Gruppentheoretische Methoden in der Zahlentheorie und Geometrie rationaler Funktionen

Peter Müller

Magdeburg, 3. Dezember 2015

Überblick

Algebraische Kurven, getrennte Variablen (Cassels, Birch)

Selten zerlegbar, wie in

$$\underbrace{(4 - 4x^2 + x^4)}_{f(x)} - \underbrace{(4y^2 - y^4)}_{g(y)} = (x^2\sqrt{2}xy + y^2 - 2)(x^2 + \sqrt{2}xy + y^2 - 2)$$

Funktionale Zerlegungen (Ritt)

Maximale funktionale Zerlegungen rationaler Funktionen

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

Permutationspolynome modulo Primzahlen (Schur)

Für welche Polynome $f(x) \in \mathbb{Z}[x]$ ist

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \\ a &\mapsto f(a) \end{aligned}$$

bijektiv für unendlich viele Primzahlen p?

Wertemengen rationaler Funktionen (Birch, Swinnerton-Dyer, Cohen)

$\mathbb{F}_q$ endlicher Körper, $f(x) \in \mathbb{F}_q(x)$ „zufällig“, $n = \deg f$:

$$\frac{1}{q}|f(\mathbb{F}_q)| = \underbrace{1 - \frac{1}{2!} + \frac{1}{3!} - \cdots - (-1)^n \frac{1}{n!}}_{\text{Anteil Permutationen in Sym}(n) \text{ mit Fixpunkt}} + O_n(q^{-1/2})$$

Invariante Kurven (Fatou, Eremenko)

$f(z), g(z) \in \mathbb{C}(z)$ rationale Funktionen mit $f(g(z)) \in \mathbb{R}(z)$.
Kurve $\Gamma = g(\mathbb{R})$ ist invariant unter $g \circ f$:

$$(g \circ f)(\Gamma) = g(\underbrace{f(g(\mathbb{R}))}_{\subset \mathbb{R}}) \subseteq g(\mathbb{R}) = \Gamma$$

- Kann Γ eine Jordankurve $\neq$ Kreis sein?

Invariante Kurven (Fatou, Eremenko)

$f(z), g(z) \in \mathbb{C}(z)$ rationale Funktionen mit $f(g(z)) \in \mathbb{R}(z)$.
Kurve $\Gamma = g(\mathbb{R})$ ist invariant unter $g \circ f$:

$$(g \circ f)(\Gamma) = g(\underbrace{f(g(\mathbb{R}))}_{\subset \mathbb{R}}) \subseteq g(\mathbb{R}) = \Gamma$$

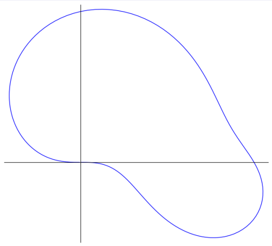
- Kann Γ eine Jordankurve $\neq$ Kreis sein? Ja (M. 2015):

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

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

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

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



Invariante Kurven (Fatou, Eremenko)

$f(z), g(z) \in \mathbb{C}(z)$ rationale Funktionen mit $f(g(z)) \in \mathbb{R}(z)$.
Kurve $\Gamma = g(\mathbb{R})$ ist invariant unter $g \circ f$:

$$(g \circ f)(\Gamma) = g(\underbrace{f(g(\mathbb{R}))}_{\subset \mathbb{R}}) \subseteq g(\mathbb{R}) = \Gamma$$

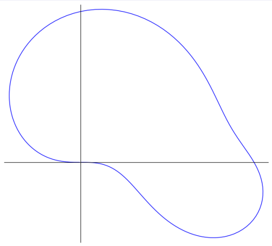
- Kann Γ eine Jordankurve $\neq$ Kreis sein? Ja (M. 2015):

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

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

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

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



- Kann $g \circ f$ injektiv auf Γ sein? Nein (M. 2015)

Monodromiegruppen (Riemann)

$f(z) \in \mathbb{C}(z)$ rationale Funktion vom Grad n $\longleftrightarrow$ $\mathrm{Mon}(f) \leq \mathrm{Sym}(n)$ Untergruppe

Monodromiegruppen (Riemann)

