Rational functions and finite permutation groups

Peter Müller

Würzburg, 1 February 2016

What I'm interested in

- Inverse Galois problem
- Combinatorial questions about finite fields, like permutation polynomials, Kakeya sets, (A)PN functions, ...
- Finite geometries, algebraic combinatorics, permutation codes
- Permutation groups and applications to
  - number theory (Hilbert's irreducibility theorem, arithmetically equivalent fields, ...)
  - polynomials and rational functions via their monodromy groups

Historic examples where group theory helped

- *Ritt:* Maximal decompositions

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

of polynomials and rational functions

Historic examples where group theory helped

- *Ritt:* Maximal decompositions

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

  of polynomials and rational functions
- *Cassels, Lewis, Davenport:* Reducibility of variable-separated algebraic curves $f(X) - g(Y) = 0$

Historic examples where group theory helped

- *Ritt:* Maximal decompositions

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

of polynomials and rational functions

- *Cassels, Lewis, Davenport:* Reducibility of variable-separated algebraic curves $f(X) - g(Y) = 0$
- *Birch, Swinnerton-Dyer, Cohen:* Value sets of "generic" rational functions $f(z) \in \mathbb{F}_q(z)$, $n = \deg f$:

$$\frac{1}{q}|f(\mathbb{F}_q)| = 1 - \frac{1}{2!} + \frac{1}{3!} - \cdots - (-1)^n \frac{1}{n!} + O_n(q^{-1/2})$$

Historic examples where group theory helped

- *Ritt:* Maximal decompositions
$$f(z) = f_1(f_2(\ldots(f_m(z))\ldots))$$
of polynomials and rational functions
- *Cassels, Lewis, Davenport:* Reducibility of variable-separated algebraic curves $f(X) - g(Y) = 0$
- *Birch, Swinnerton-Dyer, Cohen:* Value sets of "generic" rational functions $f(z) \in \mathbb{F}_q(z)$, $n = \deg f$:
$$\frac{1}{q}|f(\mathbb{F}_q)| = 1 - \frac{1}{2!} + \frac{1}{3!} - \cdots - (-1)^n \frac{1}{n!} + O_n(q^{-1/2})$$
- *Schur:* For which $f(z) \in \mathbb{Z}[z]$ is
$$\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \quad a \mapsto f(a)$$
bijective for infinitely many primes p?

Invariant curves (*Fatou, Eremenko*)

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

Invariant curves (*Fatou, Eremenko*)

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

Invariant curves (*Fatou, Eremenko*)

- $\Gamma \subset \mathbb{C}$ 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

Invariant curves (*Fatou, Eremenko*)

- $\Gamma \subset \mathbb{C}$ 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: $f, g \in \mathbb{C}(z)$, $\Gamma = g(\mathbb{R}) \not\subseteq$ circle, $f \circ g \in \mathbb{R}(z)$, $h = g \circ f$:

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

Invariant curves (*Fatou, Eremenko*)

- $\Gamma \subset \mathbb{C}$ 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: $f, g \in \mathbb{C}(z)$, $\Gamma = g(\mathbb{R}) \not\subseteq$ circle, $f \circ g \in \mathbb{R}(z)$, $h = g \circ f$:

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

  - Can Γ be a Jordan curve?

Invariant curves (*Fatou, Eremenko*)

- $\Gamma \subset \mathbb{C}$ 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, $f \circ g \in \mathbb{R}(z)$, $h = g \circ f$:

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

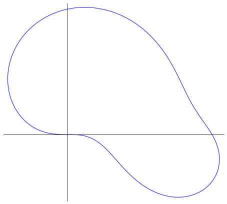
  - Can Γ be a Jordan curve? Yes (*M. 2015*):

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

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

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

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



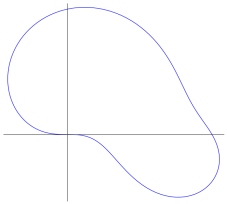
Invariant curves (*Fatou, Eremenko*)

- $\Gamma \subset \mathbb{C}$ 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, $f \circ g \in \mathbb{R}(z)$, $h = g \circ f$:

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

  - Can Γ be a Jordan curve? Yes (*M. 2015*):

$$\begin{aligned}
\omega &= e^{2\pi i/3} \\
f(z) &= \frac{(6\omega+5)z^3 + (-6\omega-3)z^2 - 3z + 1}{4z^3 - 6z^2 + 3z} \\
g(z) &= \frac{z^2 - \omega}{2z^3 + z^2 + (\omega+1)z - \omega} \\
f(g(z)) &= \frac{64z^9 - 192z^5 - 104z^3 - 48z}{96z^8 + 104z^6 + 96z^4 - 8}
\end{aligned}$$



  - can h be injective on Γ? No (*M. 2015*)

The monodromy group Mon(f) of a rational function f

K a field, $f(z) \in K(z)$ of degree n	$\longrightarrow$	$\mathrm{Mon}(f) \leq \mathrm{Sym}(n)$ transitive subgroup

- Algebraic definition by Galois theory for any field K
- Geometric definition for $K = \mathbb{C}$ (or $\mathbb{R}$)

Geometric definition of Mon(f) (*Riemann*)

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

$$a \in \mathbb{C} \cup \{\infty\} \text{ critical value}$$
$$\Leftrightarrow$$
$$|f^{-1}(a)| < \deg f$$
$$\Leftrightarrow$$
$$f(z) - a \text{ has multiple root}$$

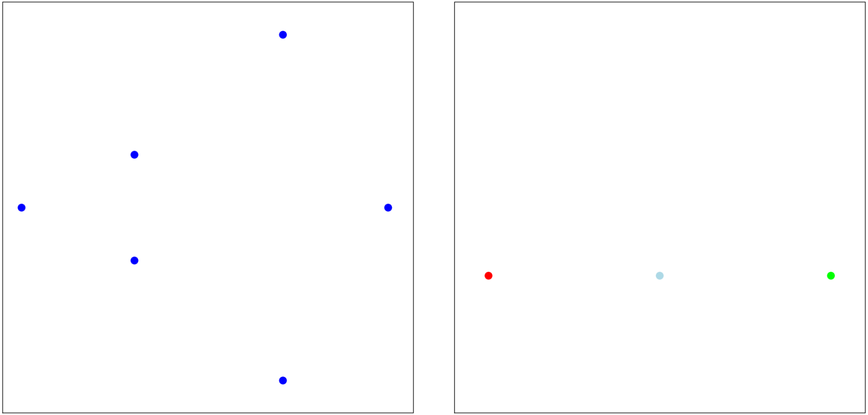
Example

$$f(z) - 0 = \frac{16(4z+5)(z-1)^5}{729z}$$
$$f(z) - 1 = \frac{4(2z-5)(4z^2-11z+16)(2z+1)^3}{729z}$$

Critical values: 0, 1 and ∞

Action of monodromy group

$$z \mapsto f(z)$$



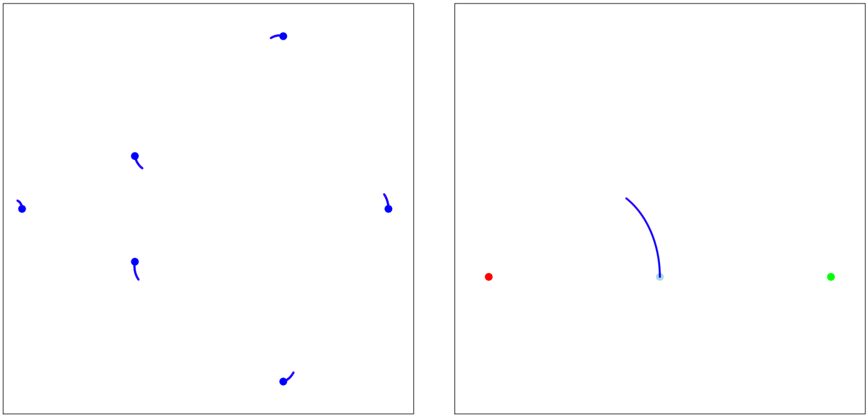
$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on $f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$

Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

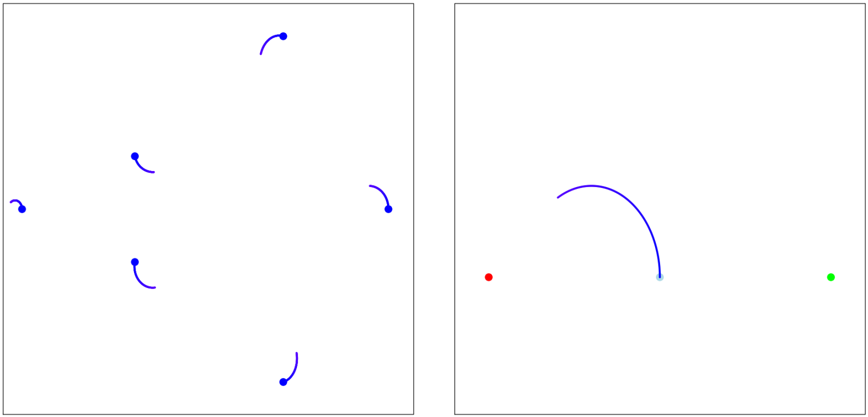


$\pi_1(\mathbb{C} \setminus \{\color{red}\bullet, \color{green}\bullet\}, \color{lightblue}\bullet)$ acts on
$f^{-1}(\color{lightblue}\bullet) = \{\color{blue}\bullet, \color{blue}\bullet, \ldots, \color{blue}\bullet\}$

Critical values: $\color{red}\bullet$, $\color{green}\bullet$
Noncritical value: $\color{lightblue}\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

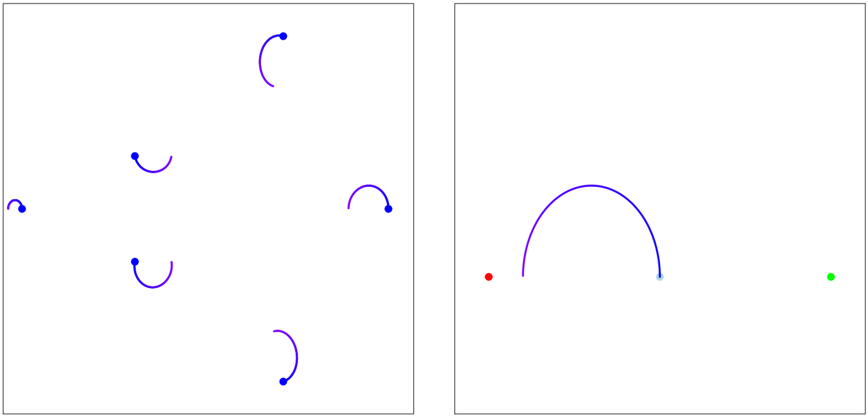


$\pi_1(\mathbb{C} \setminus \{\color{red}\bullet, \color{green}\bullet\}, \color{lightblue}\bullet)$ acts on
$f^{-1}(\color{lightblue}\bullet) = \{\color{blue}\bullet, \color{blue}\bullet, \ldots, \color{blue}\bullet\}$

