Arboreal Galois Groups: An Introduction

Rob Benedetto

Amherst College

Wednesday, April 24, 2024

Field Extensions and Galois Groups

K is a field (assume of characteristic zero), often $\mathbb{Q}$ or $\mathbb{C}(t)$

Given a polynomial $f = a_d z^d + \cdots + a_0 = a_d \prod_{j=1}^{d} (z - \alpha_j) \in K[z]$,

we have a (*normal*) *field extension* $L = K(\alpha_1, \ldots, \alpha_d)$ of K.

We have $K \subseteq L$, but we often write L/K or $\begin{matrix} L \\ | \\ K \end{matrix}$

In that case, the associated *Galois group* is

$$\boxed{\mathrm{Gal}(L/K) = \{\sigma : L \to L \text{ field isomorphism} \,|\, \forall a \in K,\, \sigma(a) = a\}}$$

Note. $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of S_d,
since any $\sigma \in \mathrm{Gal}(L/K)$:

- maps roots of f to roots of f
- is determined by how it permutes those roots.

Examples of Galois Groups

$$\boxed{\mathrm{Gal}(L/K) = \{\sigma : L \to L \text{ field isomorphism} \,|\, \forall a \in K,\, \sigma(a) = a\}}$$

Example. Fix $n \geq 1$. Let $\zeta_n := e^{2\pi i/n}$, a root of $z^n - 1 \in \mathbb{Q}[z]$. Then

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \quad \text{by} \quad (\zeta_n \mapsto \zeta_n^j) \leftarrow\!\shortmid j.$$

Abelian group of order $\phi(n) = |\{0 \leq j \leq n-1 \,|\, \gcd(j,n) = 1\}|$.

Example. Let $f = z^8 - 3 \in \mathbb{Q}[z]$, with roots $\zeta_8^j \cdot \sqrt[8]{3}$. Then

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_8, \sqrt[8]{3})/\mathbb{Q}\right) \cong C_8 \rtimes (\mathbb{Z}/8\mathbb{Z})^\times$$

Non-abelian group of order $8 \cdot 4 = 32$.

Example. Let $f = z^8 - 2 \in \mathbb{Q}[z]$, with roots $\zeta_8^j \cdot \sqrt[8]{2}$. Then

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_8, \sqrt[8]{2})/\mathbb{Q}\right) \cong C_8 \rtimes (\mathbb{Z}/4\mathbb{Z})^\times$$

Non-abelian group of order $8 \cdot 2 = 16$.

