Galois theory, dynamics, and combinatorics of Belyi maps

Valentijn Karemaker
(Utrecht University & Stockholm University)

Joint with I. Bouw and Ö. Ejder

Diamant symposium, De Bilt

November 29, 2019

Belyi maps

Let X be a compact connected Riemann surface, or equivalently (GAGA), an algebraic curve over $\mathbb{C}$.

Definition (Belyi map)

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

Belyi's theorem says X is defined over $\overline{\mathbb{Q}}$ if and only if there exists a Belyi map as above.

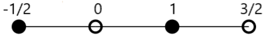
Example. Let $X = \mathbb{P}^1_{\mathbb{C}}$ and $f(x) = -2x^3 + 3x^2$.

Dessins d'enfant

A DESSIN D'ENFANT for a Belyi map is a finite bipartite graph where white (resp. black) vertices are the inverse images of 0 (resp. 1) and edges are inverse images of $(0, 1)$.
There are $\deg(f)$ edges.

A dessin d'enfant is a combinatorial representation of a Belyi map.

Example. For $f(x) = -2x^3 + 3x^2$, the dessin is



Generating systems and combinatorial types

A GENERATING SYSTEM of degree $d > 1$ is a triple $g = (g_1, g_2, g_3) \in S_d^3$ such that $g_1 g_2 g_3 = 1$ and such that $\langle g_1, g_2, g_3 \rangle$ acts transitively on $\{1, 2, \ldots, d\}$.
For a degree-d Belyi map f the g_i encode the ramification data (monodromy) above $\{0, 1, \infty\}$.

RIEMANN'S EXISTENCE THEOREM gives a bijection

$$\{\text{Generating systems}\}/\sim \qquad \longleftrightarrow \qquad \{\text{Belyi maps}\}/\simeq .$$

Let $C(g_i)$ be the conjugacy class of g_i in S_d.
The (COMBINATORIAL) TYPE of g is $(d; C(g_1), C(g_2), C(g_3))$.
When $C(g_i)$ is a single cycle of length e_i, write $C(g_i) = e_i$.

Example. For $f(x) = -2x^3 + 3x^2$, the type is $(3; 2, 2, 3)$.

Dynamical Belyi maps

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

Definition (Dynamical Belyi map)

A DYNAMICAL BELYI MAP is a Belyi map such that:

- $X = \mathbb{P}^1$ so $f : \mathbb{P}^1 \to \mathbb{P}^1$ ("genus zero");
- $C(g_i)$ is a single cycle of length e_i ("single cycle");
- $f(0) = 0$, $f(1) = 1$, $f(\infty) = \infty$ ("normalised").

The RIEMANN-HURWITZ FORMULA gives $2d + 1 = e_1 + e_2 + e_3$.
Fact: A dynamical Belyi map can be defined over $\mathbb{Q}$.

Why "dynamical"?

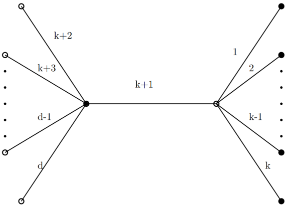
A dynamical Belyi map can be iterated and therefore exhibits dynamical behaviour. (More about that soon!)
Write $f^n = f \circ \ldots \circ f$ for the nth iterate of f, where $f^1 = f$.
Then f^n is again a dynamical Belyi map.

Examples of dynamical Belyi maps

Example. The map $f(x) = -2x^3 + 3x^2$ fits into a family of dynamical Belyi maps of type $(d; d-k, k+1, d)$ given by

$$f(x) = cx^{d-k}(a_0x^k + \ldots + a_{k-1}(x) + a_k),$$

with $a_i = \frac{(-1)^{k-i}}{d-i}\binom{k}{i}$ and $c = \frac{1}{k!}\prod_{j=0}^{k}(d-j)$.



(Dessins were worked out by Manes, Melamed, Tobin.)

Galois groups

Let f be a dynamical Belyi map.
It is defined over $\overline{\mathbb{Q}}$ (Belyi) and even $\mathbb{Q}$ (dynamical).