$f(z) \in \mathbb{C}(z)$ rationale Funktion vom Grad n $\longleftrightarrow$ $\mathrm{Mon}(f) \leq \mathrm{Sym}(n)$ Untergruppe

Kritische Werte

$$a \in \mathbb{C} \cup \{\infty\} \text{ kritischer Wert}$$
$$\Leftrightarrow$$
$$|f^{-1}(a)| < \deg f$$
$$\Leftrightarrow$$
$$f(z) - a \text{ hat mehrfache Nullstelle.}$$

Monodromiegruppen (Riemann)

$f(z) \in \mathbb{C}(z)$ rationale Funktion vom Grad n	$\longleftrightarrow$	$\mathrm{Mon}(f) \leq \mathrm{Sym}(n)$ Untergruppe

Kritische Werte

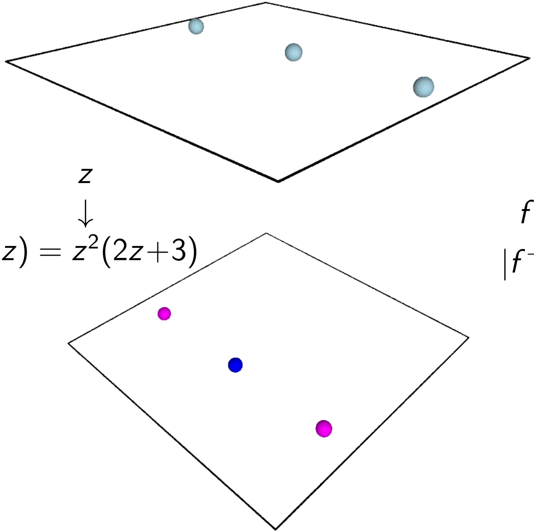
$$a \in \mathbb{C} \cup \{\infty\} \text{ kritischer Wert}$$
$$\Leftrightarrow$$
$$|f^{-1}(a)| < \deg f$$
$$\Leftrightarrow$$
$$f(z) - a \text{ hat mehrfache Nullstelle.}$$

Beispiel

$$f(z) = z^2(2z+3) \qquad f(z) - 1 = (z+1)^2(2z-1)$$

Kritische Werte: 0, 1 und ∞.