Backward orbits

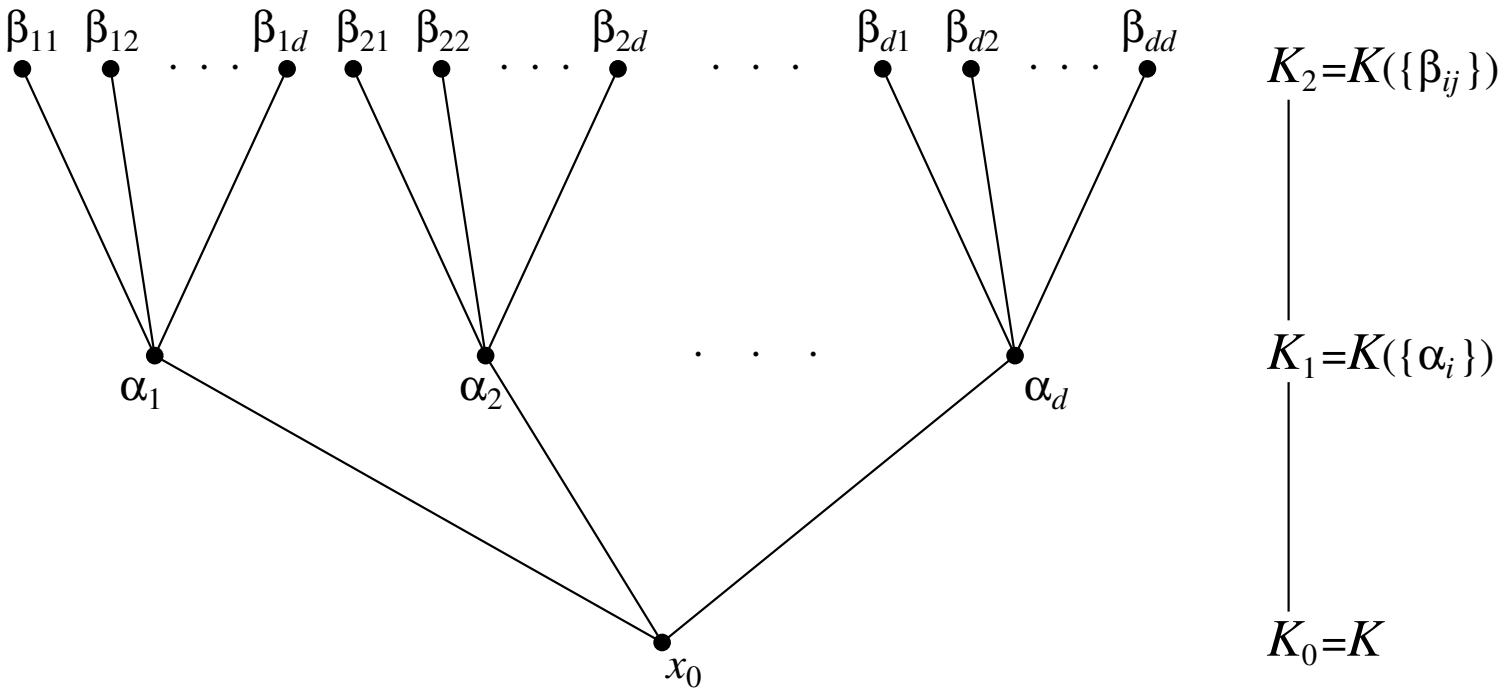
- K is a field (usually of characteristic zero)
- $\overline{K}$ is an algebraic closure of K
- $f \in K[z]$ is a polynomial of degree $d \geq 2$
- $f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n}$ is the n-th iterate of f
- $f^{-n}(x_0)$ is the set of roots of $f^n(z) = x_0$

Goal: Given $x_0 \in K$,
to understand the action of Galois on the backward orbit

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

A Tower of Extension Fields

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

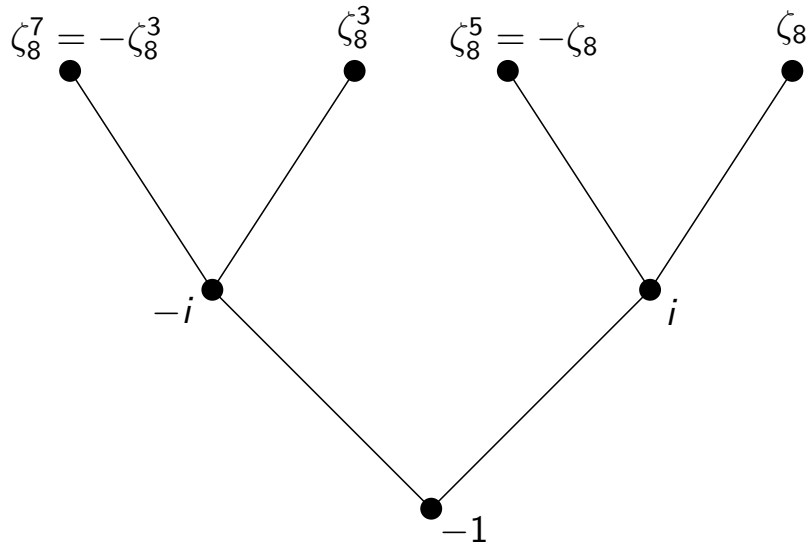


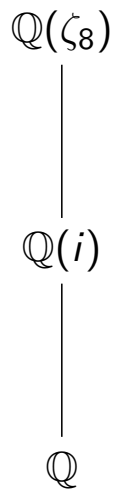
We call the groups G_n *arboreal Galois groups*.