Critical values: $\color{red}\bullet$, $\color{green}\bullet$
Noncritical value: $\color{lightblue}\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

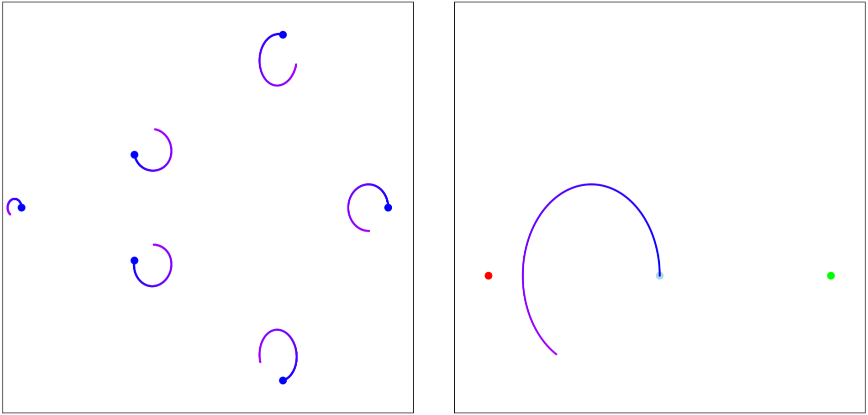


$\pi_1(\mathbb{C} \setminus \{\color{red}\bullet, \color{green}\bullet\}, \color{lightblue}\bullet)$ acts on
$f^{-1}(\color{lightblue}\bullet) = \{\color{blue}\bullet, \color{blue}\bullet, \ldots, \color{blue}\bullet\}$

Critical values: $\color{red}\bullet$, $\color{green}\bullet$
Noncritical value: $\color{lightblue}\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



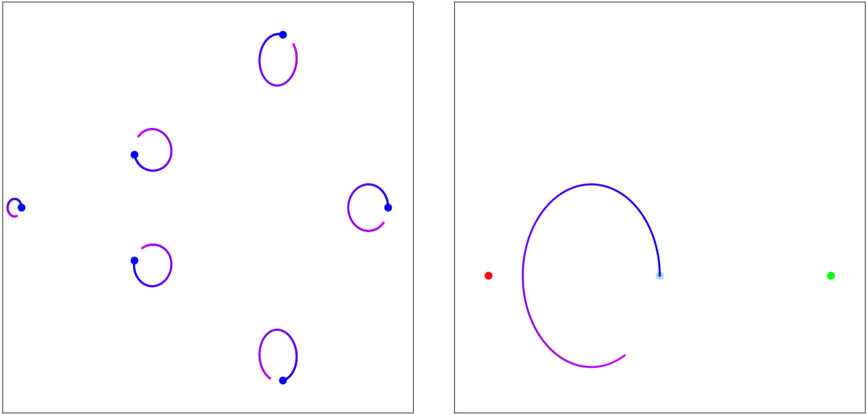
$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on $f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$

Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



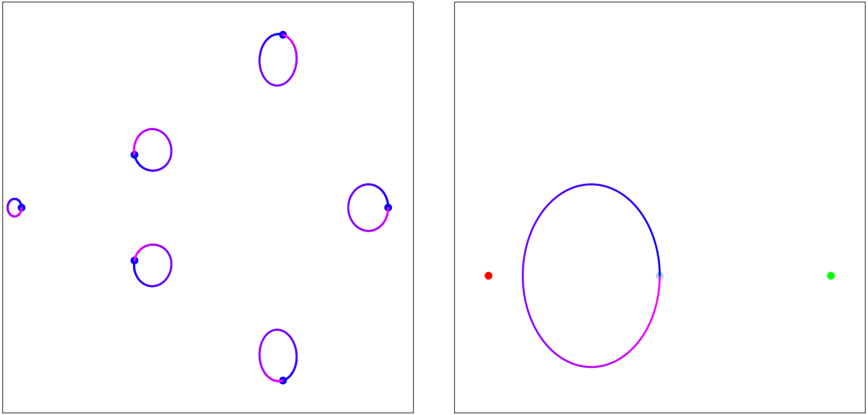
$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on $f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$

Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

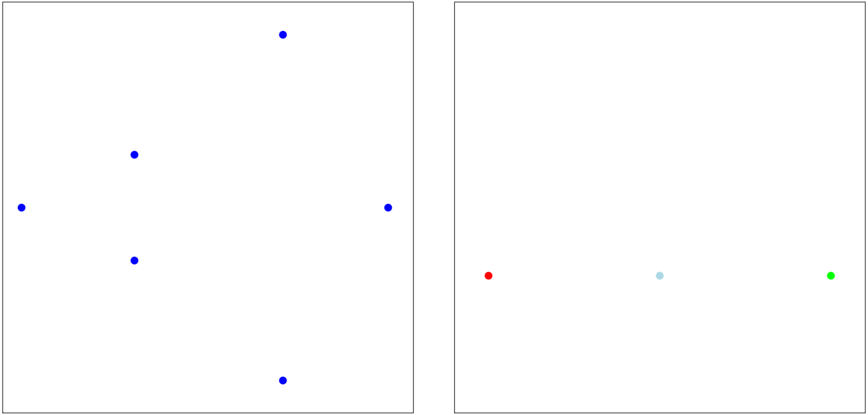


$\pi_1(\mathbb{C} \setminus \{●, ●\}, ●)$ acts on
$f^{-1}(●) = \{●, ●, \ldots, ●\}$

Critical values: ●, ●
Noncritical value: ●

Action of monodromy group

$$z \mapsto f(z)$$

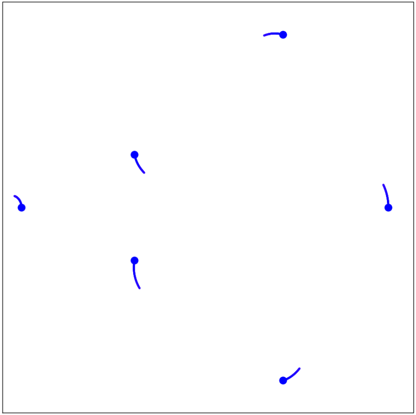


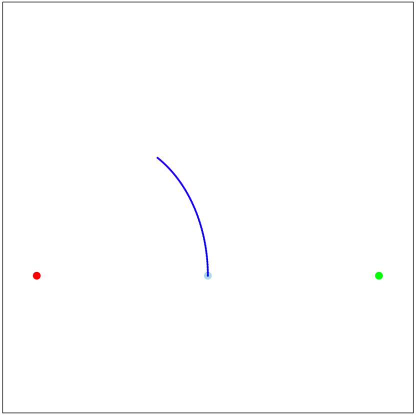
$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$





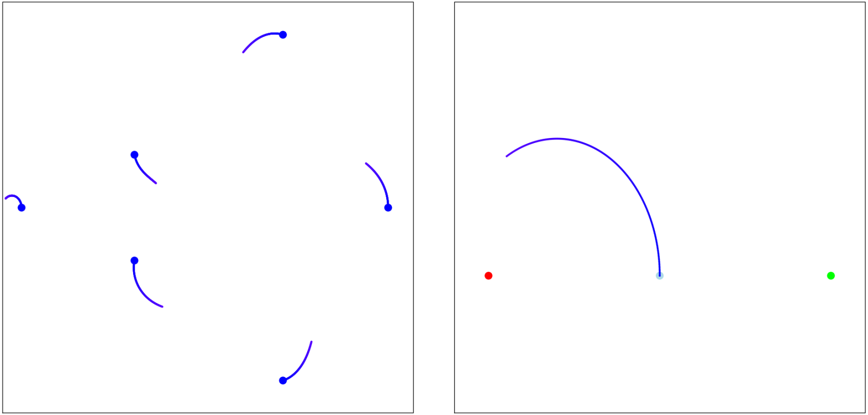
$\pi_1(\mathbb{C} \setminus \{\color{red}{\bullet}, \color{green}{\bullet}\}, \color{lightblue}{\bullet})$ acts on $f^{-1}(\color{lightblue}{\bullet}) = \{\color{blue}{\bullet}, \color{blue}{\bullet}, \ldots, \color{blue}{\bullet}\}$

Critical values: $\color{red}{\bullet}$, $\color{green}{\bullet}$

Noncritical value: $\color{lightblue}{\bullet}$

Action of monodromy group

$$z \mapsto f(z)$$

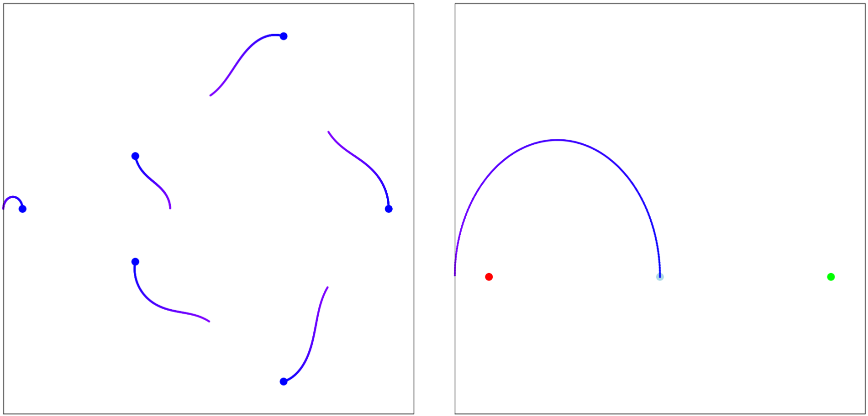


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



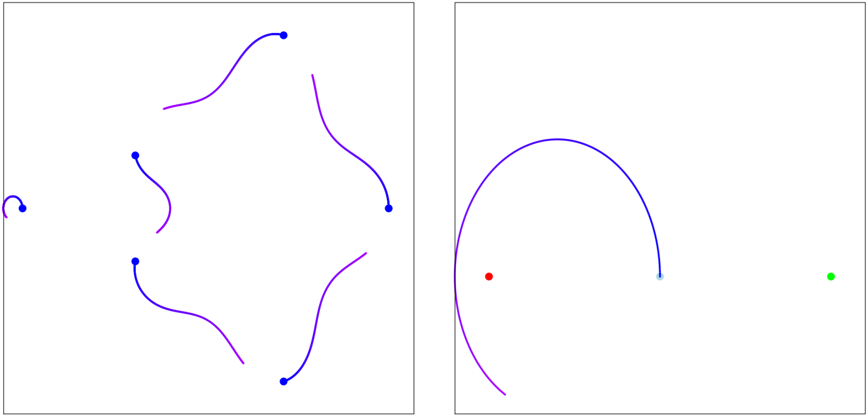
$\pi_1(\mathbb{C} \setminus \{\textcolor{red}{\bullet}, \textcolor{green}{\bullet}\}, \textcolor{lightblue}{\bullet})$ acts on
$f^{-1}(\textcolor{lightblue}{\bullet}) = \{\textcolor{blue}{\bullet}, \textcolor{blue}{\bullet}, \dots, \textcolor{blue}{\bullet}\}$