Operation der Monodromiegruppe

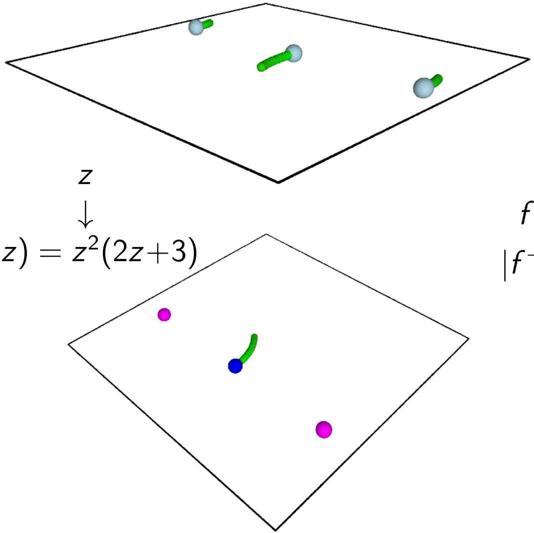


$$z \downarrow f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

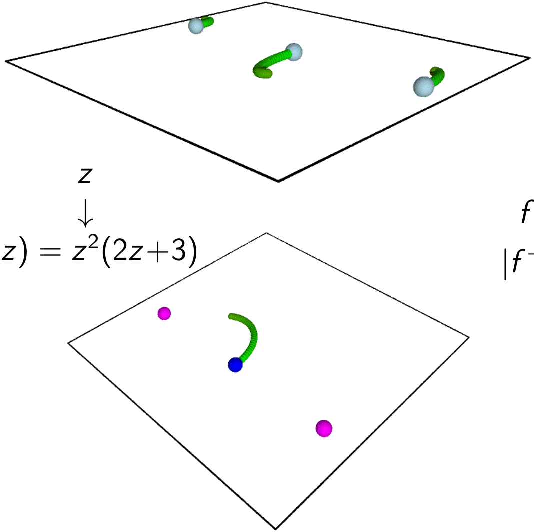


$$z \downarrow f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



z

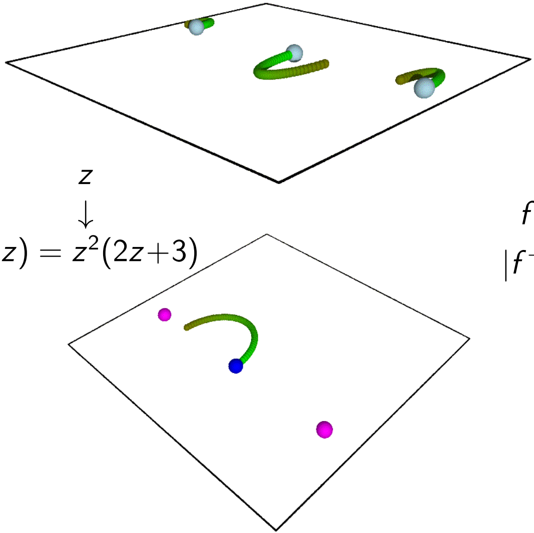
$\downarrow$

$f(z) = z^2(2z+3)$

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

$|f^{-1}(\bullet)| < 3$

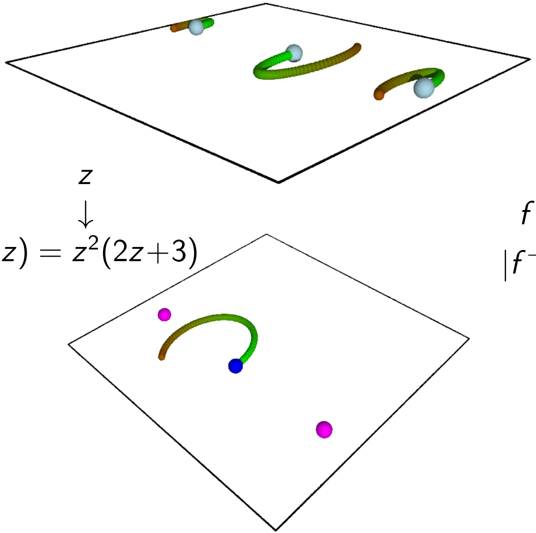
Operation der Monodromiegruppe



$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$

$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$
$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

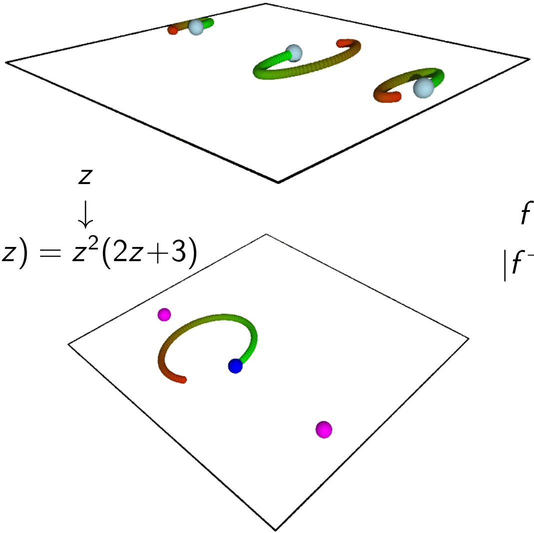


$$z \downarrow f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

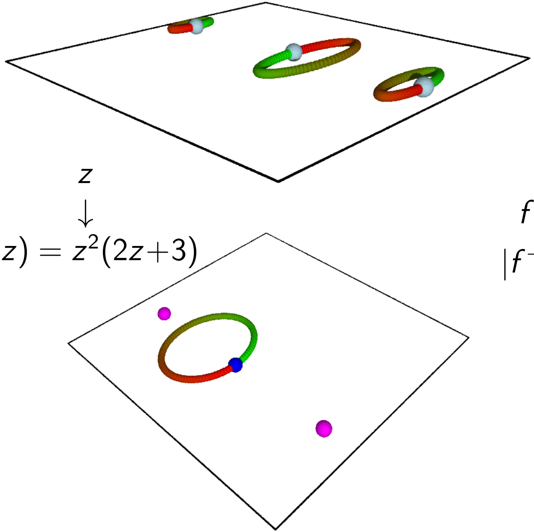
Operation der Monodromiegruppe



$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$

$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$
$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