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

A Misleadingly Simple Example

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

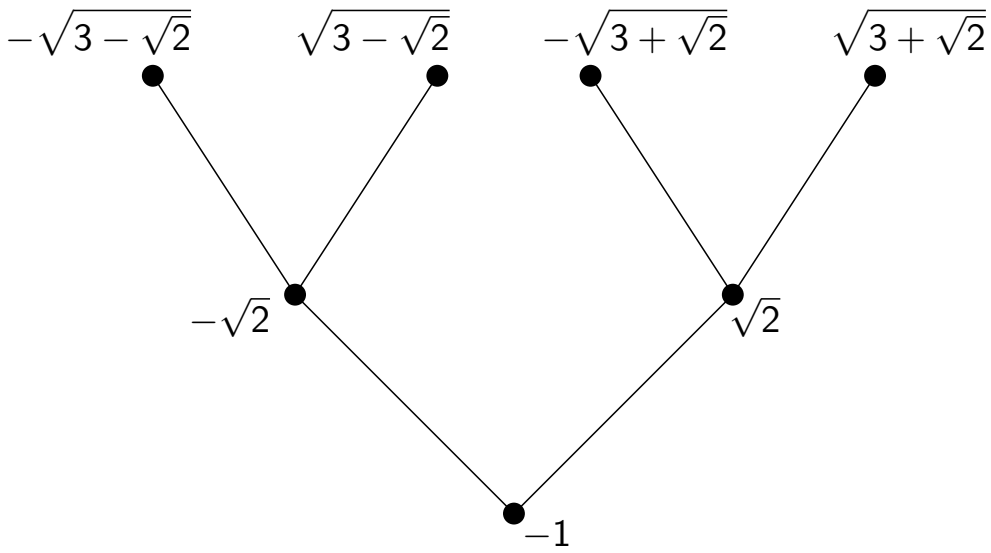


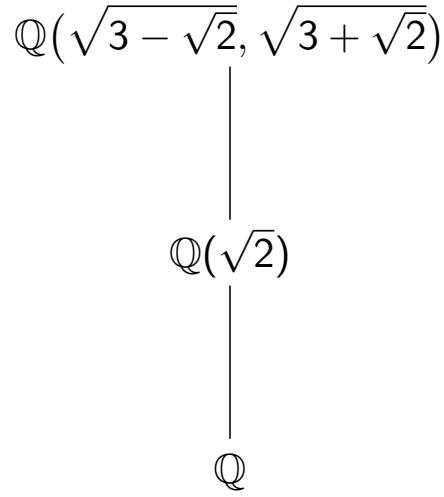


$G_1 \cong C_2$, and $G_2 \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$.
In general, $G_n \cong (\mathbb{Z}/2^{n+1}\mathbb{Z})^\times$, and $[\mathrm{Aut}(T_{2,n}) : G_n] \to \infty$.

