(8/3/2021)

# Arboreal Galois representations

(with Irene Bouw & Özlem Ejder)

## § Motivation: dynamical sequences

**Question** Let $(a_n)_{n\geq 1}$ s.t. $a_n = f(a_{n-1})$.
What is the density of
$\mathcal{P} := \{p \in \mathbb{Q} \text{ prime} : p \text{ divides at least one nonzero term of } (a_n)_n\}$ ?

1970's: $f$ linear (Laxton, vld Poorten, Stephens, Ward...)

**Example** [Laxton-Stephens] $w_{n+2} = (a+1)w_{n+1} - aw_n$, $(\pm 1 \neq) a \in \mathbb{Z}$.
Then the density of $\mathcal{P}$ is $\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} e_p(a)/(p-1)$
order of $a$ mod $p$

$\exists$ more explicit formulas assuming GRH

1980's: $\deg(f)\geq 2$, $f(x)\in\mathbb{Z}[x]$, $a_1\in\mathbb{Z}$ (Odoni)

**Example** $a_1 = 2$, $a_{n+1} = 1 + a_1 a_2 \dots a_n$ (Euclid's theorem!)
$b_1 = a_1$, $b_n = a_1 a_2 \dots a_n$
Then $b_{n+1} = b_n^2 + b_n$
and $a_{n+1} = 1 + b_n = 1 + b_{n-1}^2 + b_{n-1} = 1 + (a_n - 1)^2 + (a_n - 1)$
$= a_n^2 - a_n + 1 = f(a_n)$ for $f(x) = x^2 - x + 1 \in \mathbb{Z}[x]$

**Notation** Write $f^n = f\circ \dots \circ f$ for the $n^{th}$ iterate of $f$.

Note: $\delta(\{p\in\mathbb{Q} \text{ prime} : a_i \equiv a \pmod p \text{ for some } i\geq 1\}) \leq$
$\delta(\{p\in\mathbb{Q} \text{ prime} : a_i \not\equiv a \pmod p \text{ for } i\leq n-1 \text{ and } f^n(x) - a \text{ has a root mod } p\})$

# § Dynamical Belyi maps

Let $X$ be an algebraic curve over $\mathbb{C}$.

A Belyi map is a finite cover $f: X \to \mathbb{P}^1_{\mathbb{C}}$ branched exactly over $\{0,1,\infty\}$.

Belyi's theorem: $X$ is defined over $\overline{\mathbb{Q}}$ $\Leftrightarrow$ $\exists$ Belyi map $f: X \to \mathbb{P}^1_{\mathbb{C}}$

Example: $X = \mathbb{P}^1_{\mathbb{C}}$ and $f(x) = -2x^3 + 3x^2$

We consider dynamical Belyi maps, where

- $X = \mathbb{P}^1_{\mathbb{C}}$ (genus 0)
- $\exists!$ ramification point above each branch point (single-cycle)
- $f(0) = 0$, $f(1) = 1$, $f(\infty) = \infty$ (normalised)

Combinatorial type $(d; e_1, e_2, e_3)$

degree: $d$; ramification indices above $0, 1, \infty$: $2 \leq e_1 \leq e_2 \leq e_3$

Riemann-Hurwitz: $e_1 + e_2 + e_3 = 2d + 1$

Example: $f(x) = -2x^3 + 3x^2$ has type $(3; 2, 2, 3)$.

Fact: For any type $(d; e_1, e_2, e_3)$ with $e_1 + e_2 + e_3 = 2d + 1$
$\exists$ a corresponding Belyi map,
which is defined over $\mathbb{Q}$!

We consider the following Galois groups:

1. $f^n : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}} \rightsquigarrow F_n / \mathbb{Q}(t) \rightsquigarrow G_{n,\mathbb{Q}} := \mathrm{Gal}(\widetilde{F_n}/\mathbb{Q}(t))$

2. $f^n : \mathbb{P}^1_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}} \rightsquigarrow G_{n,\bar{\mathbb{Q}}} := \mathrm{Gal}(\widetilde{(F_n \otimes_{\mathbb{Q}} \bar{\mathbb{Q}})} / \bar{\mathbb{Q}}(t))$

3. Choose $a \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0,1,\infty\}$ s.t. numerator of $f^n - a$ is irreducible $\forall n$. Let $K_{n,a}$ be the extension of $K_{0,a} := \mathbb{Q}$ obtained by adjoining a root of the numerator of $f^n - a$.
$\rightsquigarrow G_{n,a} := \mathrm{Gal}(\widetilde{K_{n,a}} / \mathbb{Q})$.

