $f \in K[z]$ with $\deg f = 3$ and such that the two critical points γ_1, γ_2 collide at the ℓ-th iteration, for some $\ell \geq 2$.

The moduli space of such maps is one-dimensional.

Fix $x_0 \in K$ not periodic and not (strictly) post-critical.

This time, the discriminant formula for $\Delta_n := \Delta(f^n - x_0)$ gives:

$$\Delta_n = (\text{square in } K) \cdot (-3) \cdot \Delta_{n-1} \cdot E_n(x_0)$$

where $E_n(x_0) = (f^n(\gamma_1) - x_0)(f^n(\gamma_2) - x_0)$. In particular,

$$\Delta_\ell = \square \cdot (-3) \cdot \Delta_{\ell-1}$$

So any $\sigma \in G_n = \mathrm{Gal}(K_n/K)$ has the same sum of parities $\ell - 1$ levels and ℓ levels above every node of the tree.

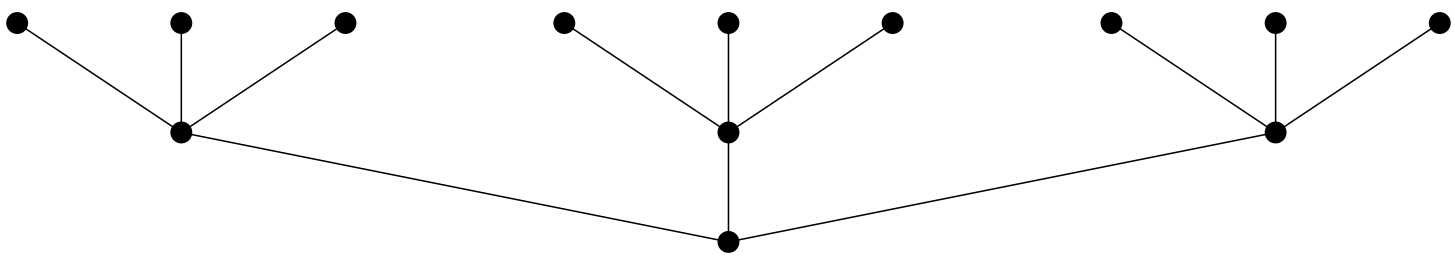
So $G_n \subseteq \widetilde{Q}_n$, the subgroup of $\mathrm{Aut}(T_{3,n})$ carved out by this parity restriction, above **every** node of the tree.

Another Obstacle

The following obstacle arises for every $\ell \geq 2$, but I'll draw diagrams for $\ell = 2$ on the next couple slides.

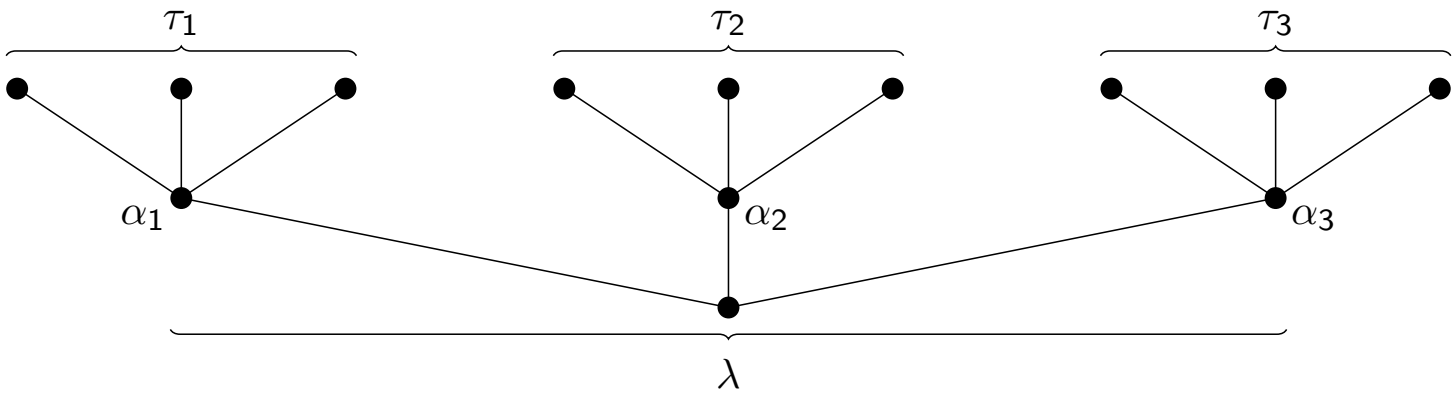
At the second level of the tree, suppose we can show G_2

- acts transitively at level 2, and
- has both even and odd permutations at both levels 1 and 2.