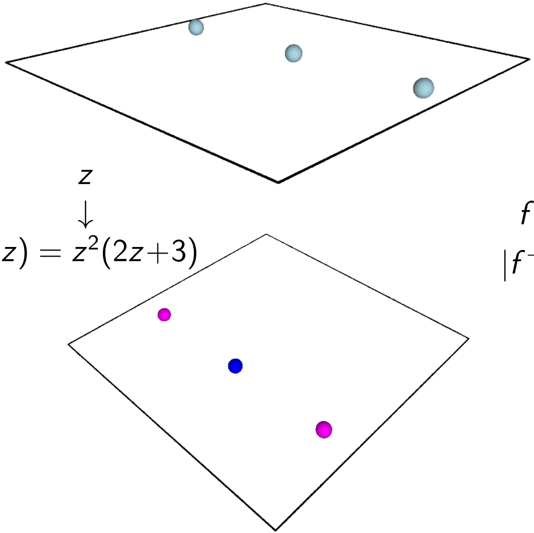


$$z \downarrow f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

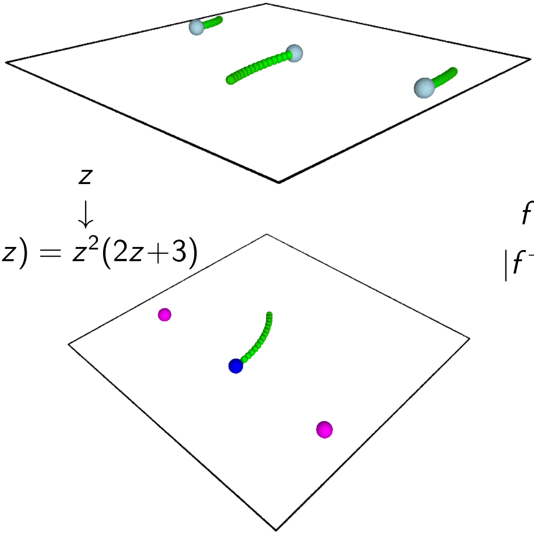


$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

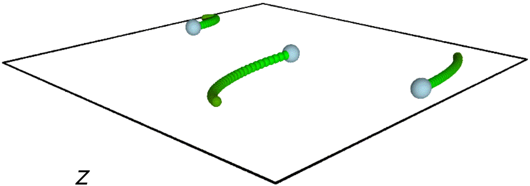


$$z \downarrow f(z) = z^2(2z+3)$$

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

$|f^{-1}(\bullet)| < 3$

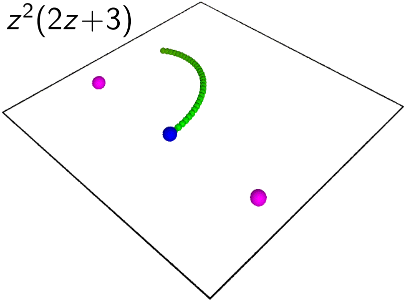
Operation der Monodromiegruppe



z

$\downarrow$

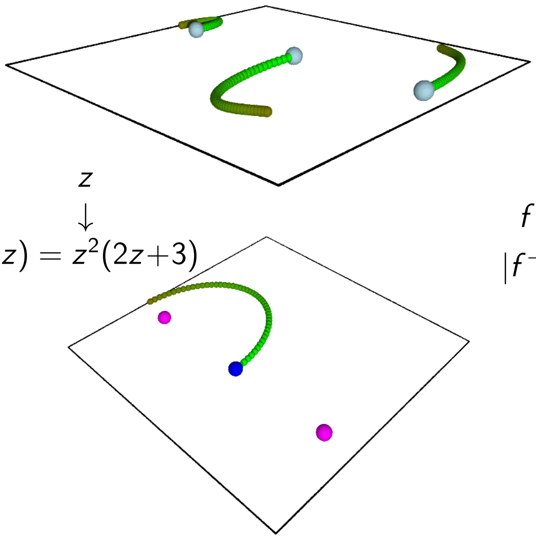
$f(z) = z^2(2z+3)$



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

$|f^{-1}(\bullet)| < 3$

Operation der Monodromiegruppe