$\boxed{\text{Goal}}$ Determine and relate these groups.

$$\begin{array}{ccc} & G_{n,\mathbb{Q}} & \\ \rotatebox{45}{$\subseteq$} & & \rotatebox{-45}{$\supseteq$} \\ G_{n,\bar{\mathbb{Q}}} & & G_{n,a} \end{array}$$

First observations:

1. $G_{n,\bar{\mathbb{Q}}} \subseteq G_{n,\mathbb{Q}}$
   descent: $=$ holds. (can fail already at $n=1$)

2. $K_{n,a} \otimes_{\mathbb{Q}} \mathbb{Q}(t) \simeq F_n \Rightarrow G_{n,a} \subseteq G_{n,\mathbb{Q}}$
   Hilbert irreducibility theorem: "$=$" holds for $a$ in nonempty Zariski open $\subseteq \mathbb{P}^1(\mathbb{Q})$;
   we will give explicit conditions on $a$.

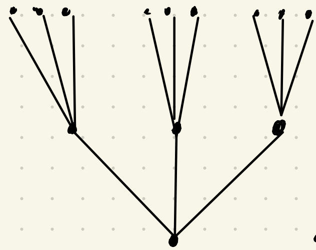
$\boxed{\text{Idea}}$ Embed all Galois groups into automorphism groups of trees.

# § Arboreal representations

Fix $d \geq 2$. For $n \geq 1$, let $T_n :=$ regular $d$-ary rooted tree of level $n$,

$$T_\infty := \varprojlim T_n$$

Example $d=3$, $n=2$




$\exists\, d^n$ leaves $\Rightarrow \mathrm{Aut}(T_n) \hookrightarrow S_{d^n}$

In fact, $\mathrm{Aut}(T_n) \simeq \mathrm{Aut}(T_{n-1}) \wr \mathrm{Aut}(T_1) \simeq \mathrm{Aut}(T_{n-1}) \wr S_d$

write $(\underline{\sigma}, \tau) = ((\sigma_1, \ldots, \sigma_d), \tau) \in \mathrm{Aut}(T_n)$

Picking $t$ (or $a$) as root and its preimages under $f$ as nodes $\rightsquigarrow$

---

Arboreal Galois representation $G_{n,a} \hookrightarrow \mathrm{Aut}(T_n)$

$G_{\infty,a} \hookrightarrow \mathrm{Aut}(T_\infty)$

---

Questions: What is the image? What is $[\mathrm{Aut}(T_\infty) : G_{\infty,a}]$?

E.g. for $f(x) = x^2 - x + 1$, $G_{\infty,2} \simeq \mathrm{Aut}(T_\infty)$ surjective [Odoni]

Odoni's conjecture: $\forall d \geq 2$, $\exists$ monic polynomial $f \in K[x]$ of degree $d$ and $a \in F$ s.t. $G_{\infty,a} \simeq \mathrm{Aut}(T_\infty)$

$\Rightarrow$ True for number fields (Looper, Benedetto-Juul, Kadets, Specter '18) but not for every char 0 Hilbertian field (Dittmann-Kadets '20)

Finite index can be proven in special cases; for us the index is infinite ($2^{d^{n-1}+d^{n-2}+\ldots+d+1}$ at level $n$) since $f$ is postcritically finite.

# § The groups $G_{n,\bar{\mathbb{Q}}}$

Any $f$ of type $(d; e_1, e_2, e_3)$ has a generating system $(g_1, g_2, g_3)$ where $g_i \in S_d$ is an $e_i$-cycle, $g_1 g_2 g_3 = 1$, and $\langle g_1, g_2, g_3 \rangle$ acts transitively on $\{1, 2, \dots, d\}$

Then $G_{1,\bar{\mathbb{Q}}} \cong \langle g_1, g_2, g_3 \rangle$.

