Monodromy groups of rational functions, related group theoretic questions and computation of interesting rational functions

Peter Müller

Erlangen, 15 July 2016

Maximal decompositions

$$f(z) = f_1(f_2(\ldots(f_m(z))\ldots))$$

of polynomials and rational functions (Ritt 1922)

Maximal decompositions

$$f(z) = f_1(f_2(\ldots(f_m(z))\ldots))$$

of polynomials and rational functions (Ritt 1922)

Reducibility of variable-separated algebraic curves f(X) - g(Y) = 0 (Cassels, Birch, Lewis, Davenport 1970)

Maximal decompositions

$$f(z) = f_1(f_2(\ldots(f_m(z))\ldots))$$

of polynomials and rational functions (Ritt 1922)

- Reducibility of variable-separated algebraic curves f(X) g(Y) = 0 (Cassels, Birch, Lewis, Davenport 1970)
- ▶ Value sets of "generic" polynomials $f(z) \in \mathbb{F}_q[z]$:

$$\frac{1}{q}|f(\mathbb{F}_q)| = 1 - \frac{1}{2!} + \frac{1}{3!} - \dots - (-1)^n \frac{1}{n!} + O_n(q^{-1/2}),$$
 $n = \deg f \ (Birch, \ Swinnerton-Dyer \ 1959, \ Cohen \ 1970)$

Maximal decompositions

$$f(z) = f_1(f_2(\ldots(f_m(z))\ldots))$$

of polynomials and rational functions (Ritt 1922)

- Reducibility of variable-separated algebraic curves f(X) g(Y) = 0 (Cassels, Birch, Lewis, Davenport 1970)
- ▶ Value sets of "generic" polynomials $f(z) \in \mathbb{F}_q[z]$:

$$\frac{1}{q}|f(\mathbb{F}_q)| = 1 - \frac{1}{2!} + \frac{1}{3!} - \dots - (-1)^n \frac{1}{n!} + O_n(q^{-1/2}),$$
 $n = \deg f \text{ (Birch, Swinnerton-Dyer 1959, Cohen 1970)}$

Around Hilbert's Irreducibility Theorem: $f(t,X) \in \mathbb{Q}(t)[X]$, $G = \operatorname{Gal}(f(t,X)/\mathbb{Q}(t))$ simple, $\neq C_2, A_n$. Then $\operatorname{Gal}(f(\tau,X)/\mathbb{Q}) = G$ for all but finitely many $\tau \in \mathbb{Z}$. (Müller 2000)

▶ $\Gamma \subset \mathbb{C}$ curve with $h(\Gamma) \subseteq \Gamma$ for $h \in \mathbb{C}(z)$

- ▶ $\Gamma \subset \mathbb{C}$ curve with $h(\Gamma) \subseteq \Gamma$ for $h \in \mathbb{C}(z)$
- lacksquare Boring examples: $\Gamma=\mathbb{R}$ and $h\in\mathbb{R}(z)$

- ▶ $\Gamma \subset \mathbb{C}$ curve with $h(\Gamma) \subseteq \Gamma$ for $h \in \mathbb{C}(z)$
- lacksquare Boring examples: $\Gamma=\mathbb{R}$ and $h\in\mathbb{R}(z)$, or $\Gamma\subseteq$ circle

- ▶ $\Gamma \subset \mathbb{C}$ curve with $h(\Gamma) \subseteq \Gamma$ for $h \in \mathbb{C}(z)$
- ▶ Boring examples: $\Gamma = \mathbb{R}$ and $h \in \mathbb{R}(z)$, or $\Gamma \subseteq$ circle
- ▶ Better examples: $f, g \in \mathbb{C}(z)$, $\Gamma = g(\mathbb{R}) \not\subset$ circle, $f \circ g \in \mathbb{R}(z)$, $h = g \circ f$:

$$h(\Gamma) = (g \circ f)(\Gamma) = g(f(g(\mathbb{R}))) \subseteq g(\mathbb{R}) = \Gamma$$

- ▶ $\Gamma \subset \mathbb{C}$ curve with $h(\Gamma) \subseteq \Gamma$ for $h \in \mathbb{C}(z)$
- ▶ Boring examples: $\Gamma = \mathbb{R}$ and $h \in \mathbb{R}(z)$, or $\Gamma \subseteq$ circle
- ▶ Better examples: $f,g \in \mathbb{C}(z)$, $\Gamma = g(\mathbb{R}) \not\subset$ circle, $f \circ g \in \mathbb{R}(z)$, $h = g \circ f$:

$$h(\Gamma) = (g \circ f)(\Gamma) = g(f(g(\mathbb{R}))) \subseteq g(\mathbb{R}) = \Gamma$$

Can Γ be a Jordan curve? (Eremenko 2012)

- ▶ $\Gamma \subset \mathbb{C}$ curve with $h(\Gamma) \subseteq \Gamma$ for $h \in \mathbb{C}(z)$
- ▶ Boring examples: $\Gamma = \mathbb{R}$ and $h \in \mathbb{R}(z)$, or $\Gamma \subseteq$ circle
- ▶ Better examples: $f,g \in \mathbb{C}(z)$, $\Gamma = g(\mathbb{R}) \not\subset$ circle, $f \circ g \in \mathbb{R}(z)$, $h = g \circ f$:

$$h(\Gamma) = (g \circ f)(\Gamma) = g(f(g(\mathbb{R}))) \subseteq g(\mathbb{R}) = \Gamma$$