The cover $f^n : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ corresponds to a function field extension F_n over $F_0 = \mathbb{Q}(t)$. Define

$$G_{n,\mathbb{Q}} := \mathrm{Gal}(\widetilde{F_n}/\mathbb{Q}(t)).$$

Similarly, we define

$$G_{n,\overline{\mathbb{Q}}} := \mathrm{Gal}((\widetilde{F_n \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}})/\overline{\mathbb{Q}}(t)).$$

Finally, choose $a \in \mathbb{Q}$ s.t. (the numerator of) $f^n - a$ is irreducible for all n. Let $K_{n,a}$ be the extension of $K_{0,a} := \mathbb{Q}$ obtained by adjoining a root of (the numerator of) $f^n - a$, and define

$$G_{n,a} := \mathrm{Gal}(\widetilde{K_{n,a}}/\mathbb{Q}).$$

Galois groups

For a dynamical Belyi map f, we want to determine the groups

$$G_{n,\overline{\mathbb{Q}}}, \qquad G_{n,\mathbb{Q}}, \qquad G_{n,a}.$$

First observations:

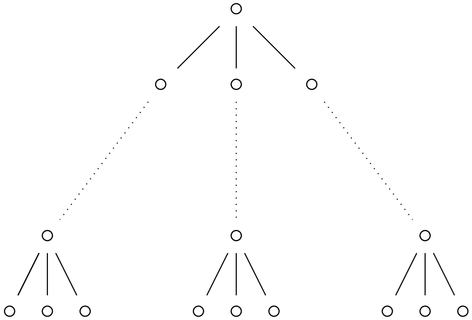
1. We have
$$G_{n,\overline{\mathbb{Q}}} \subseteq G_{n,\mathbb{Q}}.$$
When equality holds, we say the groups *descend*;
we will give sufficient conditions for descent.
2. Since $a \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$ is such that (the numerator of) $f^n - a$ is irreducible, then $K_{n,a} \otimes_{\mathbb{Q}} \mathbb{Q}(t) \simeq F_n$, inducing
$$G_{n,a} \subseteq G_{n,\mathbb{Q}}.$$

Arboreal representations

Idea

Embed all Galois groups into automorphism groups of trees.

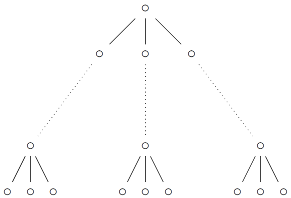
For $d \geq 2$ and $n \geq 1$, let T_n be the d-ary rooted tree of level n:



The outer nodes of T_n are the *leaves*. There are d^n leaves, so

$$\mathrm{Aut}(T_n) \hookrightarrow S_{d^n}.$$

Arboreal representations



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 our root and its preimages as the other nodes, we get the ARBOREAL GALOIS REPRESENTATION

$$G_{n,\mathbb{Q}} \hookrightarrow \mathrm{Aut}(T_n).$$

The groups $G_{n,\overline{\mathbb{Q}}}$

Idea

The groups $G_{n,\overline{\mathbb{Q}}} \subseteq \mathrm{Aut}(T_n)$ are completely (and combinatorially) determined by the generating system of f^n.

Recall: f has generating system $g = (g_1, g_2, g_3)$, where g_i are e_i-cycles in S_d s.t. $g_1 g_2 g_3 = 1$. May take:

$$\begin{aligned} g_1 &= (d, d-1, \dots, e_3, 1, 2, \dots, d-e_2); \\ g_2 &= (d-e_2+1, d-e_2+2, \dots, d); \\ g_3 &= (e_3, e_3-1, \dots, 2, 1). \end{aligned}$$

Then

$$G_{1,\overline{\mathbb{Q}}} = \langle g_1, g_2, g_3 \rangle \simeq \begin{cases} S_d & \text{if one of the } e_i \text{ is even;} \\ A_d & \text{otherwise.} \end{cases}$$

The groups $G_{n,\overline{\mathbb{Q}}}$

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

$$g_{1,n} = ((g_{1,n-1}, \mathrm{id}, \ldots, \mathrm{id}), g_1);$$
$$g_{2,n} = ((\mathrm{id}, \ldots, \mathrm{id}, g_{2,n-1}, \mathrm{id}, \ldots, \mathrm{id}), g_2);$$
$$g_{3,n} = ((\mathrm{id}, \ldots, \mathrm{id}, g_{3,n-1}, \mathrm{id}, \ldots, \mathrm{id}), g_3).$$

Then $G_{n,\overline{\mathbb{Q}}} = \langle g_{1,n}, g_{2,n}, g_{3,n} \rangle$, and

Theorem 1 (Bouw-Ejder-K.)