A More Complicated/Typical Example

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



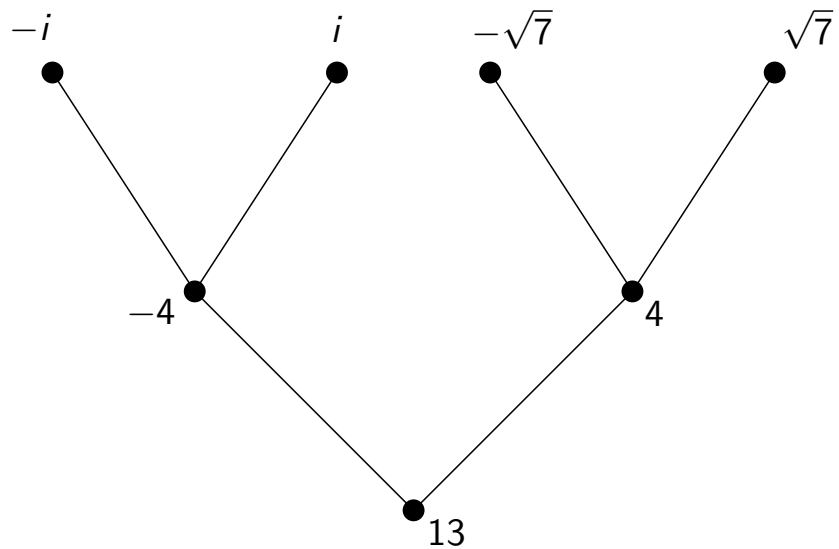


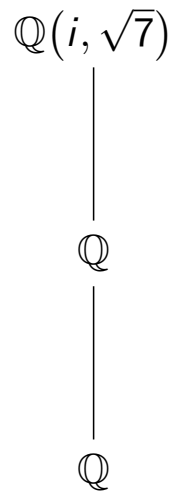
$G_1 \cong C_2$, and $G_2 \cong \mathrm{Aut}(T_{2,2}) \cong D_4$.
In general, $G_n \cong \mathrm{Aut}(T_{2,n})$ consists of all automorphisms of the n-level tree, for all $n \geq 1$.

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 $x_0 = 13$.