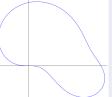
Can Γ be a Jordan curve? (Eremenko 2012), Yes (Müller 2015):

$$\omega = e^{2\pi i/3}$$

$$f(z) = \frac{(6\omega + 5)z^3 + (-6\omega - 3)z^2 - 3z + 1}{4z^3 - 6z^2 + 3z}$$

$$g(z) = \frac{z^2 - \omega}{2z^3 + z^2 + (\omega + 1)z - \omega}$$

$$f(g(z)) = \frac{64z^9 - 192z^5 - 104z^3 - 48z}{96z^8 + 104z^6 + 96z^4 - 8}$$



- ▶ $\Gamma \subset \mathbb{C}$ curve with $h(\Gamma) \subseteq \Gamma$ for $h \in \mathbb{C}(z)$
- ▶ Boring examples: $\Gamma = \mathbb{R}$ and $h \in \mathbb{R}(z)$, or $\Gamma \subseteq$ circle
- ▶ Better examples: $f,g \in \mathbb{C}(z)$, $\Gamma = g(\mathbb{R}) \not\subset$ circle, $f \circ g \in \mathbb{R}(z)$, $h = g \circ f$:

$$h(\Gamma) = (g \circ f)(\Gamma) = g(f(g(\mathbb{R}))) \subseteq g(\mathbb{R}) = \Gamma$$

Can Γ be a Jordan curve? (Eremenko 2012), Yes (Müller 2015):

$$\omega = e^{2\pi i/3}$$

$$f(z) = \frac{(6\omega + 5)z^3 + (-6\omega - 3)z^2 - 3z + 1}{4z^3 - 6z^2 + 3z}$$

$$g(z) = \frac{z^2 - \omega}{2z^3 + z^2 + (\omega + 1)z - \omega}$$

$$f(g(z)) = \frac{64z^9 - 192z^5 - 104z^3 - 48z}{96z^8 + 104z^6 + 96z^4 - 8}$$

► Can h be injective on Γ? (Eremenko 2013), No (Müller 2015)



Monodromy group $\mathsf{Mon}(f)$ of rational function $f(z) = \frac{p(z)}{q(z)} \in \mathcal{K}(z)$

 $\mathsf{Mon}(f) \leq \mathsf{Sym}(n) \text{ transitive}, \ n = \deg f = \mathsf{max}(\deg p, \deg q)$

Monodromy group $\mathsf{Mon}(f)$ of rational function $f(z) = \frac{p(z)}{q(z)} \in K(z)$

 $Mon(f) \le Sym(n)$ transitive, $n = \deg f = \max(\deg p, \deg q)$

▶ Algebraic definition: Mon(f) = Gal(p(z) - tq(z)/K(t)), acting on roots of p(z) - tq(z)

Monodromy group Mon(f) of rational function $f(z) = \frac{p(z)}{q(z)} \in K(z)$

 $Mon(f) \le Sym(n)$ transitive, $n = \deg f = \max(\deg p, \deg q)$

▶ Algebraic definition: $\mathsf{Mon}(f) = \mathsf{Gal}(p(z) - tq(z)/K(t))$, acting on roots of p(z) - tq(z) $\mathsf{Mon}_{\mathsf{geo}}(f) = \mathsf{Gal}(p(z) - tq(z)/\bar{K}(t)) \leq \mathsf{Mon}(f)$

Monodromy group Mon(f) of rational function $f(z) = \frac{p(z)}{q(z)} \in K(z)$

 $Mon(f) \le Sym(n)$ transitive, $n = \deg f = \max(\deg p, \deg q)$

- ▶ Algebraic definition: $\mathsf{Mon}(f) = \mathsf{Gal}(p(z) tq(z)/K(t))$, acting on roots of p(z) tq(z) $\mathsf{Mon}_{\mathsf{geo}}(f) = \mathsf{Gal}(p(z) - tq(z)/\bar{K}(t)) \leq \mathsf{Mon}(f)$
- ▶ Geometric definition for $K = \mathbb{C}$ (or \mathbb{R}): Coming soon . . .

Monodromy group Mon(f) of rational function $f(z) = \frac{p(z)}{q(z)} \in K(z)$

 $Mon(f) \le Sym(n)$ transitive, $n = \deg f = \max(\deg p, \deg q)$

- ▶ Algebraic definition: $\mathsf{Mon}(f) = \mathsf{Gal}(p(z) tq(z)/K(t))$, acting on roots of p(z) tq(z) $\mathsf{Mon}_{\mathsf{geo}}(f) = \mathsf{Gal}(p(z) - tq(z)/\bar{K}(t)) \leq \mathsf{Mon}(f)$
- ▶ Geometric definition for $K = \mathbb{C}$ (or \mathbb{R}): Coming soon . . .

Advantages/Disadvantages

- \oplus Works over any field K.
- \oplus Often the pair $Mon_{geo}(f)$, Mon(f) matters.
- \oplus Some properties of Mon(f) can be proven algebraically.
- \ominus Important properties, even for $K=\mathbb{C}$, cannot (yet) be proven algebraically.
- → Some considerations look natural in a geometric setting, and artificial in this algebraic setting.