1. If $G_{1,\overline{\mathbb{Q}}} \simeq S_d$, then inductively
$$G_{n,\overline{\mathbb{Q}}} \simeq (G_{n-1} \wr G_1) \cap \ker(\mathrm{sgn}_2) \subseteq \mathrm{Aut}(T_n),$$
where $\mathrm{sgn}_2 : \mathrm{Aut}(T_n) \xrightarrow{\pi_2} \mathrm{Aut}(T_2) \to \{\pm 1\}$,
$$((\sigma_1, \ldots, \sigma_d), \tau) \mapsto \mathrm{sgn}(\tau) \prod \mathrm{sgn}(\sigma_i).$$
2. If $G_{1,\overline{\mathbb{Q}}} \simeq A_d$, then $G_{n,\overline{\mathbb{Q}}} \simeq \wr^n A_d \subseteq \mathrm{Aut}(T_n)$ for all $n \geq 2$.

Descent: when is $G_{n,\overline{\mathbb{Q}}} = G_{n,\mathbb{Q}}$?

Theorem 2 (Bouw-Ejder-K.)

If $G_{1,\overline{\mathbb{Q}}} = G_{1,\mathbb{Q}} \simeq A_d$, or if $G_{1,\overline{\mathbb{Q}}} \simeq S_d$ and f has odd degree and is either a polynomial or of type $(d; d-k, 2k+1, d-k)$, then $G_{n,\overline{\mathbb{Q}}} = G_{n,\mathbb{Q}}$ for all $n \geq 1$.

Proof

- By Theorem 1: if $G_{2,\overline{\mathbb{Q}}} = G_{2,\mathbb{Q}}$, then $G_{n,\overline{\mathbb{Q}}} \simeq G_{n,\mathbb{Q}}$, $\forall n \geq 2$.
- Write $f(x) = g(x)/h(x)$ and $g(x) - th(x) = \ell \prod_i (x - t_i)$. We have $G_{2,\mathbb{Q}} \subseteq \ker(\mathrm{sgn}_2)$ if and only if

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

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

Specialisation: when is $G_{n,\overline{\mathbb{Q}}} \subseteq G_{n,a}$?

(We have $G_{n,\overline{\mathbb{Q}}} \subseteq G_{n,\mathbb{Q}}$ and suppose that $G_{n,a} \subseteq G_{n,\mathbb{Q}}$.)

Theorem 3 (Bouw-Ejder-K.)

Choose $a \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$ and distinct primes p, q_1, q_2, q_3 s.t.:

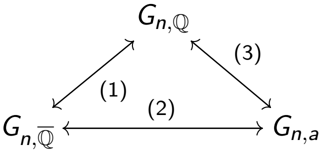
$$(\dagger) \begin{cases} f(x) \equiv x^d \pmod{p}; \\ f \text{ has good separable reduction modulo } q_1, q_2, q_3; \\ v_p(a) = 1 \text{ and } v_{q_1}(a) > 0, v_{q_2}(1-a) > 0, v_{q_3}(a) < 0. \end{cases}$$

Then $G_{n,\overline{\mathbb{Q}}} \subseteq G_{n,a}$ for all $n \geq 2$.

Proof

- Conditions at p: $G_{n,a}$ is a transitive subgroup of S_{d^n}.
- Conditions at q_1, q_2, q_3: prescribe the ramification in $K_{n,a}/K_{n-1,a}$ & construct elements of $G_{n,a}$ conjugate to the $g_{i,n} \in G_{n,\mathbb{Q}}$.

Summary of Galois groups



Theorem 1: We understand $G_{n,\overline{\mathbb{Q}}} = \langle g_{1,n}, g_{2,n}, g_{3,n} \rangle$.