That only forces $|G_2| \geq \frac{1}{4} \cdot 6^4$, vs. $|\widetilde{Q}_2| = |\operatorname{Aut}(T_{3,2})| = 6^4$.

A proper subgroup of Aut($T_{3,2}$)



$$H = \left\{ \left(\lambda, (\tau_1, \tau_2, \tau_3)\right) \,\middle|\, \mathrm{sgn}(\tau_1) = \mathrm{sgn}(\tau_2) = \mathrm{sgn}(\tau_3) \right\}$$

Four conjugate subgroups: $H_1 = H, H_2, H_3, H_4$ of Aut($T_{3,2}$).

H_1 fixes $\delta_1 := \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3$, where $\beta_i = \sqrt{\Delta(f^{\ell-1} - \alpha_i)}$

So we need $g(y) = (y - \delta_1)(y - \delta_2)(y - \delta_3)(y - \delta_4) \in K[y]$
to have no roots in K.

Colliding critical points for $\deg(f) = 3$

Let K be a number field, let $f(z) \in K[z]$ be a cubic polynomial with critical points γ_1, γ_2 such that $f^\ell(\gamma_1) = f^\ell(\gamma_2)$. Let $x_0 \in K$ not periodic.

Let $\tilde{E}_\ell := f^\ell(\gamma_1) - x_0 = f^\ell(\gamma_2) - x_0$.

Fact: In that case, the polynomial $\tilde{g}(y) = (y - \delta_1)(y - \delta_2)(y - \delta_3)(y - \delta_4) \in K[y]$ from the previous slide, but with $E_{\ell-1}(\alpha_i)$ in place of $\sqrt{\Delta(f^{\ell-1} - \alpha_i)}$, is of the form

$$\boxed{\tilde{g}(y) = y^4 + (*)\tilde{E}_\ell y^2 + (*)\tilde{E}_\ell^2 y + (*)\tilde{E}_\ell^2}$$

So if there is a prime $\mathfrak{p}$ of K such that $v_\mathfrak{p}(\tilde{E}_\ell)$ is odd and positive, then $\tilde{g}$ has no K-rational roots, as desired.

Colliding critical points for $\deg(f) = 3$

Let K be a number field, let $f(z) \in K[z]$ be a cubic polynomial with critical points γ_1, γ_2 such that $f^\ell(\gamma_1) = f^\ell(\gamma_2)$, for (minimal) $\ell \geq 2$. Let $x_0 \in K$ not periodic.

Define $\tilde{E}_n := \begin{cases} \left(f^n(\gamma_1) - x_0\right)\left(f^n(\gamma_2) - x_0\right) & \text{if } 1 \leq n \leq \ell - 1, \\ f^n(\gamma_1) - x_0 = f^n(\gamma_2) - x_0 & \text{if } n \geq \ell. \end{cases}$

Theorem (RB,DeGroot,Ni,Seid,Wei,Winton, 2024**)

With notation as above, then $G_n \subseteq \widetilde{Q}_n$.
Moreover, if we suppose:

1. *$f(z) - x_0$ is Eisenstein for some prime $\mathfrak{p}$ of K,*
2. *$[K(\sqrt{-3}) : K] = 2$,*
3. *For each $n \geq 1$, there is a prime $\mathfrak{q}_n \notin \{\mathfrak{p}, \mathfrak{q}_2, \ldots, \mathfrak{q}_{n-1}\}$ of K such that $v_{\mathfrak{q}_n}(\tilde{E}_n) > 0$ is odd,*
4. *(plus some minor restrictions on the previous condition).*

Then $G_n = \tilde{Q}_n$ for all $n \geq 1$.

Thank you!!