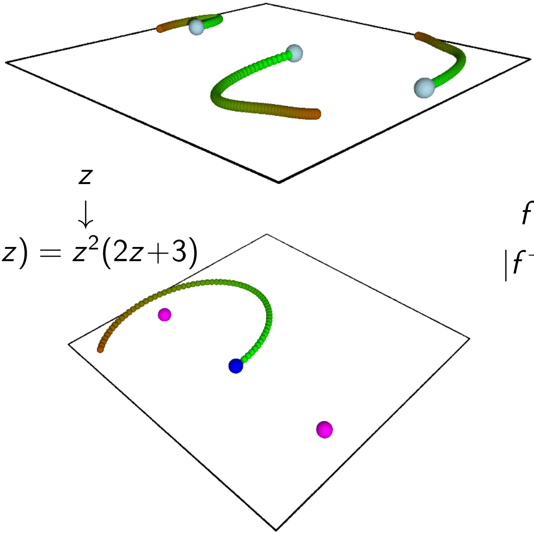


$$z \downarrow f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

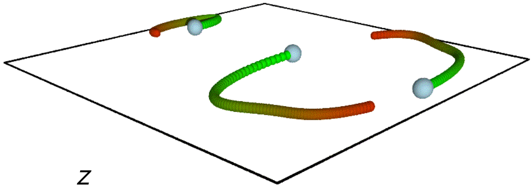
Operation der Monodromiegruppe



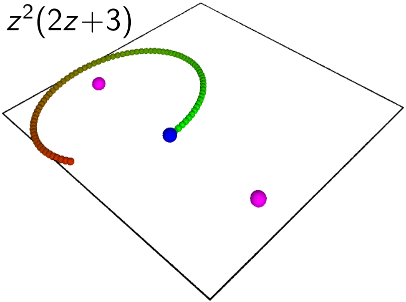
$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

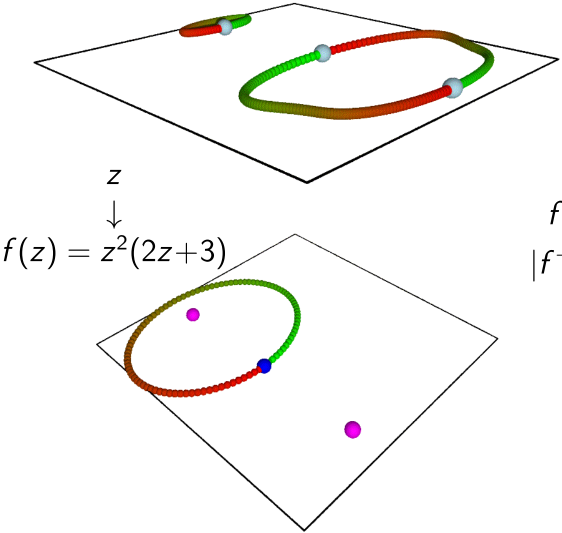


$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$



$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$
$$|f^{-1}(\bullet)| < 3$$

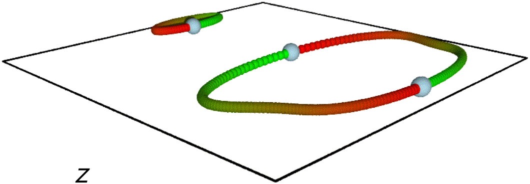
Operation der Monodromiegruppe



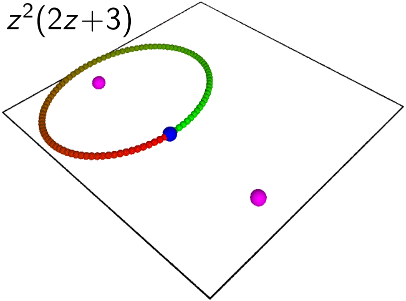
$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