Critical values: $\textcolor{red}{\bullet}$, $\textcolor{green}{\bullet}$

Noncritical value: $\textcolor{lightblue}{\bullet}$

Action of monodromy group

$$z \mapsto f(z)$$

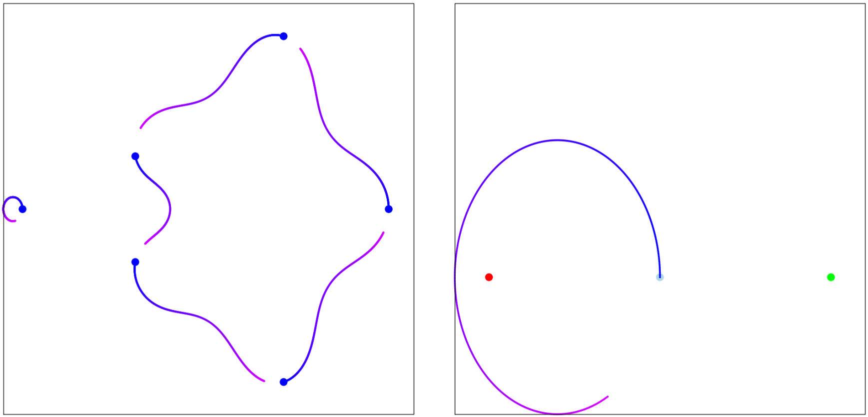


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

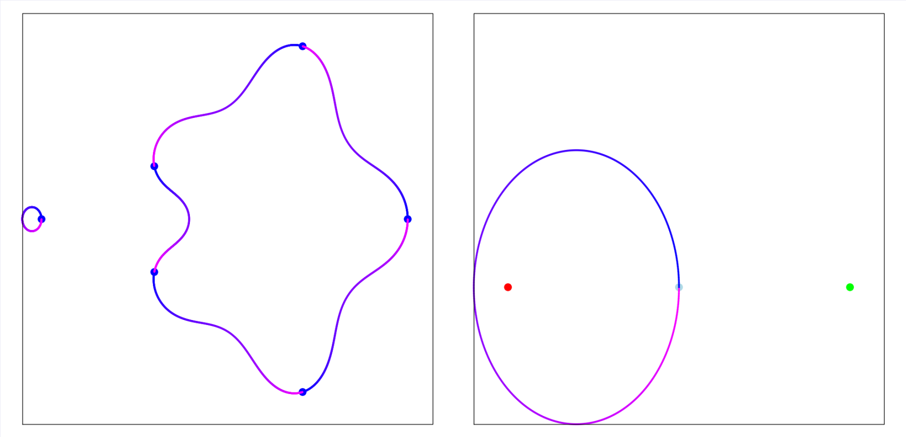


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



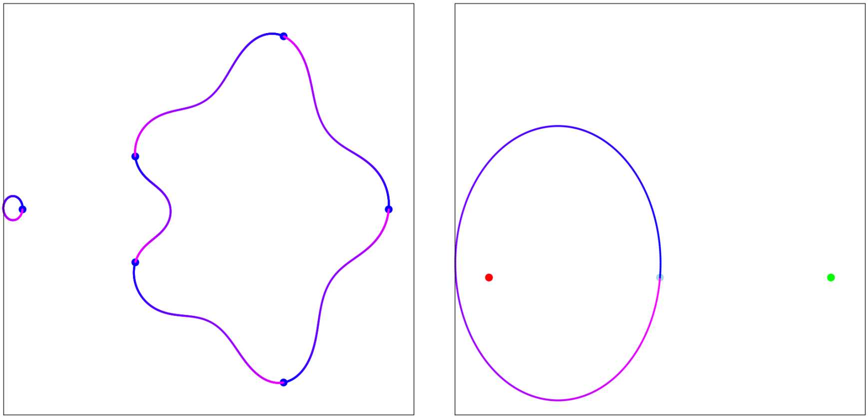
$\pi_1(\mathbb{C} \setminus \{\textcolor{red}{\bullet}, \textcolor{green}{\bullet}\}, \textcolor{lightblue}{\bullet})$ acts on $f^{-1}(\textcolor{lightblue}{\bullet}) = \{\textcolor{blue}{\bullet}, \textcolor{blue}{\bullet}, \ldots, \textcolor{blue}{\bullet}\}$

Critical values: $\textcolor{red}{\bullet}$, $\textcolor{green}{\bullet}$

Noncritical value: $\textcolor{lightblue}{\bullet}$

Action of monodromy group

$$z \mapsto f(z)$$

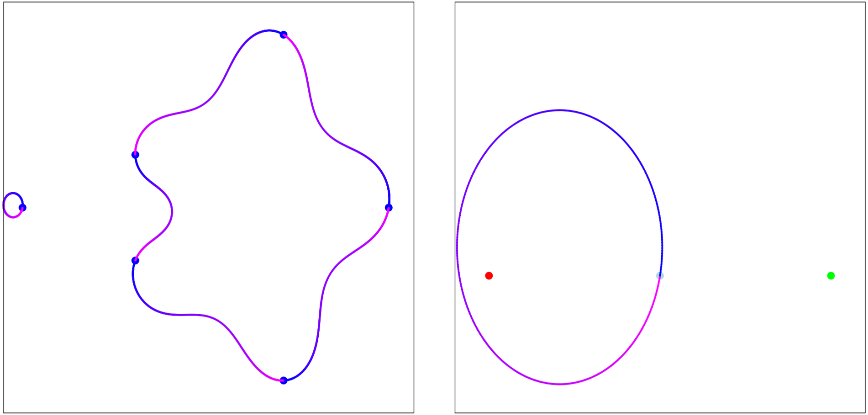


$\pi_1(\mathbb{C} \setminus \{\textcolor{red}{\bullet}, \textcolor{green}{\bullet}\}, \textcolor{lightblue}{\bullet})$ acts on
$f^{-1}(\textcolor{lightblue}{\bullet}) = \{\textcolor{blue}{\bullet}, \textcolor{blue}{\bullet}, \ldots, \textcolor{blue}{\bullet}\}$

Critical values: $\textcolor{red}{\bullet}$, $\textcolor{green}{\bullet}$
Noncritical value: $\textcolor{lightblue}{\bullet}$

Action of monodromy group

$$z \mapsto f(z)$$

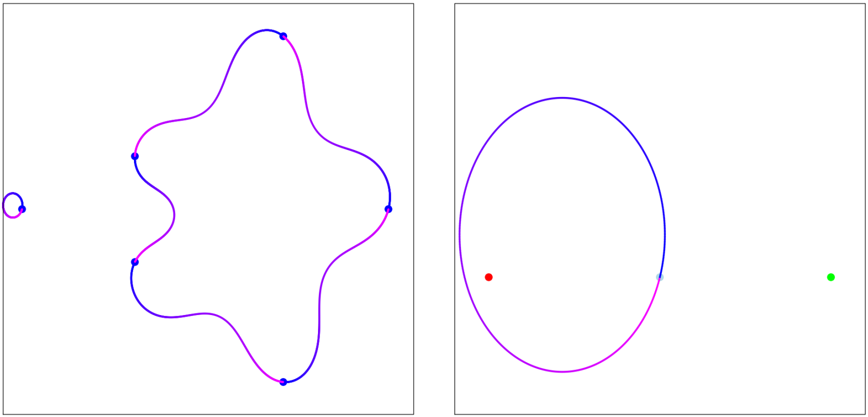


$\pi_1(\mathbb{C} \setminus \{\color{red}\bullet, \color{green}\bullet\}, \color{lightblue}\bullet)$ acts on
$f^{-1}(\color{lightblue}\bullet) = \{\color{blue}\bullet, \color{blue}\bullet, \ldots, \color{blue}\bullet\}$

Critical values: $\color{red}\bullet$, $\color{green}\bullet$
Noncritical value: $\color{lightblue}\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



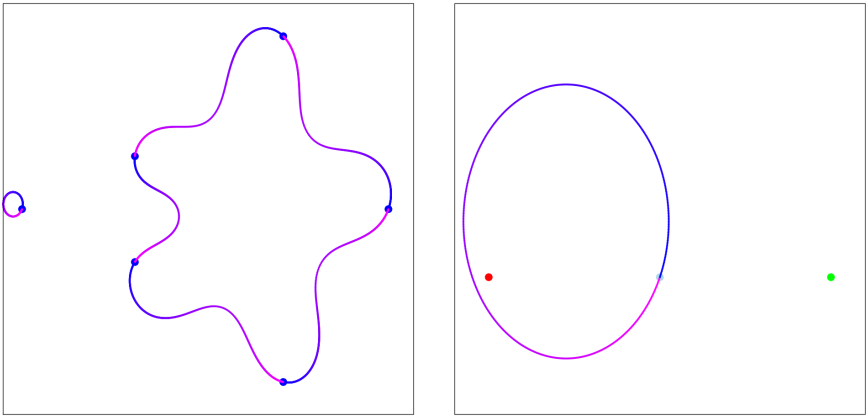
$\pi_1(\mathbb{C} \setminus \{●, ●\}, ●)$ acts on $f^{-1}(●) = \{●, ●, \dots, ●\}$