[Liu-Osserman]: $G_{1,\bar{\mathbb{Q}}} \simeq \begin{cases} S_d & \text{if one of the } e_i \text{ is even} \\ A_d & \text{otherwise} \end{cases}$

For $n \geq 2$, inductively define generating system $(g_{1,n}, g_{2,n}, g_{3,n})$ for $f^n$:

$$g_{1,n} = ((g_{1,n-1}, id, \dots, id), g_1)$$

$$g_{2,n} = ((id, \dots, id, \underset{\uparrow \text{ in position } (1)g_1}{g_{2,n-1}}, id, \dots, id), g_2)$$

$$g_{3,n} = ((id, \dots, id, \underset{\uparrow \text{ in position } (1)g_1 g_2}{g_{3,n-1}}, id, \dots, id), g_3)$$

Then $G_{n,\bar{\mathbb{Q}}} \simeq \langle g_{1,n}, g_{2,n}, g_{3,n} \rangle$

Theorem 1 (BEK) ① If $G_{1,\bar{\mathbb{Q}}} \simeq S_d$, then inductively

$$G_{n,\bar{\mathbb{Q}}} \simeq (G_{n-1,\bar{\mathbb{Q}}} \wr G_{1,\bar{\mathbb{Q}}}) \cap \ker(\mathrm{sgn}_2) \subseteq \mathrm{Aut}(T_n)$$

where $\mathrm{sgn}_2 : \mathrm{Aut}(T_n) \xrightarrow{\mathrm{proj}} \mathrm{Aut}(T_2) \longrightarrow \{\pm 1\}$

$$((\sigma_1, \dots, \sigma_d), \tau) \longmapsto \mathrm{sgn}(\tau) \cdot \prod_{i=1}^{d} \mathrm{sgn}(\sigma_i).$$

② If $G_{1,\bar{\mathbb{Q}}} \simeq A_d$, then $G_{n,\bar{\mathbb{Q}}} \simeq \wr^n A_d \subseteq \mathrm{Aut}(T_n)$ $\forall n \geq 2$.

Proof sketch:
- Check $\mathrm{sgn}_2(g_{i,2}) = 1$ $\forall i$
- Compare sizes (actually, indices in $\mathrm{Aut}(T_n)$) of LHS & RHS by describing explicit elements of $\ker(G_{n,\bar{\mathbb{Q}}} \xrightarrow{\mathrm{proj}} G_{n-1,\bar{\mathbb{Q}}})$.

# § Descent: $G_{n,\bar{\mathbb{Q}}} \overset{?}{=} G_{n,\mathbb{Q}}$

**Theorem 2 (BEK)** If
- $G_{1,\bar{\mathbb{Q}}} \simeq G_{1,\mathbb{Q}} \simeq Ad$, or
- $G_{1,\bar{\mathbb{Q}}} \simeq S_d$ and $d = \deg(f)$ is odd and $\begin{cases} f \text{ is polynomial, or} \\ \text{of type } (d;\, d-k, 2k+1, d-k), \end{cases}$

then $G_{n,\mathbb{Q}} \simeq G_{n,\bar{\mathbb{Q}}}$ $\forall n \geq 1$.

**Example** Descent holds for $f(x) = -2x^3 + 3x^2$.

**Proof sketch**
- By Thm 1: If $G_{1,\mathbb{Q}} \simeq G_{1,\bar{\mathbb{Q}}}$ and $G_{2,\mathbb{Q}} \simeq G_{2,\bar{\mathbb{Q}}}$, then $G_{n,\mathbb{Q}} \simeq G_{n,\bar{\mathbb{Q}}}$ $\forall n \geq 2$.

  ($G_{n,\mathbb{Q}}$ is either $G_{n-1,\mathbb{Q}} \wr G_{1,\mathbb{Q}}$ or $(G_{n-1,\mathbb{Q}} \wr G_{1,\mathbb{Q}}) \cap \ker(\mathrm{sgn}_2)$ and we distinguish these after projection to $G_{2,\mathbb{Q}}$.)
- "Modified discriminant": Write $f(x) = g(x)/h(x)$ and $g(x) - t h(x) = \ell \prod_i (x - t_i)$.