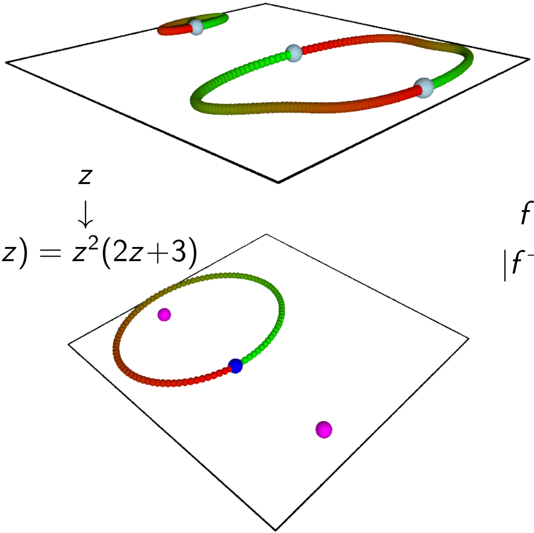
$$z \downarrow f(z) = z^2(2z+3)$$



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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

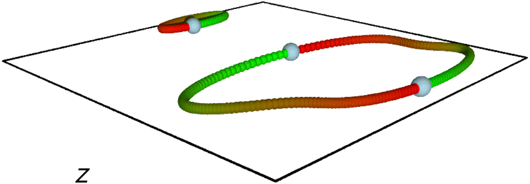


$$z \\ \downarrow \\ f(z) = z^2(2z+3)$$

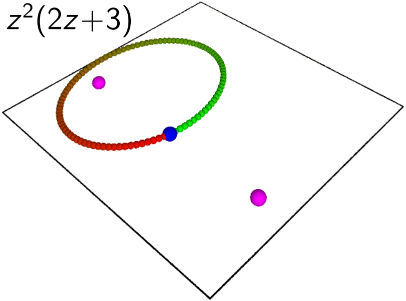
$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

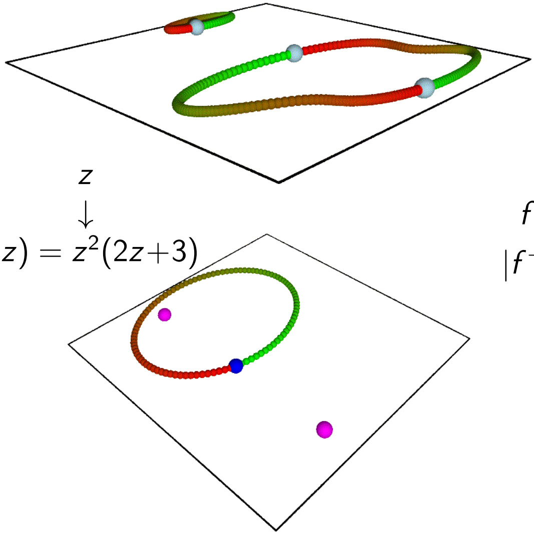


$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$



$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$
$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