Critical values: ●, ●

Noncritical value: ●

Action of monodromy group

$$z \mapsto f(z)$$



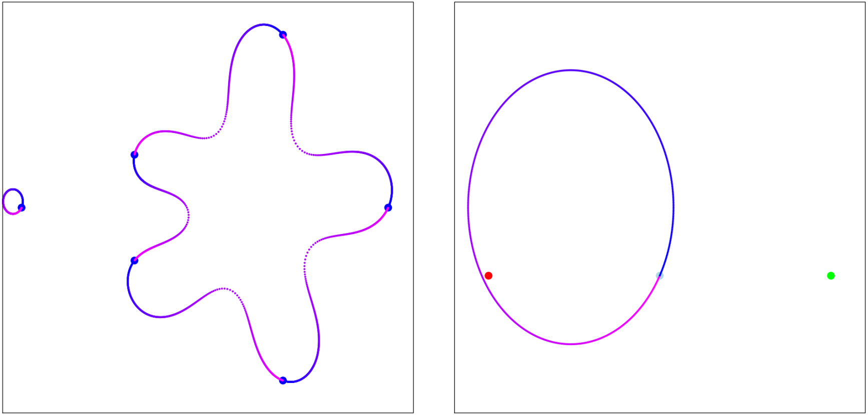
$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on $f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$

Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



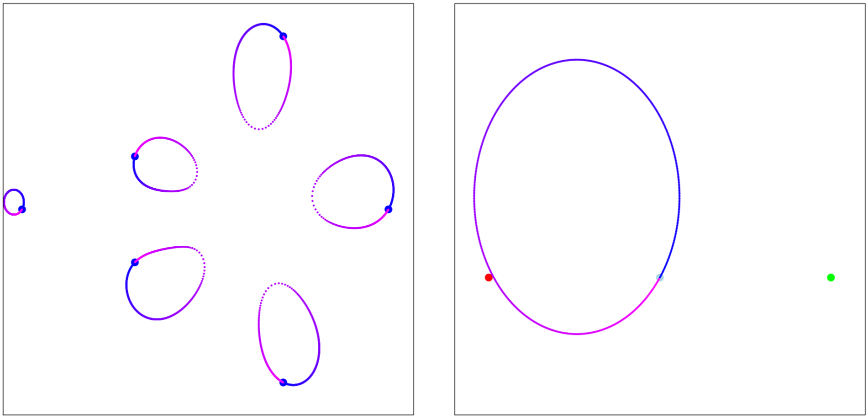
$\pi_1(\mathbb{C} \setminus \{\textcolor{red}{\bullet}, \textcolor{green}{\bullet}\}, \textcolor{lightblue}{\bullet})$ acts on $f^{-1}(\textcolor{lightblue}{\bullet}) = \{\textcolor{blue}{\bullet}, \textcolor{blue}{\bullet}, \ldots, \textcolor{blue}{\bullet}\}$

Critical values: $\textcolor{red}{\bullet}$, $\textcolor{green}{\bullet}$

Noncritical value: $\textcolor{lightblue}{\bullet}$

Action of monodromy group

$$z \mapsto f(z)$$

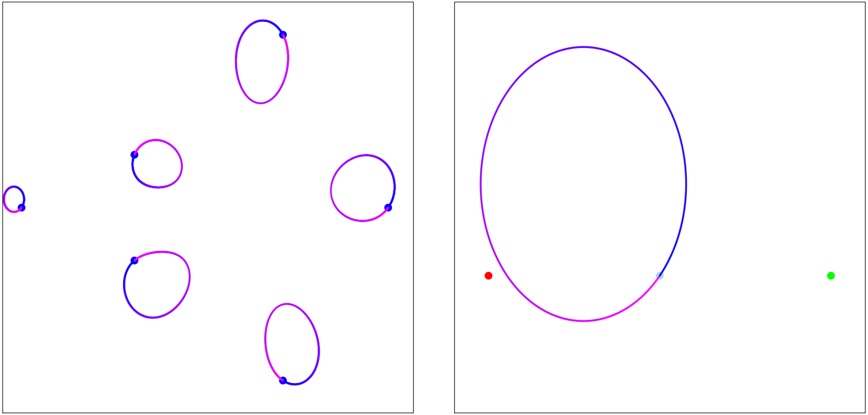


$\pi_1(\mathbb{C} \setminus \{$●, ●$\},$ ●$)$ acts on
$f^{-1}($●$) = \{$●, ●, $\ldots$, ●$\}$

Critical values: ●, ●
Noncritical value: ●

Action of monodromy group

$$z \mapsto f(z)$$

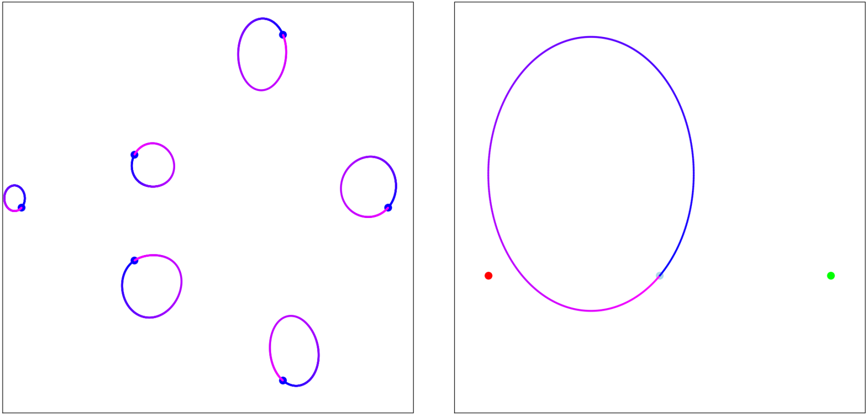


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: ●, ●
Noncritical value: ●

Action of monodromy group

$$z \mapsto f(z)$$

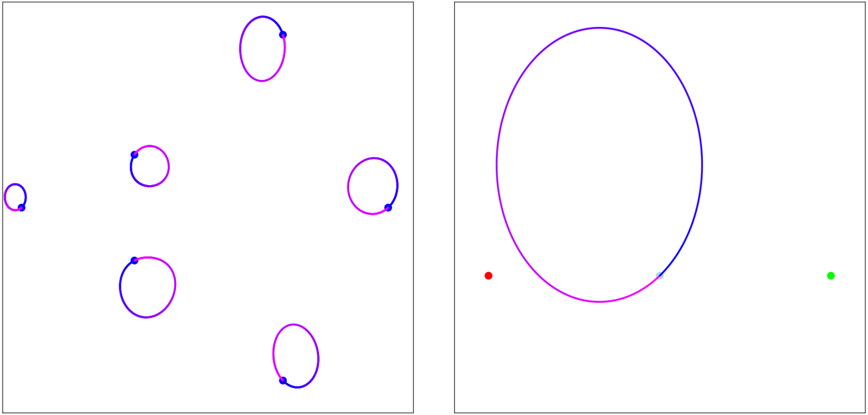


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



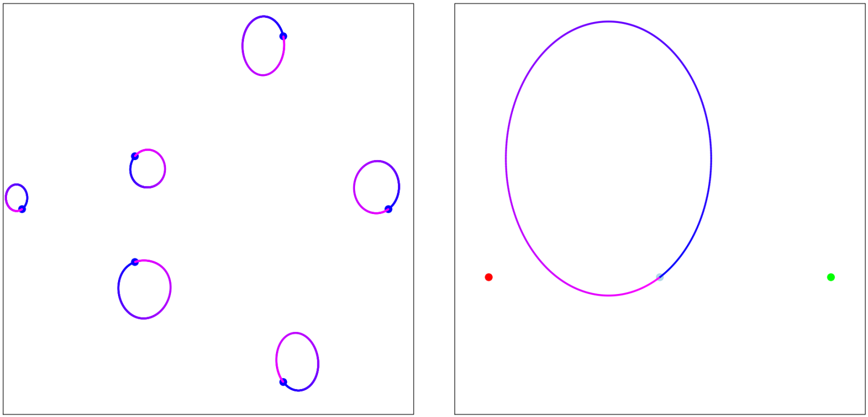
$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on $f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$

Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



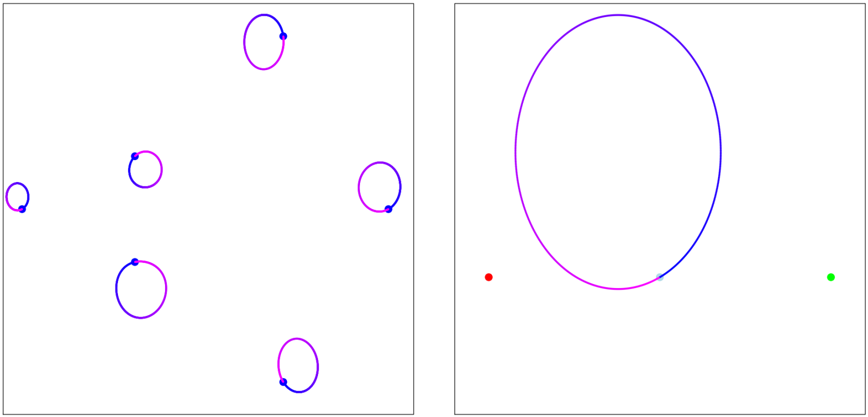
$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on $f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$

Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

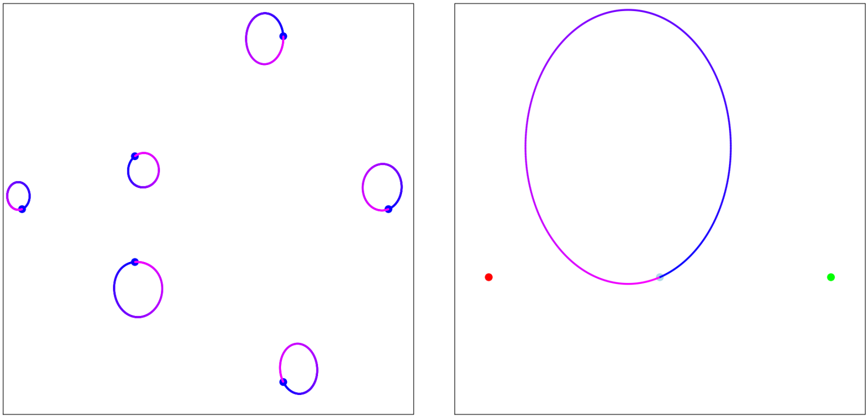


$\pi_1(\mathbb{C} \setminus \{\text{●}, \text{●}\}, \text{●})$ acts on
$f^{-1}(\text{●}) = \{\text{●}, \text{●}, \ldots, \text{●}\}$