Geometric definition of Mon(f) (Riemann)

Critical values (= branch points) of
$$f \in \mathbb{C}(z)$$

$$a \in \mathbb{C} \cup \{\infty\} \text{ critical value}$$

$$\Leftrightarrow$$

$$|f^{-1}(a)| < \deg f$$

$$\Leftrightarrow$$

$$f(z) - a \text{ has multiple root}$$

Geometric definition of Mon(f) (Riemann)

Critical values (= branch points) of
$$f \in \mathbb{C}(z)$$

$$a \in \mathbb{C} \cup \{\infty\} \text{ critical value}$$

$$\Leftrightarrow$$

$$|f^{-1}(a)| < \deg f$$

$$\Leftrightarrow$$

$$f(z) - a \text{ has multiple root}$$

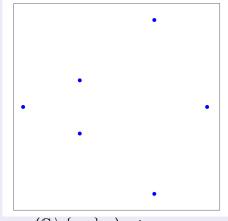
Example

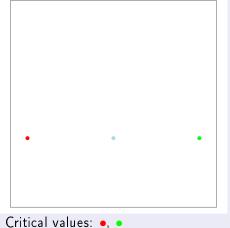
$$f(z) - 0 = \frac{16(4z+5)(z-1)^5}{729z}$$

$$f(z) - 1 = \frac{4(2z-5)(4z^2 - 11z + 16)(2z+1)^3}{729z}$$

Critical values: 0, 1 and ∞

$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

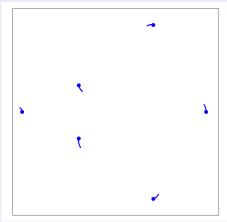




 $\pi_1(\mathbb{C}\setminus\{ullet,ullet\},ullet)$ acts on $f^{-1}(ullet)=\{ullet,ullet,\ldots,ullet\}$

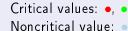
Noncritical value:

$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

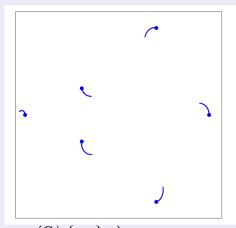


 $\pi_1(\mathbb{C}\setminus\{ullet,ullet\},ullet)$ acts on

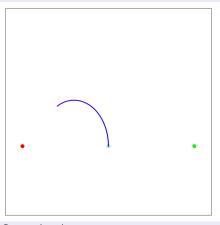
 $f^{-1}(\bullet) = \{\bullet, \bullet, \dots, \bullet\}$



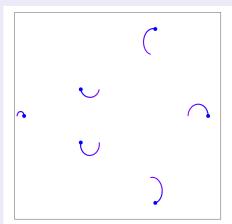
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



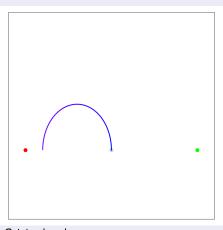




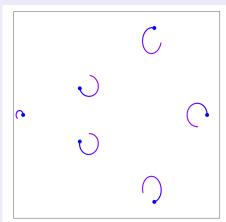
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



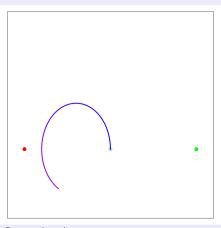




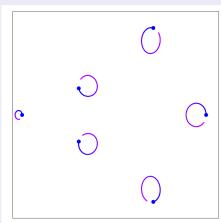
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



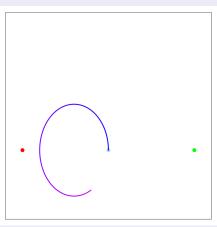




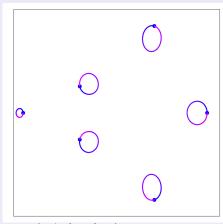
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



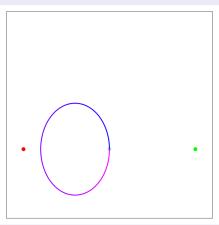




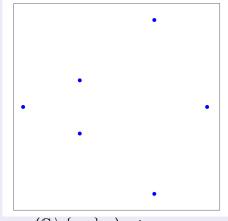
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

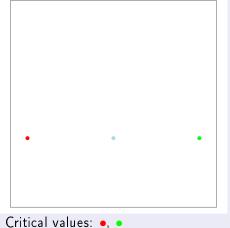






$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

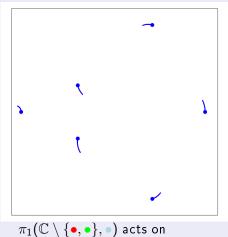




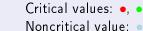
 $\pi_1(\mathbb{C}\setminus\{ullet,ullet\},ullet)$ acts on $f^{-1}(ullet)=\{ullet,ullet,\ldots,ullet\}$

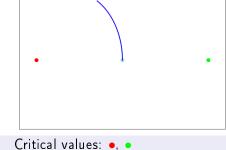
Noncritical value:

$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

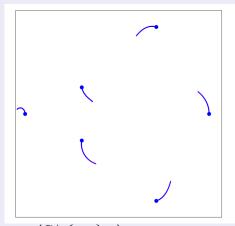


 $f^{-1}(\bullet) = \{\bullet, \bullet, \dots, \bullet\}$

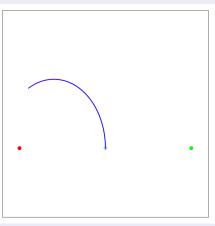




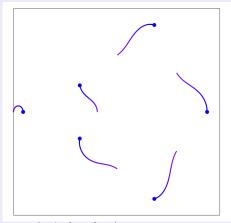
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