(1): We have $G_{n,\overline{\mathbb{Q}}} \subseteq G_{n,\mathbb{Q}}$.
Theorem 2: This is an equality if $G_{1,\overline{\mathbb{Q}}} = G_{1,\mathbb{Q}}$ and $G_{2,\overline{\mathbb{Q}}} = G_{2,\mathbb{Q}}$.

(2): Theorem 3: We have $G_{n,\overline{\mathbb{Q}}} \subseteq G_{n,a}$ when conditions (†) hold.

(3): We have $G_{n,a} \subseteq G_{n,\mathbb{Q}}$ if "$f^n - a$" is irreducible.

Conclusion: If all these conditions hold, all groups are equal!

Dynamical system

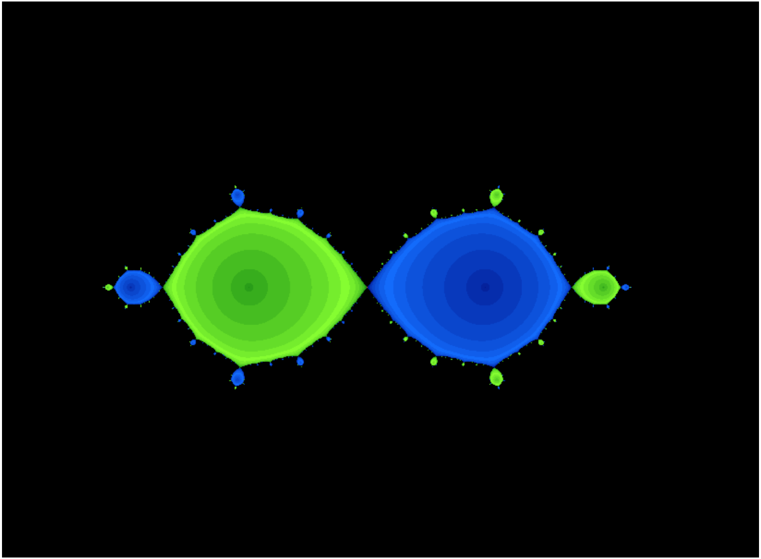
A dynamical Belyi map $f : \mathbb{P}^1 \to \mathbb{P}^1$ yields a DYNAMICAL SYSTEM

$$(f, \mathbb{P}^1).$$

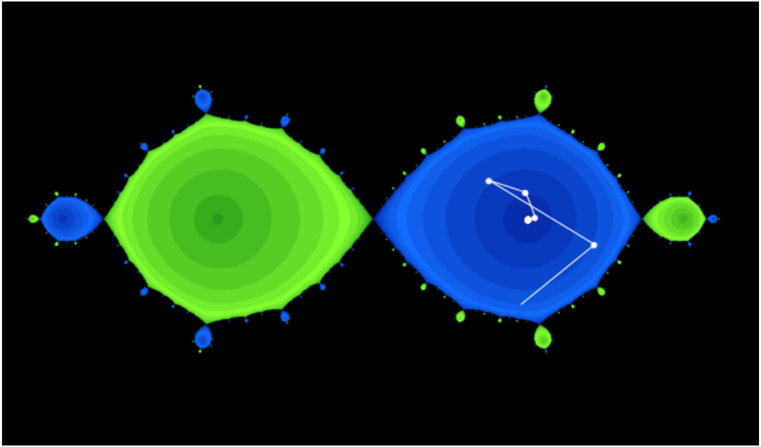
Considering $f : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$, we can study this dynamical system by computing its JULIA SET, i.e., the set

$$\{z \in \mathbb{C} : f^n(z) \not\to \infty \text{ as } n \to \infty\}.$$

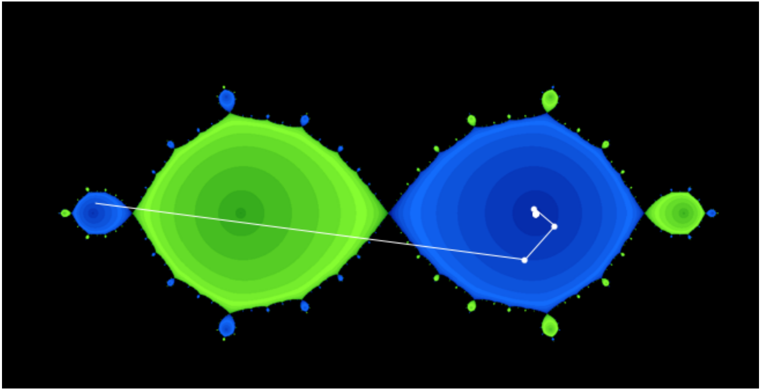
Belyi map of combinatorial type (3; 2, 2, 3)