Critical values: ●, ●
Noncritical value: ●

Action of monodromy group

$$z \mapsto f(z)$$

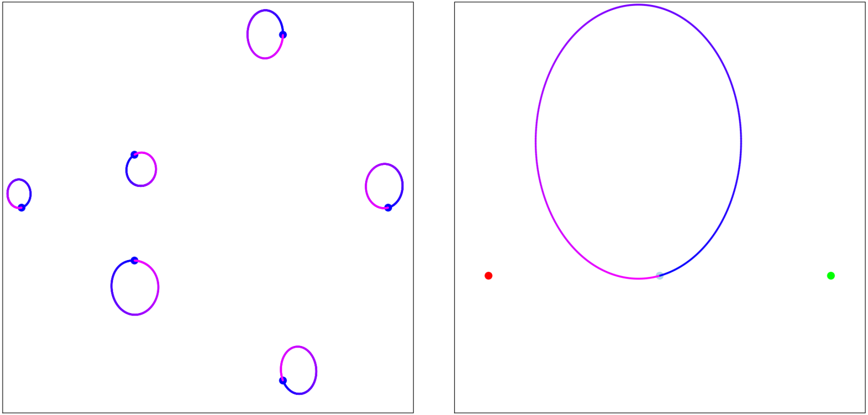


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



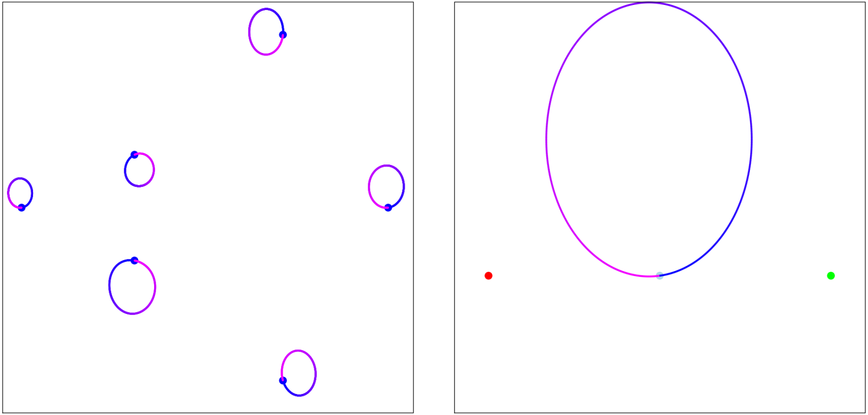
$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on $f^{-1}(\bullet) = \{\bullet, \bullet, \dots, \bullet\}$

Critical values: $\bullet$, $\bullet$

Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

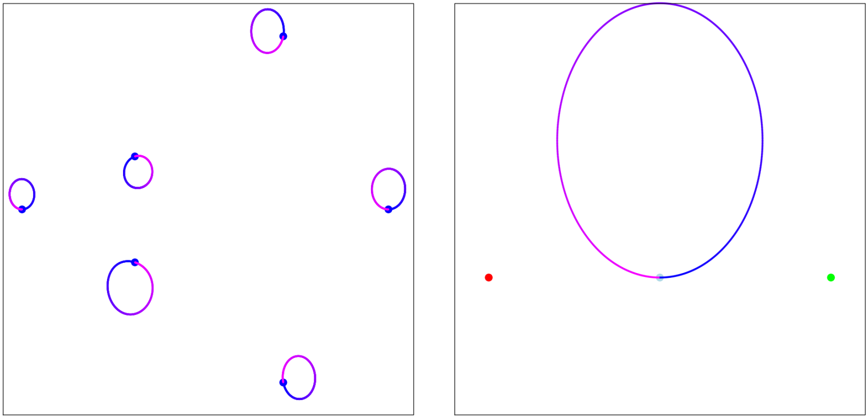


$\pi_1(\mathbb{C} \setminus \{●, ●\}, ●)$ acts on
$f^{-1}(●) = \{●, ●, \ldots, ●\}$

Critical values: ●, ●
Noncritical value: ●

Action of monodromy group

$$z \mapsto f(z)$$

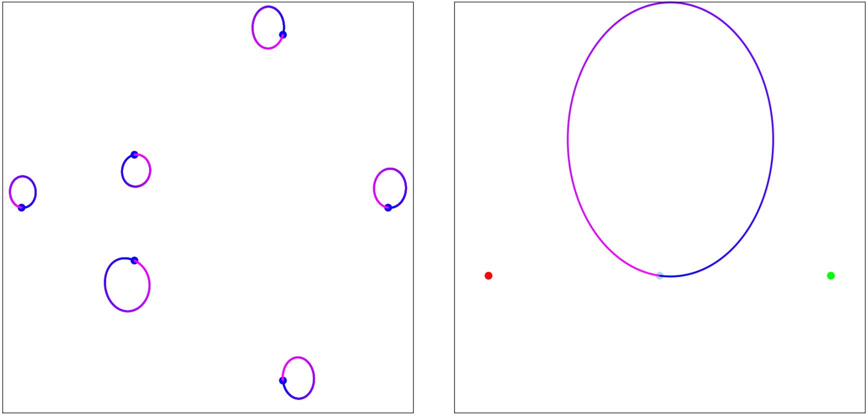


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

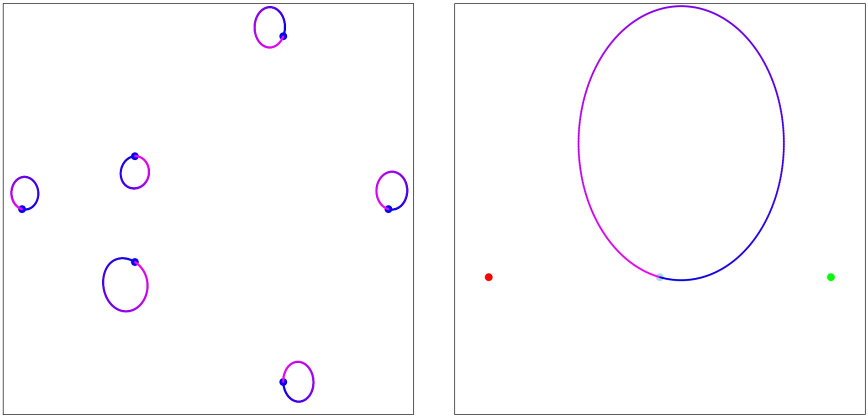


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

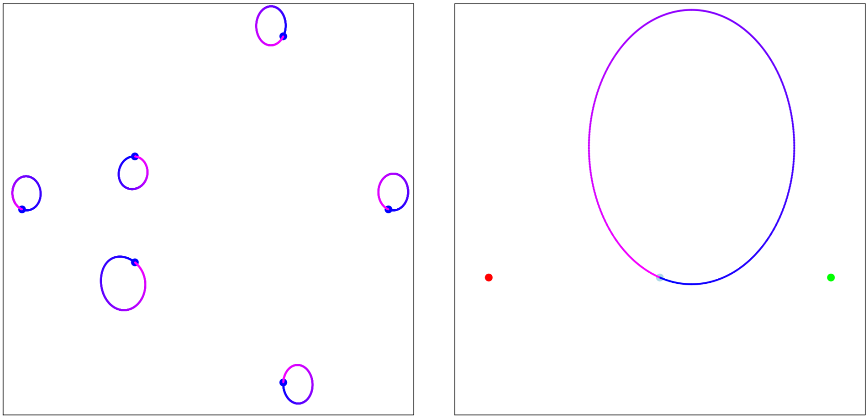


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \dots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