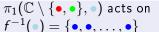


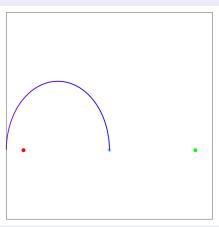




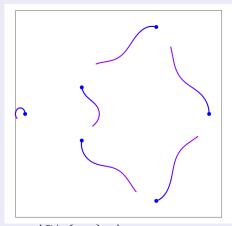
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



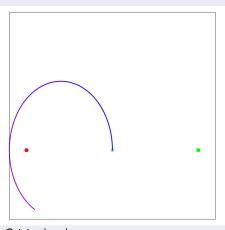




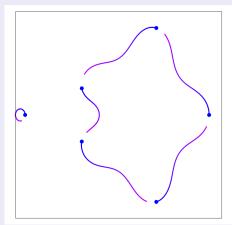
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



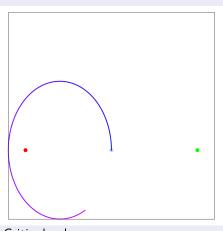




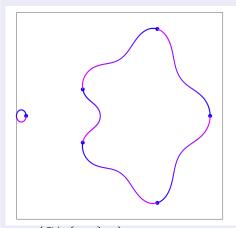
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



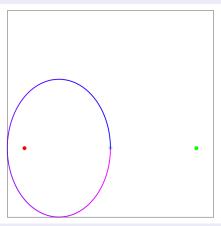




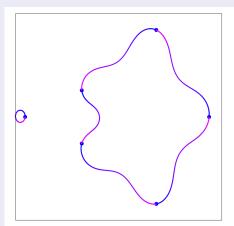
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



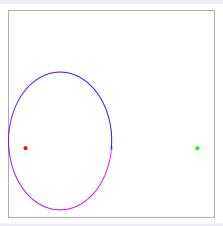




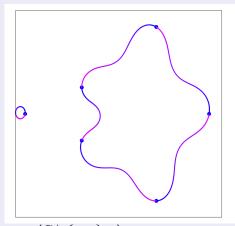
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

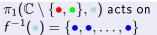


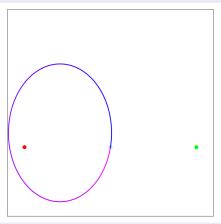




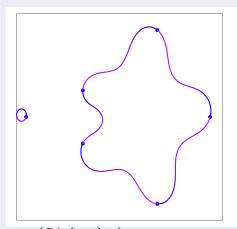
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



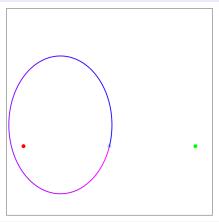




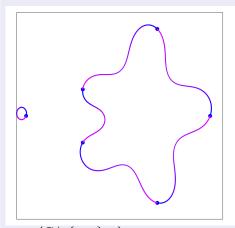
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



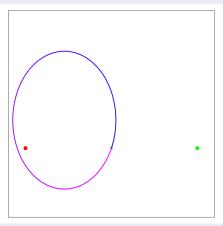
$$\pi_1(\mathbb{C}\setminus\{ullet,ullet\},ullet)$$
 acts on $f^{-1}(ullet)=\{ullet,ullet,\ldots,ullet\}$



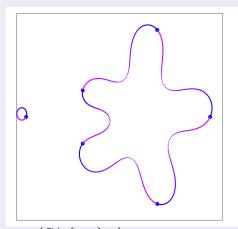
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



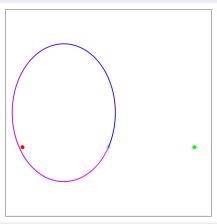




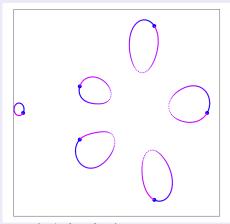
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



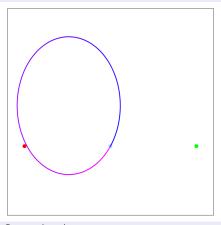
$$\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$$
 acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$



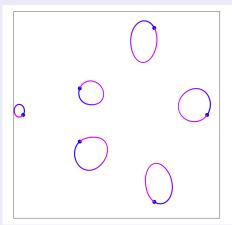
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



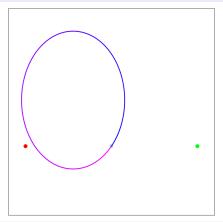




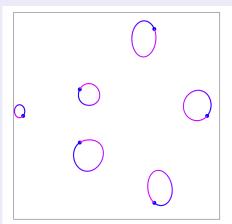
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

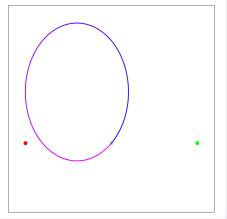






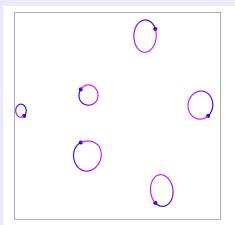
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

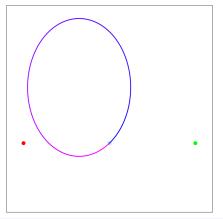




$$\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$$
 acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

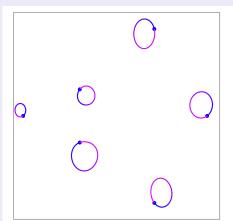
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