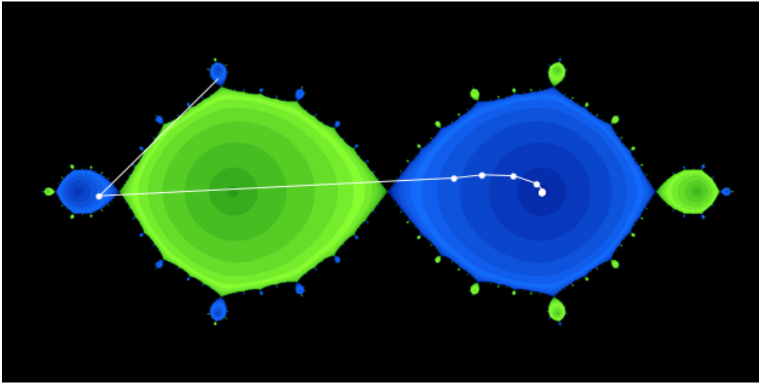
Belyi map of combinatorial type (3; 2, 2, 3)



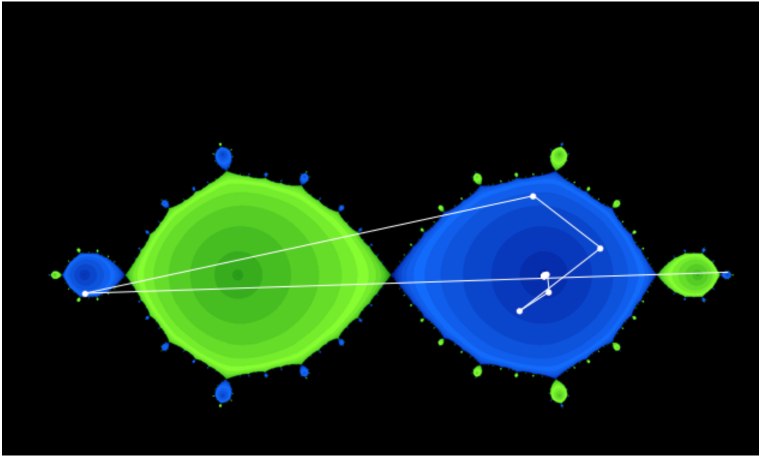
Belyi map of combinatorial type (3; 2, 2, 3)



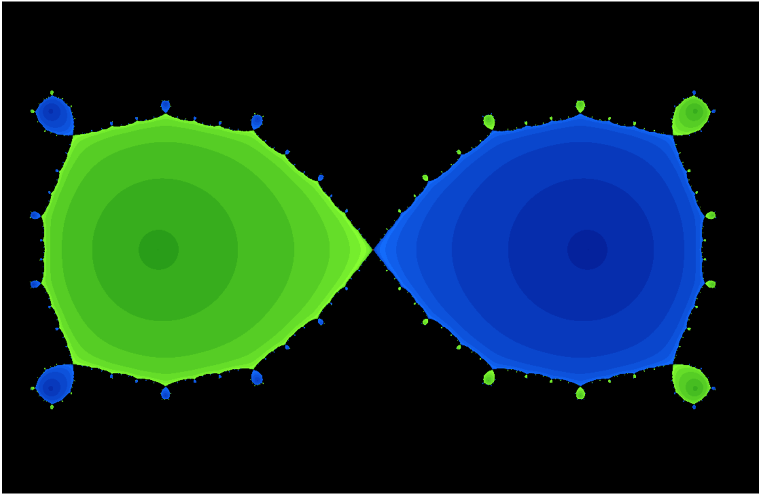
Belyi map of combinatorial type (3; 2, 2, 3)