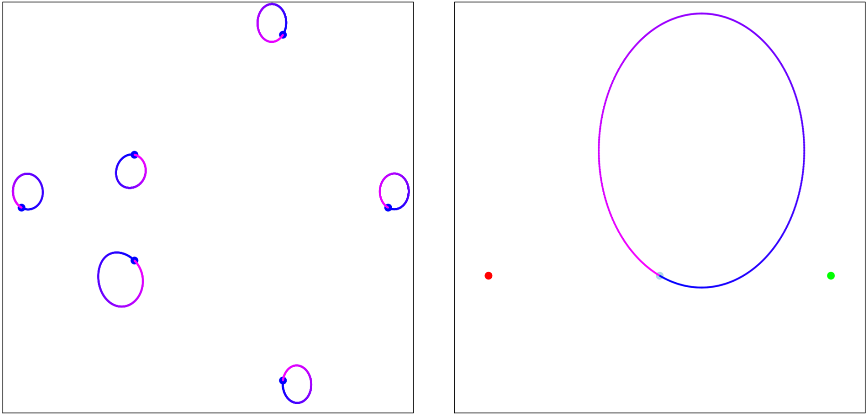


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

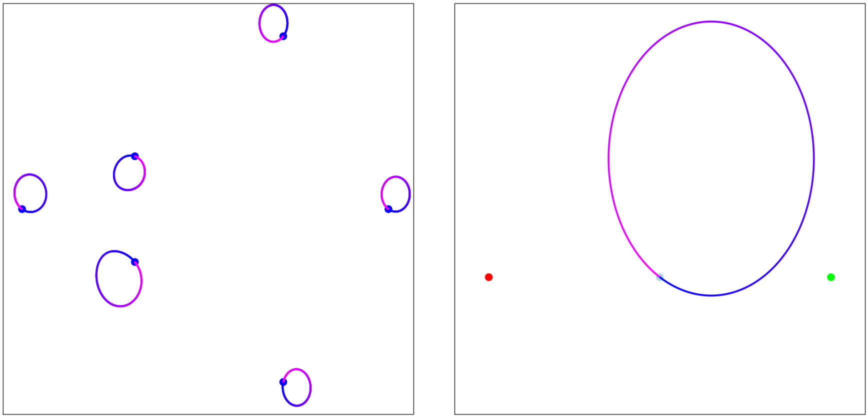


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

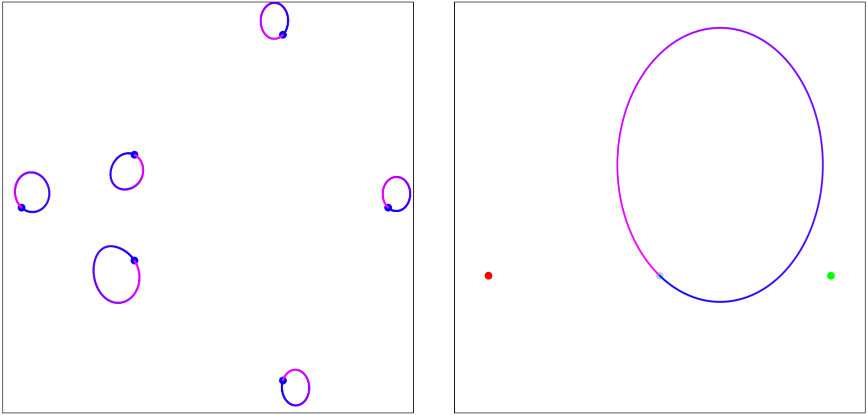


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

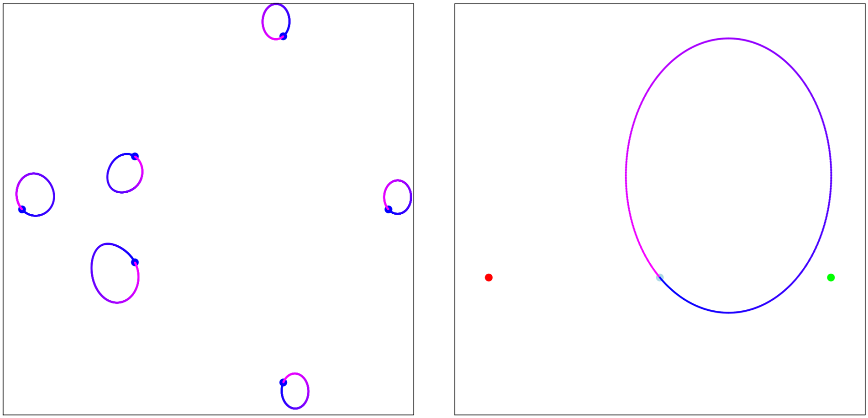


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



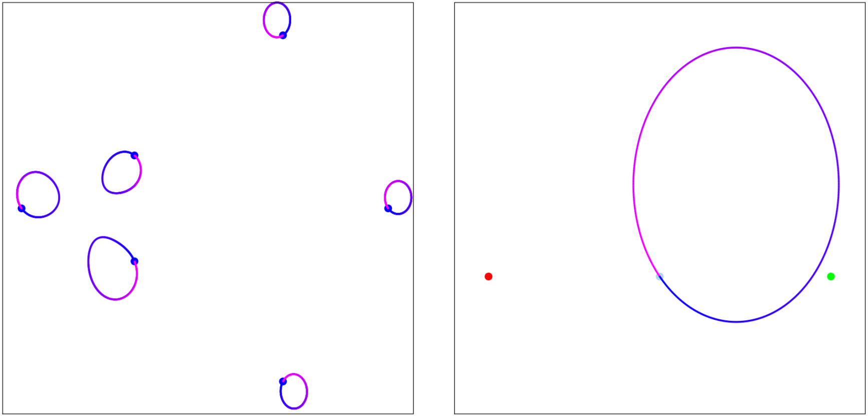
$\pi_1(\mathbb{C} \setminus \{\text{red}, \text{green}\}, \text{light blue})$ acts on $f^{-1}(\text{light blue}) = \{\text{blue}, \text{blue}, \ldots, \text{blue}\}$

Critical values: red, green

Noncritical value: light blue

Action of monodromy group

$$z \mapsto f(z)$$

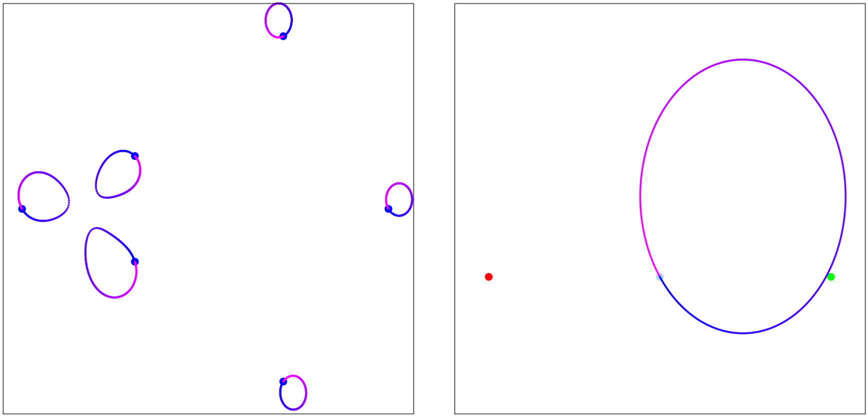


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



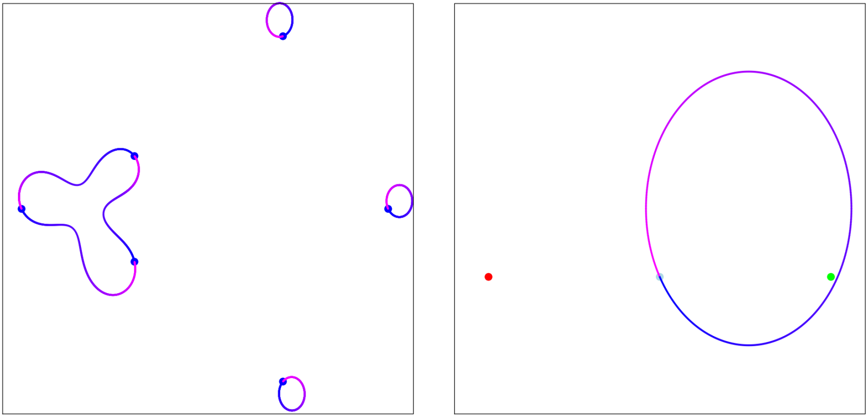
$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on $f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$

Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



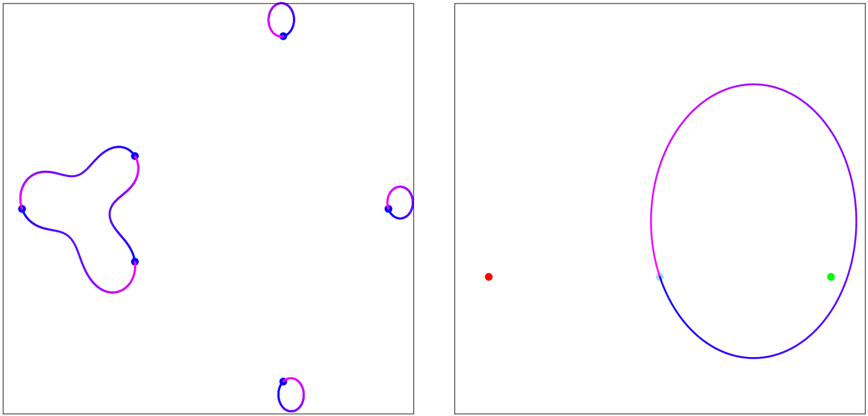
$\pi_1(\mathbb{C} \setminus \{\color{red}\bullet, \color{green}\bullet\}, \color{lightblue}\bullet)$ acts on $f^{-1}(\color{lightblue}\bullet) = \{\color{blue}\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\color{red}\bullet$, $\color{green}\bullet$

Noncritical value: $\color{lightblue}\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

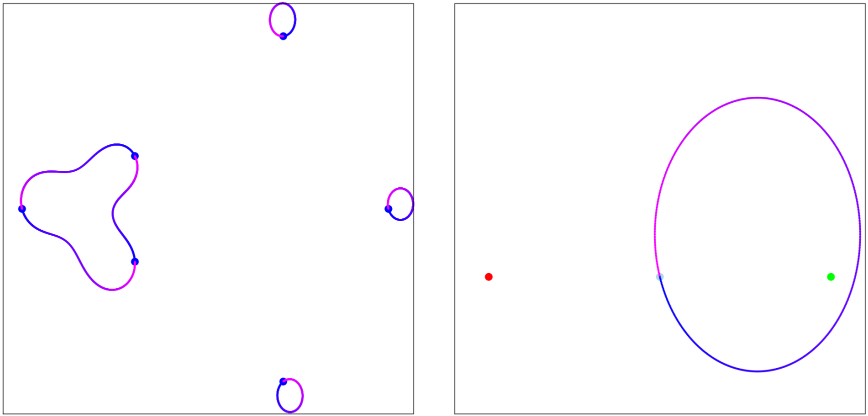


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



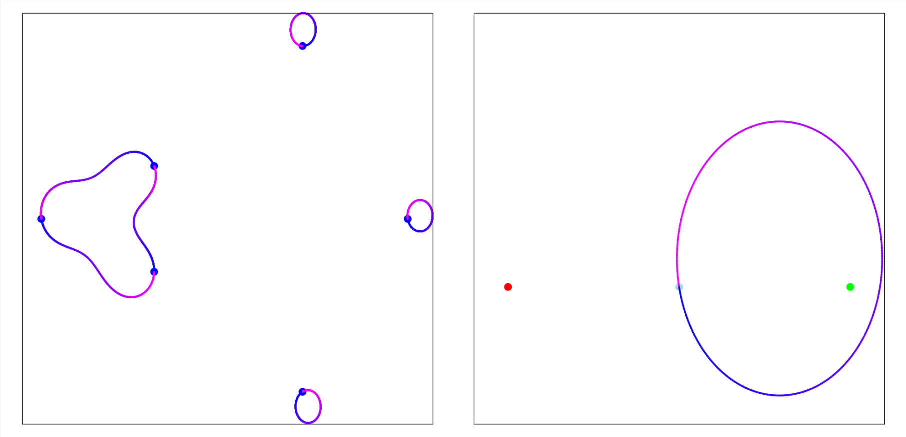
$\pi_1(\mathbb{C} \setminus \{\color{red}{\bullet}, \color{green}{\bullet}\}, \color{lightblue}{\bullet})$ acts on $f^{-1}(\color{lightblue}{\bullet}) = \{\color{blue}{\bullet}, \color{blue}{\bullet}, \ldots, \color{blue}{\bullet}\}$