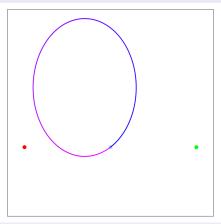




$$\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$$
 acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\dots,\bullet\}$

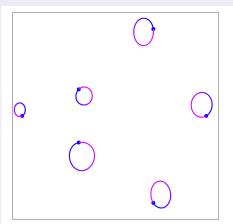
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

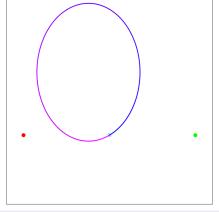




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\dots,\bullet\}$

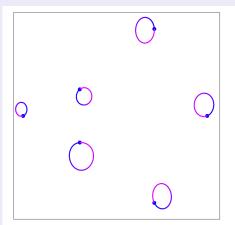
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

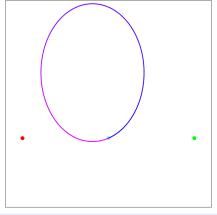




$$\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$$
 acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\dots,\bullet\}$

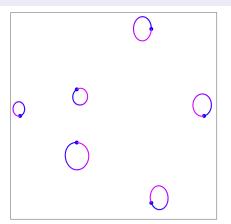
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

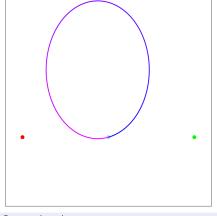




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

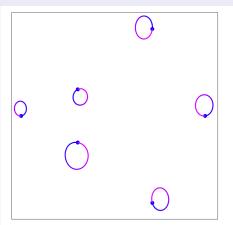
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

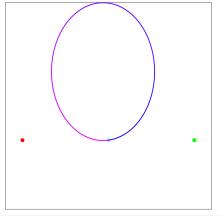




$$\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$$
 acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\dots,\bullet\}$

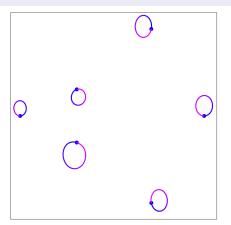
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

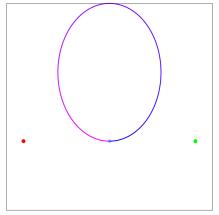




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

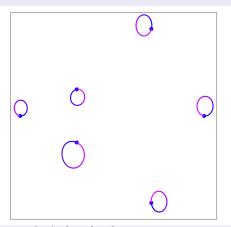
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

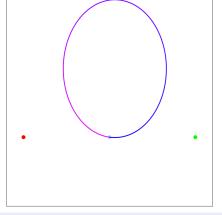




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

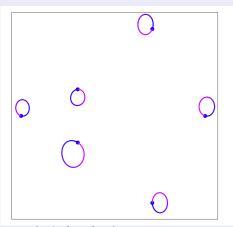
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

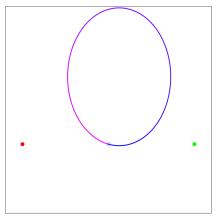




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\dots,\bullet\}$

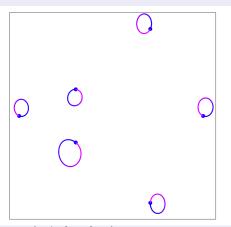
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

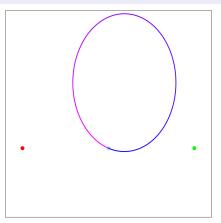




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

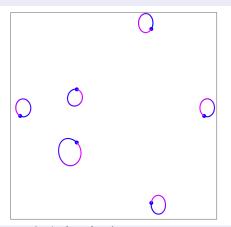
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

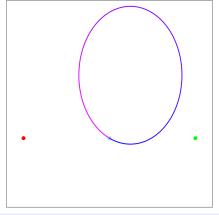




$$\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$$
 acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

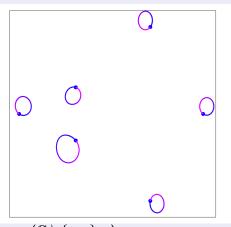
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

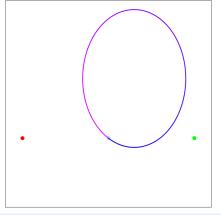




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

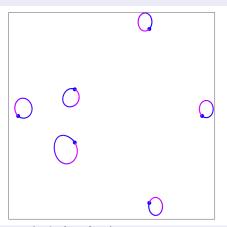
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

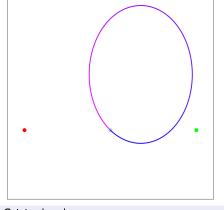




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

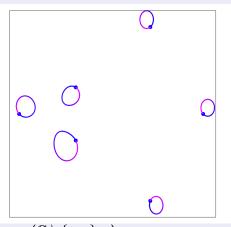
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

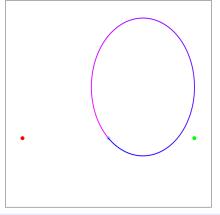




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\dots,\bullet\}$

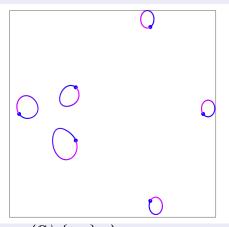
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