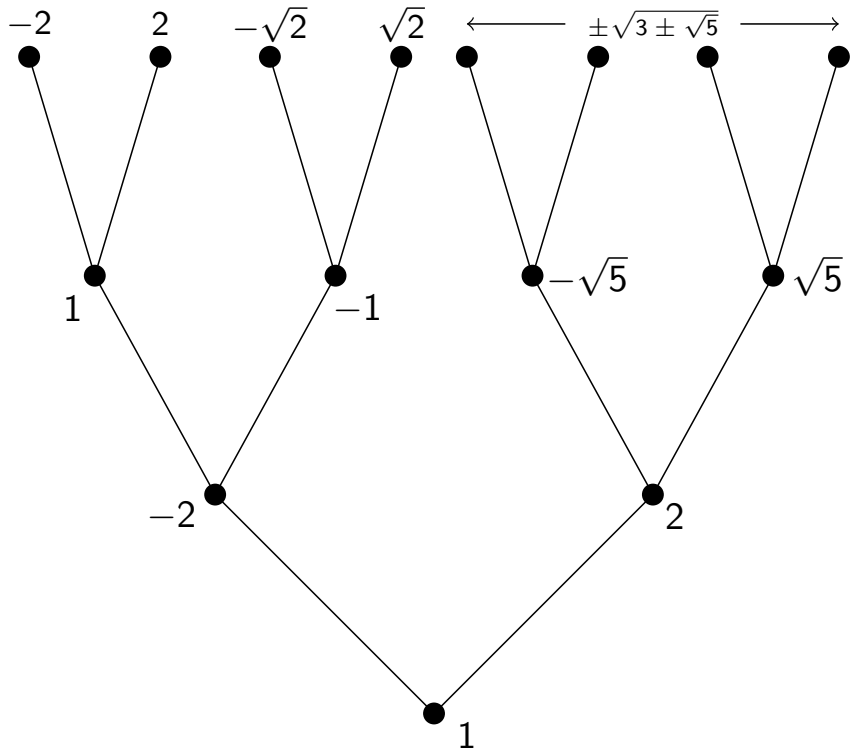


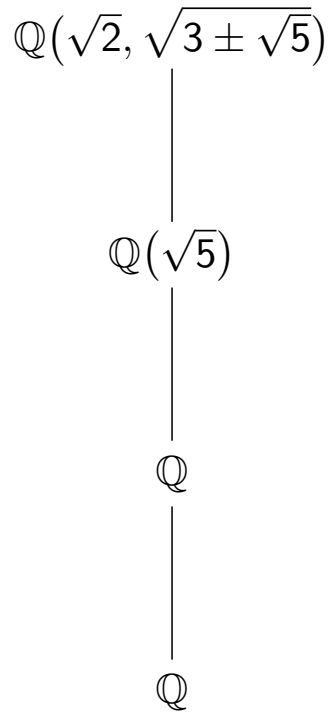


$G_1 \cong \{1\}$, and $G_2 \cong C_2 \times C_2$, so $[\mathrm{Aut}(T_{2,2}) : G_2] = 2$
But after that, the Galois group grows as much as possible:
$[\mathrm{Aut}(T_{2,n}) : G_n] = 2$. (I think!)

Even Smaller

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

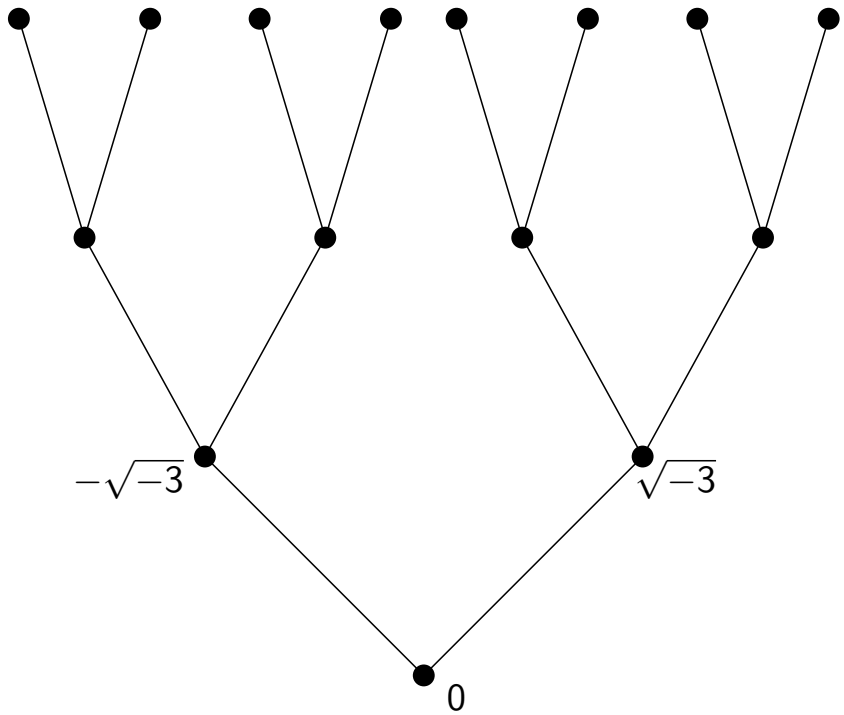


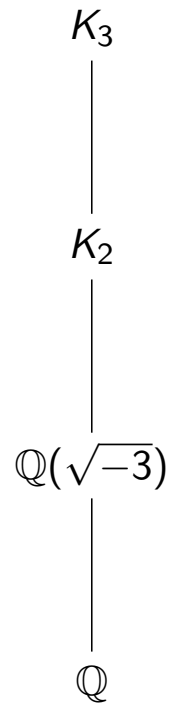


$G_1 \cong \{1\}$, and $G_2 \cong C_2$, so $[\mathrm{Aut}(T_{2,2}) : G_2] = 4$.
After that, $[\mathrm{Aut}(T_{2,n}) : G_n] \to \infty$. The issue: $x_0 = 1$ is periodic.

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

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

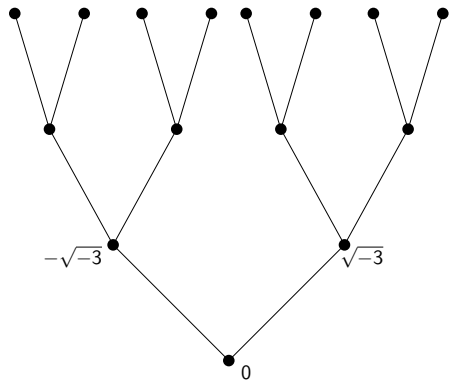
where the product is over all critical points γ of f.