Critical values: $\color{red}{\bullet}$, $\color{green}{\bullet}$

Noncritical value: $\color{lightblue}{\bullet}$

Action of monodromy group

$$z \mapsto f(z)$$



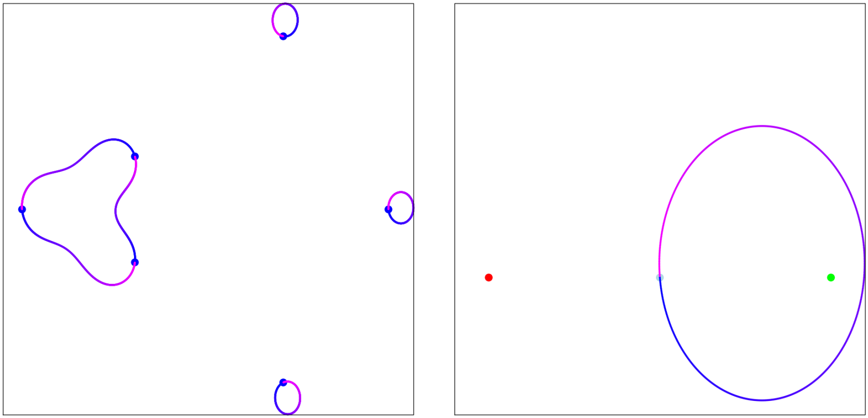
$\pi_1(\mathbb{C} \setminus \{\color{red}\bullet, \color{green}\bullet\}, \color{lightblue}\bullet)$ acts on $f^{-1}(\color{lightblue}\bullet) = \{\color{blue}\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\color{red}\bullet$, $\color{green}\bullet$

Noncritical value: $\color{lightblue}\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

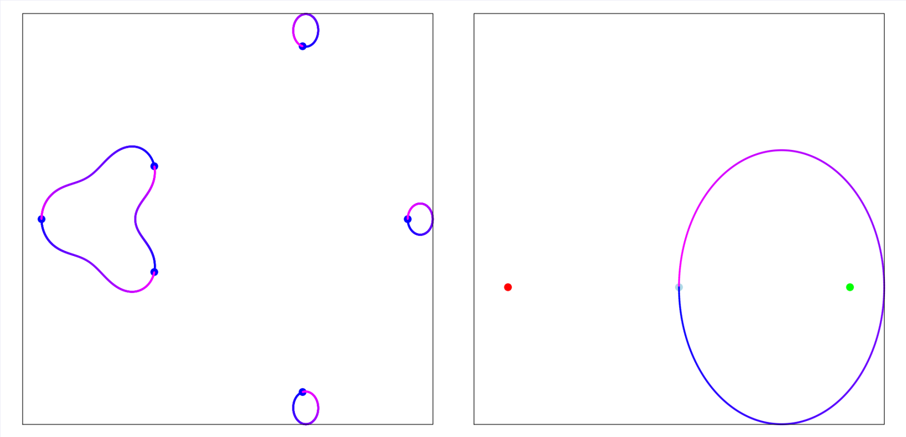


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

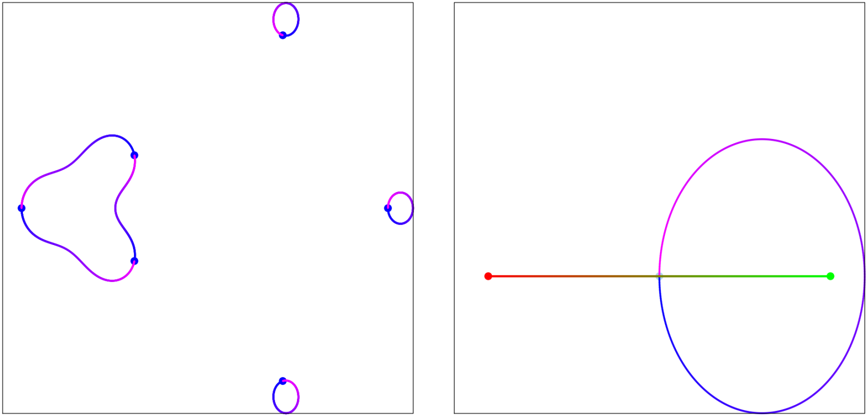


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$

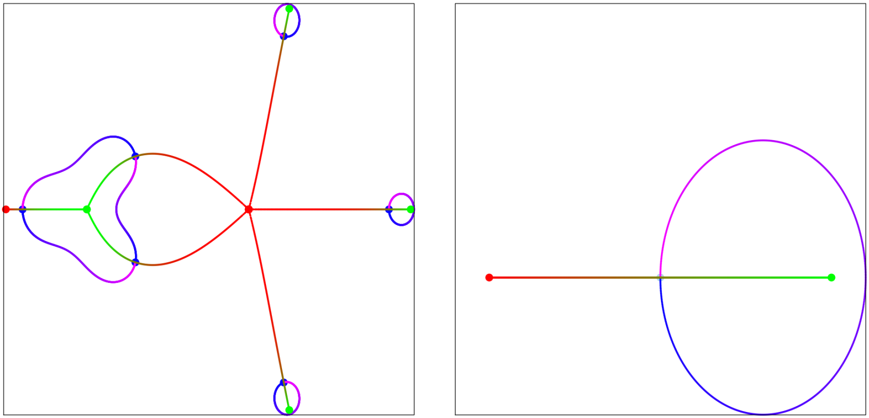


$\pi_1(\mathbb{C} \setminus \{\bullet, \bullet\}, \bullet)$ acts on
$f^{-1}(\bullet) = \{\bullet, \bullet, \ldots, \bullet\}$

Critical values: $\bullet$, $\bullet$
Noncritical value: $\bullet$

Action of monodromy group

$$z \mapsto f(z)$$



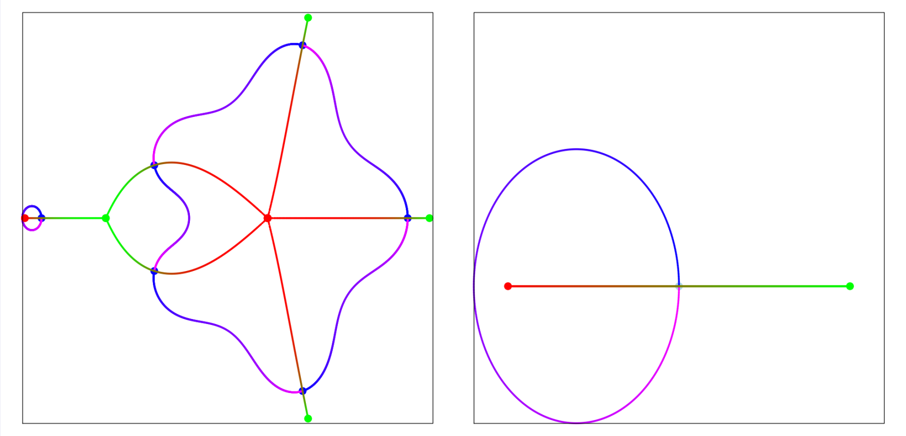
$\pi_1(\mathbb{C} \setminus \{●, ●\}, ●)$ acts on $f^{-1}(●) = \{●, ●, \ldots, ●\}$

Critical values: ●, ●

Noncritical value: ●

Action of monodromy group

$$z \mapsto f(z)$$

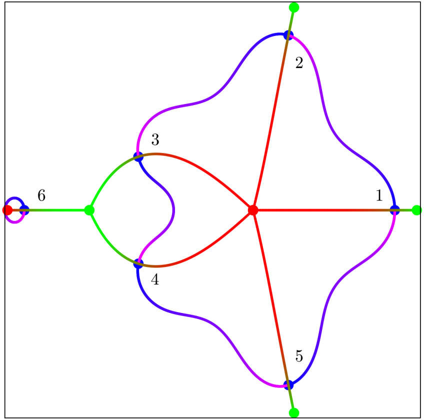


$\pi_1(\mathbb{C} \setminus \{\color{red}{\bullet}, \color{green}{\bullet}\}, \color{lightblue}{\bullet})$ acts on
$f^{-1}(\color{lightblue}{\bullet}) = \{\color{blue}{\bullet}, \color{blue}{\bullet}, \ldots, \color{blue}{\bullet}\}$

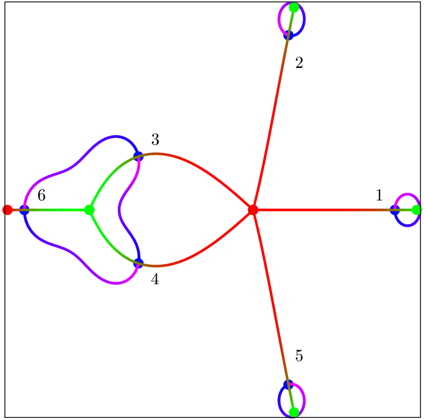
Critical values: $\color{red}{\bullet}$, $\color{green}{\bullet}$

Noncritical value: $\color{lightblue}{\bullet}$

Generators of Mon(f)



$\sigma_1 = (1\,2\,3\,4\,5)$



$\sigma_2 = (3\,6\,4)$

$$\text{Mon}(f) = <\sigma_1, \sigma_2> = \text{Alt}(6)$$

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

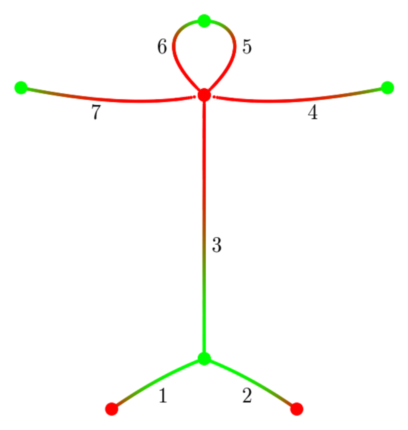
Rational function

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

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

Bipartite graph

$f^{-1}([0, 1])$, n edges



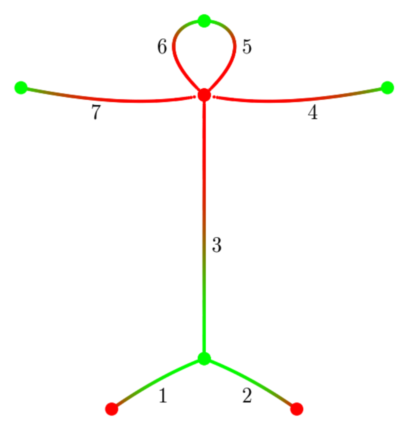
Rational function

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

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

Bipartite graph

$f^{-1}([0, 1])$, n edges



Rational function

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

Generators of Mon(f)

$$\sigma_1 = (1\,2\,3)(5\,6)$$
$$\sigma_2 = (3\,4\,5\,6\,7)$$
$$\sigma_3 = (\sigma_1\sigma_2)^{-1} = (1\,2\,3\,4\,6\,7)$$