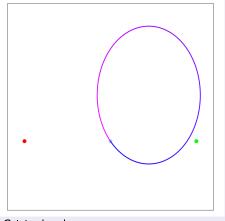




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

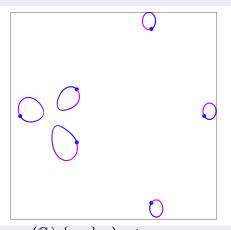
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

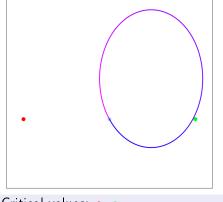




 $\pi_1(\mathbb{C}\setminus\{\bullet,\bullet\},\bullet)$ acts on $f^{-1}(\bullet)=\{\bullet,\bullet,\ldots,\bullet\}$

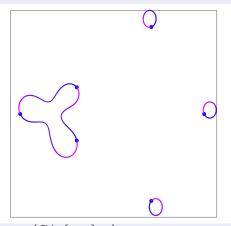
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



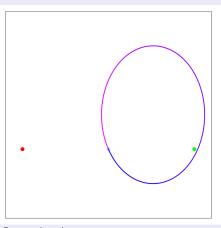


 $\pi_1(\mathbb{C}\setminus\{ullet,ullet\},ullet)$ acts on $f^{-1}(ullet)=\{ullet,ullet,\ldots,ullet\}$

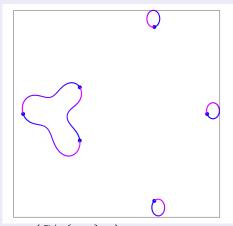
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



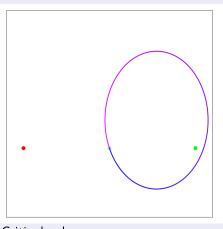




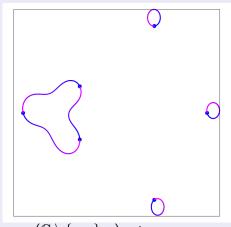
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



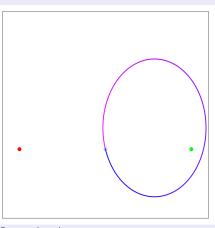




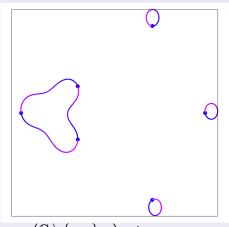
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

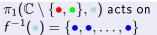


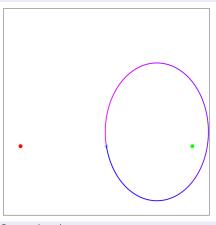




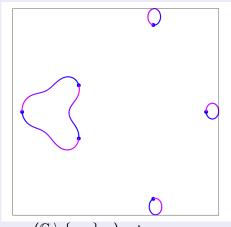
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



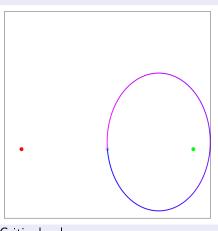




$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

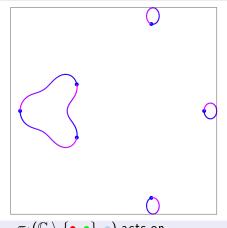




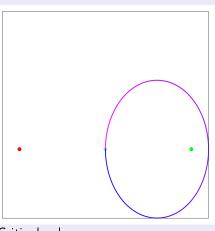


Critical values: •, •
Noncritical value: •

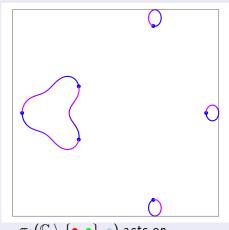
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

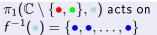


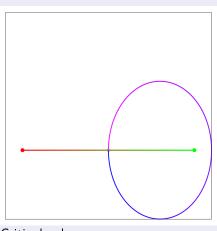




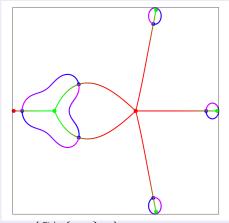
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



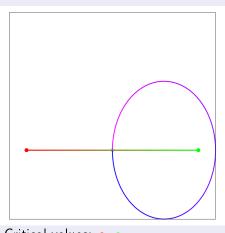




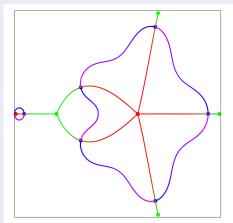
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$



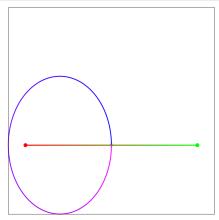




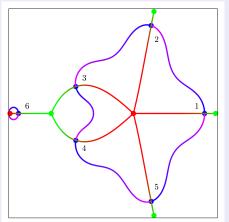
$$z \mapsto f(z) = \frac{16(4z+5)(z-1)^5}{729z}$$

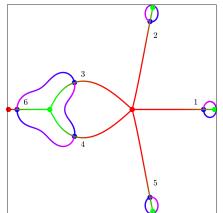






Generators of Mon(f)





$$\sigma_1 = (12345)$$

$$\sigma_2 = (364)$$

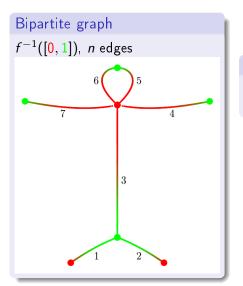
$$\mathsf{Mon}(f) = \langle \sigma_1, \sigma_2 \rangle = \mathsf{Alt}(6)$$