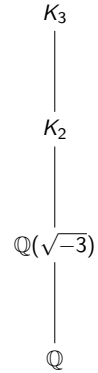
(E.g. Aitken-Hajir-Maire 2005; Jones-Manes 2012)

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

Attaining $G_n = \mathrm{Aut}(T_{d,n})$

Theorem (Odoni, 1985)

The generic polynomial $f \in K[z]$ (where $K = \mathbb{C}(x_0, a_0, \ldots, a_d)$) of degree d has $G_n = \mathrm{Aut}(T_{d,n})$ for all $n \geq 1$.

Theorem (Odoni, 1985; Stoll, 1992; Jones 2008)

For $K = \mathbb{Q}$, there are many quadratic polynomials $f \in \mathbb{Q}[z]$ and root points x_0 for which $G_n = \mathrm{Aut}(T_{2,n})$ for all $n \geq 1$.

Sketch of Proof (quadratic cases).

Step 1. Prove that each discriminant $\Delta_n = \Delta(f^n(z) - x_0)$ has a new prime factor, to an odd power. Thus, $\boxed{\sqrt{\Delta_n} \notin K_{n-1}}$

Step 2. Do some group theory: If G_{n-1} is transitive at level $n-1$ and if there is at least one odd $\sigma \in \mathrm{Gal}(K_n/K_{n-1})$, then $\mathrm{Gal}(K_n/K_{n-1}) \cong C_2^{2^{n-1}}$, i.e., it's as big as possible.

Attaining $G_n = \mathrm{Aut}(T_{d,n})$ for $d \geq 3$

Theorem (Looper, 2016 (appeared 2018))

Let $d \geq 3$ be prime. Then there are polynomials $f \in \mathbb{Q}[z]$ of degree d and root point $x_0 \in \mathbb{Q}$ such that $G_n = \mathrm{Aut}(T_{d,n})$ for all $n \geq 1$.

Theorem (2018: RB-Juul (2019); Kadets (2020); Specter)

Let $d \geq 3$. Then there are polynomials $f \in \mathbb{Q}[z]$ of degree d and root point $x_0 \in \mathbb{Q}$ such that $G_n = \mathrm{Aut}(T_{d,n})$ for all $n \geq 1$.

Sketch of Proof. Use $f(z) = z^d + cz^m$, for strategically chosen $c, x_0 \in \mathbb{Q}$ and $m \in \{1, \ldots, d-1\}$.

1. Use one prime p_1 to guarantee $f^n - x_0$ irreducible for all n. (Eisenstein's criterion.)

2. Use another prime p_2 to guarantee $\mathrm{Gal}(K_n/K_{n-1})$ contains a transposition for all n.

[3. Use a third prime p_3 to guarantee $\mathrm{Gal}(K_n/K_{n-1})$ contains an ℓ-cycle, for some $3 \leq \ell \leq d-1$ relatively prime to d.]

Now apply group theory and induction.

Postcritically Finite Maps

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 $n \to \infty$,
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 γ 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 $n \geq N$.