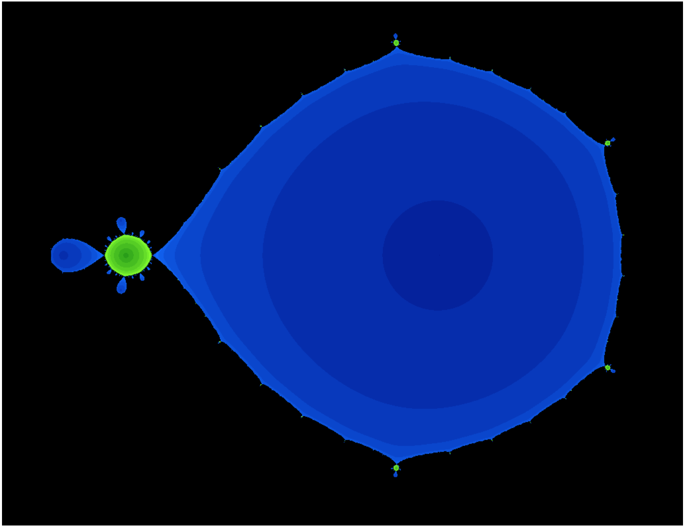
Belyi map of combinatorial type (3; 2, 2, 3)



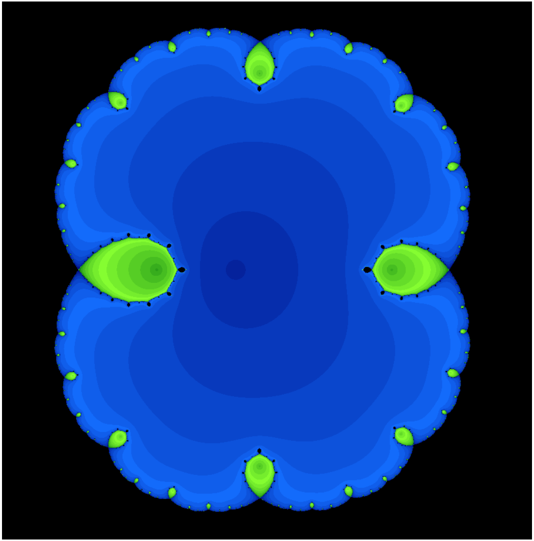
Belyi map of combinatorial type (5; 3, 3, 5)



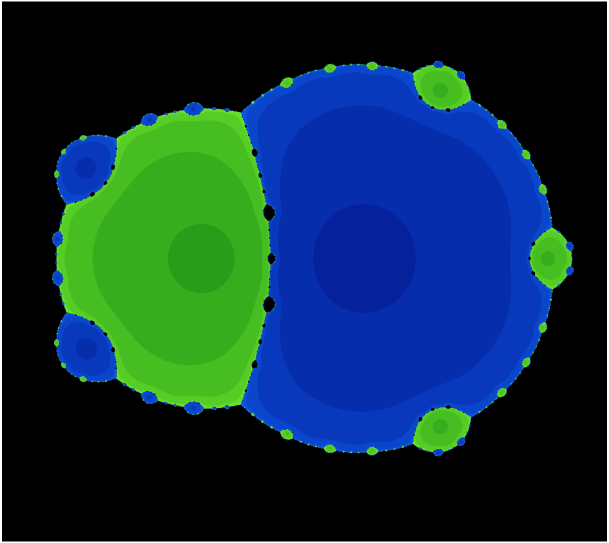
Belyi map of combinatorial type (6; 2, 5, 6)



Belyi map of combinatorial type (3; 2, 3, 2)



Belyi map of combinatorial type (9; 6, 7, 6)



Orbits

For $x \in \mathbb{P}^1$, we may form the DYNAMICAL SEQUENCE $(a_n)_{n\geq 1}$ where $a_1 = x$ and $a_{n+1} = f(a_n)$ for $n \geq 2$.
This is also called the ORBIT of x.

Classification of orbits:

- If $f^n(x) = x$ for some $n \geq 1$, then x is PERIODIC;
- If $f^m(x)$ is periodic for some $m \geq 1$, then x is PREPERIODIC;
- Otherwise, x is a WANDERING POINT.

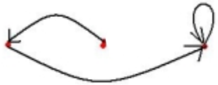


Figure: A preperiodic point.