  Then $G_{2,\mathbb{Q}} \subseteq \ker(\mathrm{sgn}_2) \iff$

  $$\Delta(g(x) - th(x)) \prod_i \Delta(f(x) - t_i) = u(1-t)^{2(e_2-1)}\, t^{2(e_1-1)}$$

  is a square in $\mathbb{Q}(t)$.

## § Specialisation : when $G_{n,\bar{\mathbb{Q}}} \subseteq G_{n,a} \subseteq G_{n,\mathbb{Q}}$?

**Theorem 3 (BEK)** Choose $a \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0,1,\infty\}$ and distinct primes $p, q_1, q_2, q_3 \in \mathbb{Q}$ such that

$$(\dagger) \begin{cases} \text{a) } f(x) \equiv x^d \pmod p \\ \text{b) } f \text{ has good separable reduction at } q_1, q_2, q_3 \\ \text{c) } v_p(a) = 1,\ v_{q_1}(a) > 0,\ v_{q_2}(1-a) > 0,\ v_{q_3}(a) < 0 \end{cases}$$

Then $G_{n,\bar{\mathbb{Q}}} \subseteq G_{n,a}$ $\forall n \geq 2$

**Proof sketch** a) $\Rightarrow$ "$f^n - a$" irreducible $\forall n$, so $[K_{n,a} : \mathbb{Q}] = d^n$ $\forall n \geq 1$

so $G_{n,a} \subseteq S_{d^n}$ is transitive.

b) + c) $\Rightarrow$ Prescribe ramification in $K_{n,a}/K_{n-1,a}$ and construct elements of $G_{n,a}$ conjugate to $g_{i,n} \in G_{n,\bar{\mathbb{Q}}}$.

( $\forall n \geq 1$, $\exists!$ ramified prime $q_n$ in $K_{n,a}/K_{n-1,a}$ above $q_{n-1}$ with ramification index $e_i$, and all other primes above $q_{n-1}$ are unramified.

The elements we construct are generators of inertia groups of the $q_i$ in $G_{n,a}$, and therefore conjugate to $g_{i,n}$. )

**Corollary** If Theorems 2 & 3 hold, then

$$\boxed{G_{n,a} \simeq G_{n,\bar{\mathbb{Q}}} \simeq G_{n,\mathbb{Q}}} \quad \forall n \geq 1.$$

## § Application: dynamical sequences

$(a_n)_{n\geq 1}$, $a_n = f(a_{n-1})$.

Let $\mathcal{P} := \{p \in \mathbb{Q} \text{ prime}: p \text{ divides at least one nonzero term of } (a_n)_{n\geq 1}\}$

$Q := \{p \in \mathbb{Q} \text{ prime}: a_i \equiv a \pmod p \text{ for some } i \geq 1\}$

**Theorem 4 (BEK)** Let $f$ be a dynamical Belyi map, with splitting field $K$.
Let $a \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0,1,\infty\}$ such that

$$G_{n,a} = G_{n,\overline{\mathbb{Q}}} \simeq G_{n,\mathbb{Q}} \quad \forall n \geq 1.$$

Consider $(a_n)_{n\geq 1}$ with $a_1 = a$, $a_n = f(a_{n-1})$.

1. $\delta(Q) = 0$.
2. If $G_{n,b_j,K} \simeq G_{n,K} \simeq G_{n,\mathbb{Q}}$ for any nonzero preimage $b_j$ of zero under $f$, then $\delta(\mathcal{P}) = 0$.

Guaranteed by conditions analogous to $(+)$ for $b_j$ over $K$

**Proof sketch** 1. Čebotarev: $\delta(Q) \leq \dfrac{\#\{\text{elements of } G_{n,\overline{\mathbb{Q}}} \text{ fixing a leaf}\}}{\# G_{n,\overline{\mathbb{Q}}}}$

and RHS $\to 0$ as $n \to \infty$.

2. $\delta(\mathcal{P}) = \delta(\{p \in \mathbb{Q} \text{ prime}: \exists \mathfrak{p} \subseteq K \text{ above } p \text{ s.t. } a_i \equiv b_j \pmod{\mathfrak{p}} \text{ for some } i,j\})$
so argue as in 1.

THANK YOU FOR LISTENING!