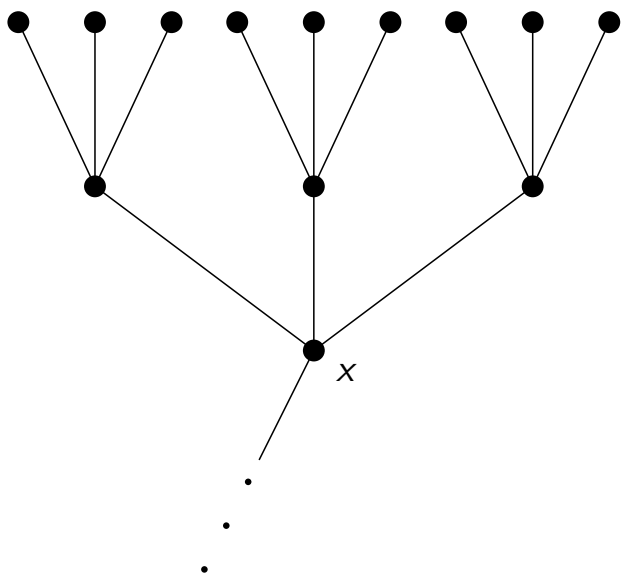
A PCF Cubic Polynomial

Let $f(z) = -2z^3 + 3z^2$. The critical points are $0, 1, \infty$.
All three are fixed, so certainly f is PCF.

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

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

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



$K(f^{-2}(x)) \subseteq K_{n+2}$

$K(f^{-1}(x)) \subseteq K_{n+1}$

$K(x) \subseteq K_n$

The PCF Cubic $f(z) = -2z^3 + 3z^2$, continued

Let E_n be the subgroup of $\mathrm{Aut}(T_{3,n})$ carved out by acting evenly on each such block of 9 nodes. One can show

$$[\mathrm{Aut}(T_{3,n}) : E_n] = \frac{|\mathrm{Aut}(T_{3,n})|}{|E_n|} = \frac{6^{(3^n-1)/2}}{2^{3^{n-1}} \cdot 3^{(3^n-1)/2}} = 2^{(3^{n-1}-1)/2}$$

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

Let $x_0 \in K = \mathbb{Q}$, and $f(z) = -2z^3 + 3z^2 \in \mathbb{Q}[z]$. Suppose that

- $v_3(x_0) = 1$, *and*
- **either** $v_2(x_0) = \pm 1$ **or** $v_2(1 - x_0) = 1$.

Then $G_n \cong E_n$ for all $n \geq 1$.

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

Note: An analogous statement is true over any number field K.

A PCF quadratic polynomial

$f(z) = z^2 - 1$ is PCF, with ∞ fixed and $0 \mapsto -1 \mapsto 0$.

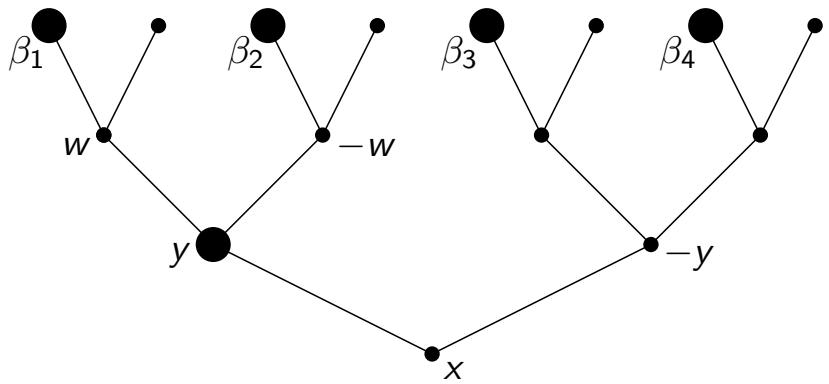
Pink (2013, unpublished):

- Assumes K is a function field, e.g. $K = \mathbb{C}(t)$ or $K = \mathbb{Q}(t)$
- Describes the associated group $M_n \subsetneq \mathrm{Aut}(T_{2,n})$ via (recursively defined) generators.
- Shows that the field K_{2n-1} necessarily contains ζ_{2^n}

But it turns out these two properties are directly connected via more elementary means.

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

For any $x \in \overline{K}$, consider $f^{-3}(x)$:



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

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

So K_3 contains $\sqrt{-1} = \zeta_4$, and for $n \geq 4$, any $\sigma \in G_n$ has to act the same on ζ_4 for *every* $T_{2,3}$ subtree of $T_{2,n}$.