Dessins d'enfants (Grothendieck 1984) Linienzüge (Felix Klein 1879)

Rational function

 $f(z) \in \mathbb{C}(z)$, degree n, critical values 0, 1 and ∞

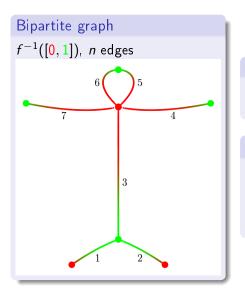
Dessins d'enfants (Grothendieck 1984) Linienzüge (Felix Klein 1879)



Rational function

 $f(z) \in \mathbb{C}(z)$, degree n, critical values 0,1 and ∞

Dessins d'enfants (Grothendieck 1984) Linienzüge (Felix Klein 1879)



Rational function

 $f(z) \in \mathbb{C}(z)$, degree \emph{n} , critical values $\emph{0}, 1$ and ∞

Generators of Mon(f)

$$\sigma_1 = (123)(56)$$

$$\sigma_2 = (34567)$$

$$\sigma_3 = (\sigma_1 \sigma_2)^{-1} = (123467)$$

Properties of monodromy groups

Riemann's Existence Theorem

$$f(z) \in \mathbb{C}(z)$$
 of degree n with r critical values

- ▶ $\mathsf{Mon}(f) = \langle \sigma_1, \sigma_2, \dots, \sigma_r \rangle \leq \mathsf{Sym}(n)$ transitive
- $ightharpoonup \sum_{i=1}^r \text{number of cycles of } \sigma_i = (r-2)n+2$

Properties of monodromy groups

Riemann's Existence Theorem

$$f(z) \in \mathbb{C}(z)$$
 of degree n with r critical values \updownarrow

- ▶ $\mathsf{Mon}(f) = \langle \sigma_1, \sigma_2, \dots, \sigma_r \rangle \leq \mathsf{Sym}(n)$ transitive
- $ightharpoonup \sum_{i=1}^r \text{number of cycles of } \sigma_i = (r-2)n+2$

Examples

f(z)	r	Mon(f)
	2	<(12 n)> cyclic

Properties of monodromy groups

Riemann's Existence Theorem

$$f(z) \in \mathbb{C}(z)$$
 of degree n with r critical values \uparrow

- ▶ $\mathsf{Mon}(f) = \langle \sigma_1, \sigma_2, \dots, \sigma_r \rangle \leq \mathsf{Sym}(n)$ transitive
- $ightharpoonup \sum_{i=1}^r \text{number of cycles of } \sigma_i = (r-2)n+2$

Examples

f(z)	r	Mon(f)
Z^n	2	<(12 n)> cyclic
$f(\cos\phi)=\cos n\phi$	3	dihedral group of order 2n

Properties of monodromy groups

Riemann's Existence Theorem

$$f(z) \in \mathbb{C}(z)$$
 of degree n with r critical values \updownarrow

- ▶ $\mathsf{Mon}(f) = \langle \sigma_1, \sigma_2, \dots, \sigma_r \rangle \leq \mathsf{Sym}(n)$ transitive
- $ightharpoonup \sum_{i=1}^r \text{number of cycles of } \sigma_i = (r-2)n+2$

Examples

f(z)	r	Mon(f)
z^n	2	<(12 n)> cyclic
$f(\cos\phi)=\cos n\phi$	3	dihedral group of order 2 <i>n</i>
"random", degree <i>n</i>	2(n-1)	Sym(n)

Properties of monodromy groups

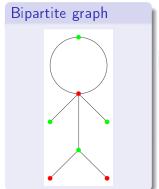
Riemann's Existence Theorem

$$f(z) \in \mathbb{C}(z)$$
 of degree n with r critical values \updownarrow

- ▶ $\mathsf{Mon}(f) = \langle \sigma_1, \sigma_2, \dots, \sigma_r \rangle \leq \mathsf{Sym}(n)$ transitive
- $ightharpoonup \sum_{i=1}^r \text{number of cycles of } \sigma_i = (r-2)n+2$

Examples

f(z)	r	Mon(f)
z ⁿ	2	<(12 n)> cyclic
$f(\cos\phi)=\cos n\phi$	3	dihedral group of order 2 <i>n</i>
"random", degree <i>n</i>	2(n-1)	Sym(<i>n</i>)
?	3	Aut(Higman-Sims), degree 100



Translate ramification data

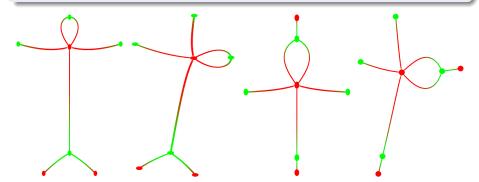
$$f(z) - 0 = \frac{(z - \alpha)^5 (z^2 + \beta z + \gamma)}{z}$$
$$f(z) - 1 = \frac{(z - \delta)^3 (z - \epsilon)^2 (z^2 + \zeta z + \eta)}{z}$$

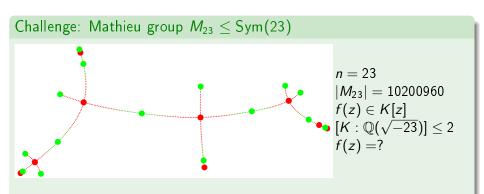
Polynomial system

Compare coefficients, solve polynomial system in $\{\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta\}$

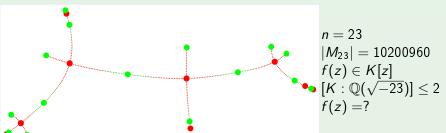
Problem

- ► This considers only vertex degrees of the dessin, one obtains many "wrong" solutions.
- ▶ Polynomial system solvable only about up to n = 10.