Want to describe the (pre)periodic points of dynamical Belyi maps.

Preperiodic points

Theorem (Silverman)

Let $f : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map of degree d over a local field K. Assume f has good reduction at p and let P be a periodic point of f of period n. Then $\overline{P}$ is a periodic point of $\overline{f}$ of period m say.
Let $r = |(\overline{f}^n)'(\overline{P})|$. Then

$$n = m; \qquad \text{or} \qquad n = mr; \qquad \text{or} \qquad n = mrp^e, e \in \mathbb{Z}_{>0}.$$

Theorem 4 (Anderson-Bouw-Ejder-Girgin-K.-Manes)

Let f be a dynamical Belyi map over $\mathbb{Q}$ of type $(d = p^\ell d', e_1, e_2, e_3)$.
Then $f \equiv x^d \pmod{p}$ if and only if $e_2 \leq p^\ell$.

Theorem 5 (Anderson-Bouw-Ejder-Girgin-K.-Manes)

Let f be a dynamical Belyi map over $\mathbb{Q}$ of type (d, e_1, e_2, e_3) such that $e_2 \leq p^\ell$ and either $2^\ell | d$ or $3^\ell | d$ or $d = p^\ell$. Then the rational preperiodic points of f are all rational fixed points of f and their preimages.

Preperiodic points

Theorem 5 (Anderson-Bouw-Ejder-Girgin-K.-Manes)

Let f be a dynamical Belyi map over $\mathbb{Q}$ of type (d, e_1, e_2, e_3) such that $e_2 \leq p^\ell$ and either $2^\ell | d$ or $3^\ell | d$ or $d = p^\ell$. Then the rational preperiodic points of f are all rational fixed points of f and their preimages.

Example. For $f(x) = -2x^3 + 3x^2$ of type $(3; 2, 2, 3)$ we find

Rational periodic points	$\mathrm{Per}(f) = \{0, \frac{1}{2}, 1, \infty\}$;
Rational preperiodic points	$\mathrm{PrePer}(f) = \{-\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, \infty\}$.

Dynamical sequences

Let $(a_n)_{n\geq 1}$ be a dynamical sequence for a map f.
We want to know the density δ of each of the sets

$$\mathcal{Q} := \{p \text{ prime } : a_i \equiv a \pmod{p} \text{ for some } i \geq 0\};$$
$$\mathcal{P} := \{p \text{ prime } : p \text{ divides at least one non-zero term of } (a_n)_{n\geq 1}\}.$$

We see that $\delta(Q) \leq$

$$\delta(\{p : a_i \not\equiv a \pmod{p} \text{ for } i \leq n-1 \text{ and } f^n - a \text{ has a root mod } p\}).$$

Chebotarev density theorem:

$$= \frac{1}{|G_{n,a}|} |\{ \text{ elements of } G_{n,a} \subseteq \mathrm{Aut}(T_n) \text{ fixing a leaf } \}|.$$

Dynamical sequences

$$\mathcal{Q} := \{p \text{ prime } : a_i \equiv a \pmod{p} \text{ for some } i \geq 0\};$$
$$\mathcal{P} := \{p \text{ prime } : p \text{ divides at least one non-zero term of } (a_n)_{n\geq 1}\}.$$

Theorem 6 (Bouw-Ejder-K.)

Let f be a dynamical Belyi map with splitting field K and let $a \in \mathbb{P}^1(\mathbb{Q}) \setminus \{0, 1, \infty\}$ such that $G_{n,a} \simeq G_{n,\mathbb{Q}} \simeq G_{n,\overline{\mathbb{Q}}}$ for all $n \geq 1$. Consider $(a_n)_{n\geq 1}$ with $a_1 = a$.

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

Proof

1. $\{$ elements of $G_{n,\overline{\mathbb{Q}}}$ fixing a leaf $\}|/|G_{n,\overline{\mathbb{Q}}}| \to 0$ as $n \to \infty$.
2. $\delta(\mathcal{P}) = \delta(\{p : \exists \mathfrak{p} \mid p \text{ s.t. } a_i \equiv b_j \pmod{\mathfrak{p}} \text{ for some } i, j\})$.