Properties of monodromy groups

Riemann's Existence Theorem

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

$\updownarrow$

- $\mathrm{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_r> \leq \mathrm{Sym}(n)$ transitive
- $\sigma_1 \cdot \sigma_2 \cdots \sigma_r = 1$
- $\sum_{i=1}^{r}$ 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

$\updownarrow$

- $\mathrm{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_r> \leq \mathrm{Sym}(n)$ transitive
- $\sigma_1 \cdot \sigma_2 \cdots \sigma_r = 1$
- $\sum_{i=1}^{r}$ number of cycles of $\sigma_i = (r-2)n + 2$

Examples

$f(z)$	r	$\mathrm{Mon}(f)$
z^n	2	$<(1\,2\,\ldots\,n)>$ cyclic

Properties of monodromy groups

Riemann's Existence Theorem

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

$\updownarrow$

- $\mathrm{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_r> \leq \mathrm{Sym}(n)$ transitive
- $\sigma_1 \cdot \sigma_2 \cdots \sigma_r = 1$
- $\sum_{i=1}^{r}$ number of cycles of $\sigma_i = (r-2)n + 2$

Examples

$f(z)$	r	$\mathrm{Mon}(f)$
z^n	2	$<(1\,2\,\ldots\,n)>$ 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

$$\updownarrow$$

- $\mathrm{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_r> \leq \mathrm{Sym}(n)$ transitive
- $\sigma_1 \cdot \sigma_2 \cdots \sigma_r = 1$
- $\sum_{i=1}^{r}$ number of cycles of $\sigma_i = (r-2)n + 2$

Examples

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

Properties of monodromy groups

Riemann's Existence Theorem

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

$\updownarrow$

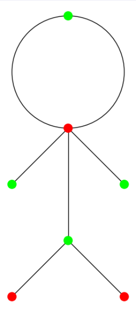
- $\mathrm{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_r> \leq \mathrm{Sym}(n)$ transitive
- $\sigma_1 \cdot \sigma_2 \cdots \sigma_r = 1$
- $\sum_{i=1}^{r}$ number of cycles of $\sigma_i = (r-2)n + 2$

Examples

$f(z)$	r	$\mathrm{Mon}(f)$
z^n	2	$<(1\,2\,\ldots\,n)>$ cyclic
$f(\cos\phi) = \cos n\phi$	3	dihedral group of order $2n$
"random", degree n	$2(n-1)$	$\mathrm{Sym}(n)$
?	3	Aut(Higman–Sims), degree 100

From the dessin to the rational function

Bipartite graph



Translate ramification data

$$f(z) - 0 = \frac{(z-\alpha)^5(z^2+\beta z+\gamma)}{z}$$

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

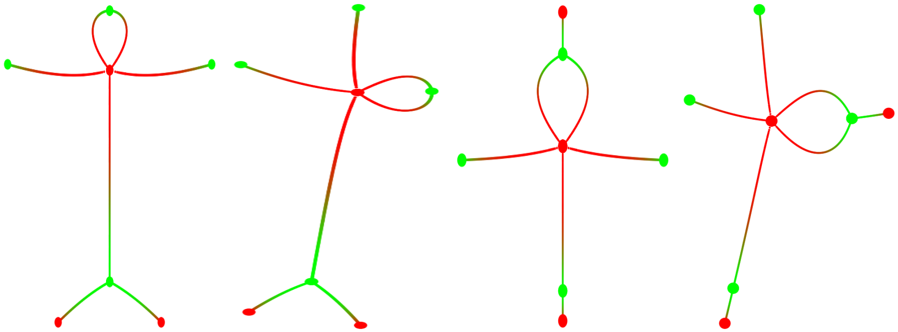
Polynomial system

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

From the dessin to the rational function

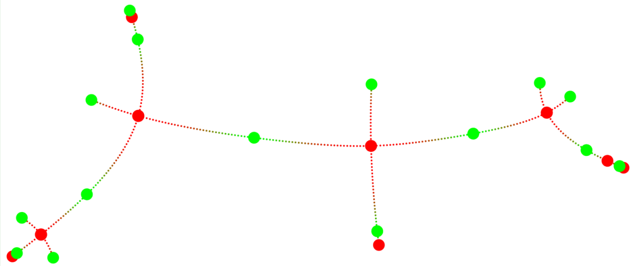
Problem

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



From the dessin to the rational function

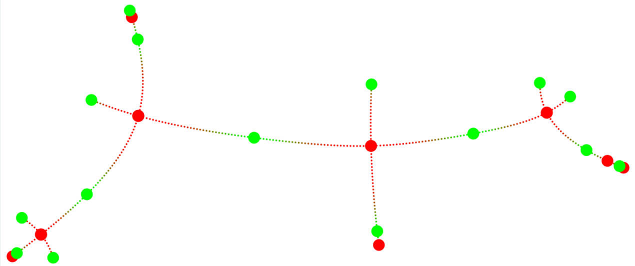
Challenge: Mathieu group $M_{23} \leq \mathrm{Sym}(23)$



$n = 23$
$|M_{23}| = 10200960$
$f(z) \in K[z]$
$[K : \mathbb{Q}(\sqrt{-23})] \leq 2$
$f(z) = ?$

From the dessin to the rational function

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

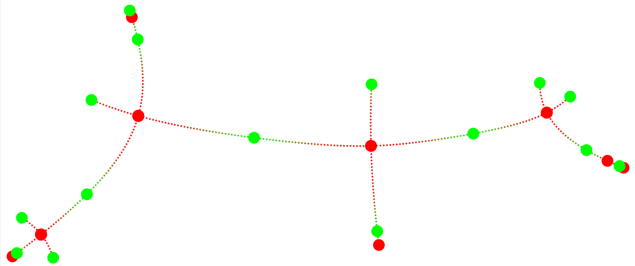


$n = 23$
$|M_{23}| = 10200960$
$f(z) \in K[z]$
$[K : \mathbb{Q}(\sqrt{-23})] \leq 2$
$f(z) = ?$

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

From the dessin to the rational function

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

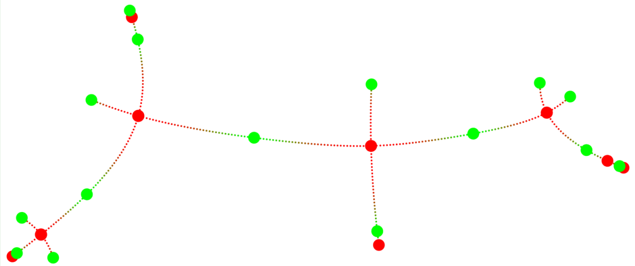


$n = 23$
$|M_{23}| = 10200960$
$f(z) \in K[z]$
$[K : \mathbb{Q}(\sqrt{-23})] \leq 2$
$f(z) = ?$

- (*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.

From the dessin to the rational function

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



$n = 23$
$|M_{23}| = 10200960$
$f(z) \in K[z]$
$[K : \mathbb{Q}(\sqrt{-23})] \leq 2$
$f(z) = ?$

- (*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.
- (*M. 2015*) Formal power series and group action yield a polynomial system which can be solved directly.

Invariant curves

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) $\mathbb{C}(g(z)) = \mathbb{C}(\bar{g}(z))$.

Invariant curves

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*
- $\mathbb{R} \to \mathbb{R}$, $a \mapsto f(g(a))$ *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* $\lambda \in \mathbb{C}(z)$.

Invariant curves

Proposition

Given

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

Then $M = \sigma M \sigma^{-1}$ for each subgroup M with $G_1 \leq M \leq G$.

Invariant curves

Proof of the theorem (sketch).

- W.l.o.g. $f(g(z)) = \frac{p(z)}{q(z)}$ with $p, q \in \mathbb{R}[z]$ relatively prime, and
  - $\deg p > \deg q$
  - $p(z) = \prod(z - \alpha_i)$ separable
  - $\alpha_1 \in \mathbb{R}$
  - $\alpha_i \notin \mathbb{R}$ for $i \geq 2$

Invariant curves

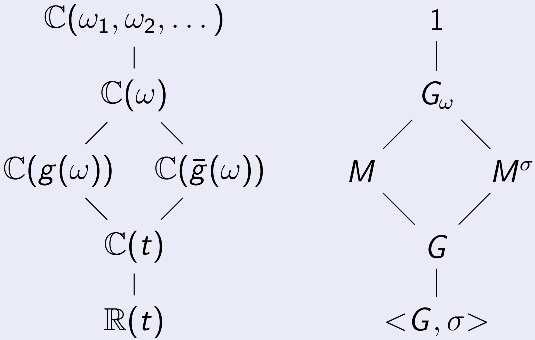
Proof of the theorem (sketch).

- W.l.o.g. $f(g(z)) = \frac{p(z)}{q(z)}$ with $p, q \in \mathbb{R}[z]$ relatively prime, and
  - $\deg p > \deg q$
  - $p(z) = \prod(z - \alpha_i)$ separable
  - $\alpha_1 \in \mathbb{R}$
  - $\alpha_i \notin \mathbb{R}$ for $i \geq 2$
- Hensel's Lemma: $p(z) - tq(z) = \prod(z - \omega_i)$ with
  - $\omega = \omega_1 \in \mathbb{R}[[t]]$
  - $\omega_i \in \mathbb{C}[[t]] \setminus \mathbb{R}[[t]]$ 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 $i \geq 2$
$t = \frac{p(\omega)}{q(\omega)} = f(g(\omega)) = \bar{f}(\bar{g}(\omega))$
$\sigma =$ complex conjugation on coefficients of $\mathbb{C}((t))$, restricted to $\mathbb{C}(\omega_1, \omega_2, \dots) \subset \mathbb{C}((t))$



□