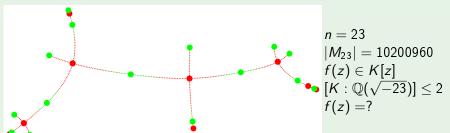


Challenge: Mathieu group $M_{23} \leq \text{Sym}(23)$



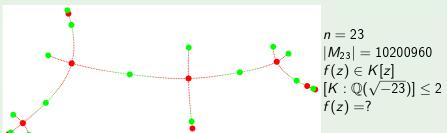
► (*Matiyasevich 1998*) Compute numerical approximation by deformation, determine algebraic coefficients.

Challenge: Mathieu group $M_{23} \leq \text{Sym}(23)$



- ► (*Matiyasevich 1998*) Compute numerical approximation by deformation, determine algebraic coefficients.
- ▶ (*Elkies 2013*) Solve polynomial system over \mathbb{F}_p , lift this to p-adic solution in \mathbb{Q}_p , determine algebraic coefficients.

Challenge: Mathieu group $M_{23} \leq \text{Sym}(23)$



- ► (*Matiyasevich 1998*) Compute numerical approximation by deformation, determine algebraic coefficients.
- ▶ (*Elkies 2013*) Solve polynomial system over \mathbb{F}_p , lift this to p-adic solution in \mathbb{Q}_p , determine algebraic coefficients.
- ► (Müller 2015) Formal power series and group action yield a polynomial system which can be solved directly.

Lemma

For $g(z) \in \mathbb{C}(z)$ the following properties are equivalent:

- (i) $\Gamma = g(\mathbb{R})$ is contained in a circle.
- (ii) $\lambda(g(z)) \in \mathbb{R}(z)$ for a linear fractional $\lambda \in \mathbb{C}(z)$.
- (iii) $\mathbb{C}(g(z)) = \mathbb{C}(\bar{g}(z))$.

Lemma

For $g(z) \in \mathbb{C}(z)$ the following properties are equivalent:

- (i) $\Gamma = g(\mathbb{R})$ is contained in a circle.
- (ii) $\lambda(g(z)) \in \mathbb{R}(z)$ for a linear fractional $\lambda \in \mathbb{C}(z)$.
- (iii) $\mathbb{C}(g(z)) = \mathbb{C}(\bar{g}(z))$.

Second question about invariant curves is (essentially) equivalent to

Theorem

Take $f,g\in\mathbb{C}(z)$. Suppose that

- $f(g(z)) \in \mathbb{R}(z)$, and
- $ightharpoonup \mathbb{R} o \mathbb{R}$, $a \mapsto f(g(a))$ is injective.

Then
$$f \circ g = \underbrace{f \circ \lambda^{-1}}_{\in \mathbb{R}(z)} \circ \underbrace{\lambda \circ g}_{\in \mathbb{R}(z)}$$
 for a linear fractional $\lambda \in \mathbb{C}(z)$.

Proposition

Given

- ▶ permutation group $G \leq \operatorname{Sym}(n)$,
- $ightharpoonup \sigma \in \operatorname{Sym}(n)$ involution with $G = \sigma G \sigma^{-1}$, and
- $ightharpoonup \sigma$ has exactly one fixed point ω .

Then $M = \sigma M \sigma^{-1}$ for each subgroup M with $G_{\omega} < M < G$.

Proof of the theorem (sketch).

- ightharpoonup W.l.o.g. $f(g(z)) = rac{p(z)}{q(z)}$ with $p,q \in \mathbb{R}[z]$ relatively prime, and
 - ▶ $\deg p > \deg q$
 - $p(z) = \prod (z \alpha_i)$ separable

 - ▶ $\alpha_i \notin \mathbb{R}$ for $i \ge 2$

Proof of the theorem (sketch).

- ightharpoonup W.l.o.g. $f(g(z)) = rac{p(z)}{q(z)}$ with $p,q \in \mathbb{R}[z]$ relatively prime, and
 - $\deg p > \deg q$
 - $p(z) = \prod (z \alpha_i)$ separable

 - $\quad \quad \alpha_i \notin \mathbb{R} \text{ for } i \geq 2$
- ightharpoonup Hensel's Lemma: $p(z)-tq(z)=\prod(z-\omega_i)$ with
 - $\qquad \qquad \omega = \omega_1 \in \mathbb{R}[[t]]$
 - $\omega_i \in \mathbb{C}[[t]] \setminus \mathbb{R}[[t]]$ for $i \geq 2$



Proof continued.

$$p(z)-tq(z)=\prod(z-\omega_i)$$
 with $\omega=\omega_1\in\mathbb{R}[[t]]$ and $\omega_i\in\mathbb{C}[[t]]\setminus\mathbb{R}[[t]]$ for $i\geq 2$ $t=rac{p(\omega)}{q(\omega)}=f(g(\omega))=ar{f}(ar{g}(\omega))$ $\sigma=$ complex conjugation on coefficients of $\mathbb{C}((t))$, restricted to $\mathbb{C}(\omega_1,\omega_2,\dots)\subset\mathbb{C}((t))$