$f(z) = z^2 - 1$, continued

Previous slide: $\sigma \in G_n$ must act the same on ζ_4 for *every* $T_{2,3}$ subtree of $T_{2,n}$.

But then there is *another* relation on $f^{-5}(x)$ yielding ζ_8, and $\sigma \in G_n$ must act the same on ζ_8 for every $T_{2,5}$ subtree of T_n.

Similarly for T_7 and ζ_{16}, and in general for $T_{2,2n-1}$ 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
$\lvert\mathrm{Aut}(T_{2,n})\rvert$	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}

Main Arboreal Galois Theorem for $f(z) = z^2 - 1$

Let M_n be the subgroup of $\mathrm{Aut}(T_{2,n})$ carved out by the ζ_{2^n} restrictions described on the preceding slides.

Theorem (Ahmad, RB, Cain, Carroll, Fang; 2020 (2017 REU))

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

1. *G_n is isomorphic to a subgroup of M_n for all n, and*
2. *if $\left[K_0\left(\sqrt{x_0}, \sqrt{x_0+1}, \zeta_8\right) : K_0\right] = 16$, then $G_n \cong M_n$ for all 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 $[K_5 : K] = |M_5|$, i.e., that $G_5 \cong M_5$.

Also Note: As before, an analogous statement is true over any number field K.

Colliding Critical Points

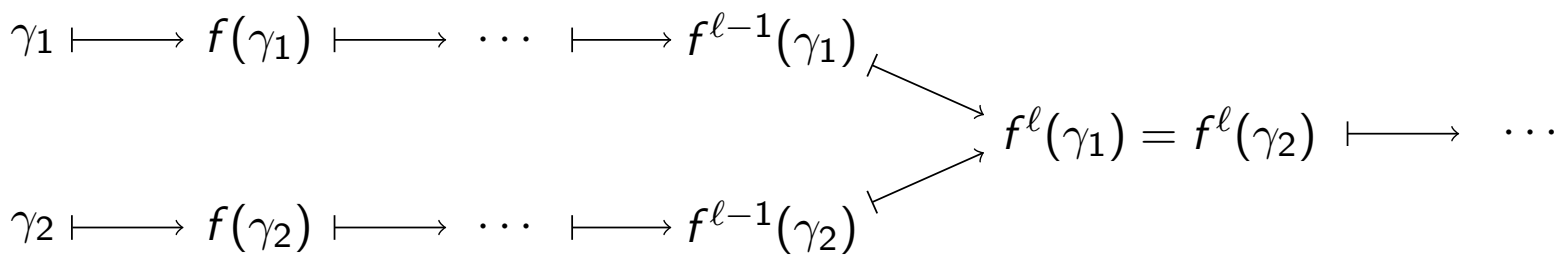
Another "obvious" reason $[\mathrm{Aut}(T_{d,n}) : G_n]$ could be unbounded:

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.

Summary: Maps with 2 critical points colliding at iterate ℓ

Quadratic Rational (with Anna Dietrich):

- Description of group $M_{\ell,n} \subseteq \mathrm{Aut}(T_{2,n})$ with $G_n \subseteq M_{\ell,n}$ for all $n \geq 1$.
- Sufficient condition to force $G_n = M_{\ell,n}$ for all $n \geq 1$. (Infinitely many "κ_n is not a square in K" conditions.)

Cubic Polynomial (with Will DeGroot, Xinyu Ni, Jesse Seid, Annie Wei, and Samantha (Min) Winton):

- Description of group $Q_{\ell,n} \subseteq \mathrm{Aut}(T_{3,n})$ with $G_n \subseteq Q_{\ell,n}$ for all $n \geq 1$.
- Sufficient condition to force $G_n = Q_{\ell,n}$ for all $n \geq 1$. (Infinitely many "μ_n is not a square in K" conditions.)

Thank you!!