z

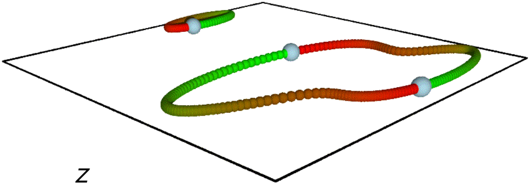
$\downarrow$

$f(z) = z^2(2z+3)$

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

$|f^{-1}(\bullet)| < 3$

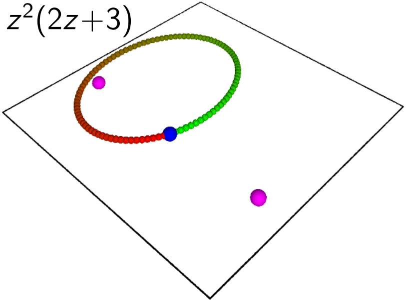
Operation der Monodromiegruppe



z

$\downarrow$

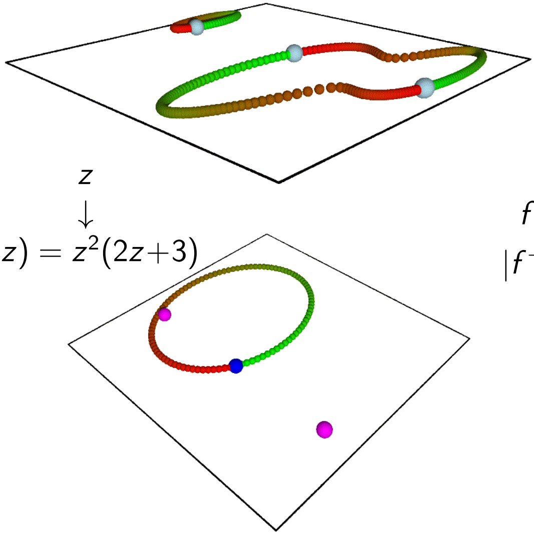
$f(z) = z^2(2z+3)$



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

$|f^{-1}(\bullet)| < 3$

Operation der Monodromiegruppe

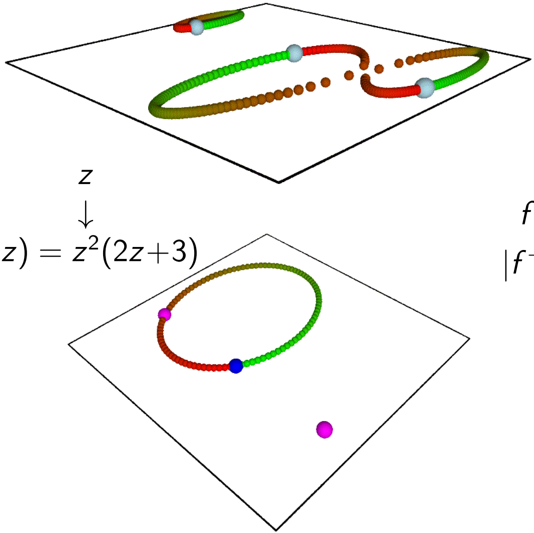


$$z \downarrow f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

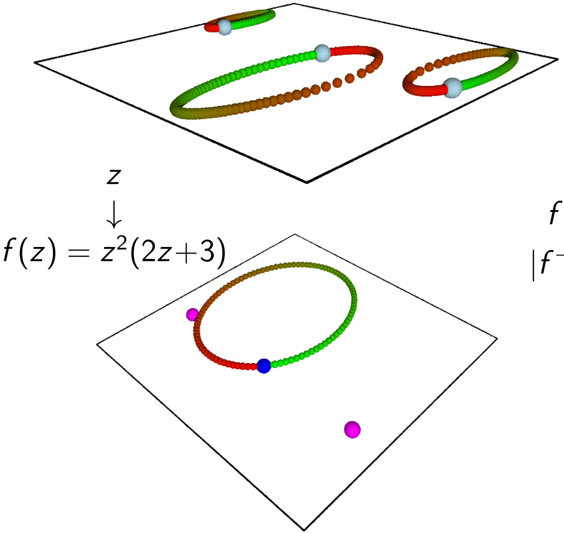


$$z \downarrow f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

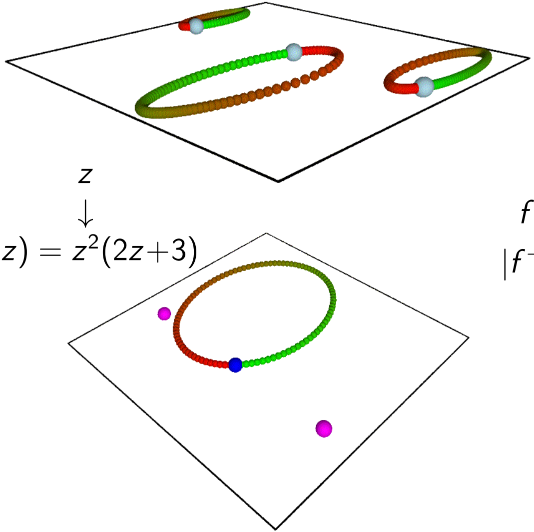
Operation der Monodromiegruppe



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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



z

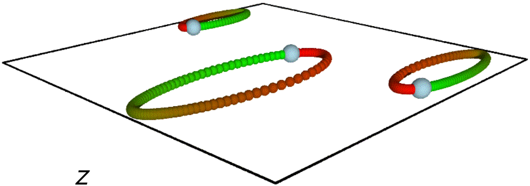
$\downarrow$

$f(z) = z^2(2z+3)$

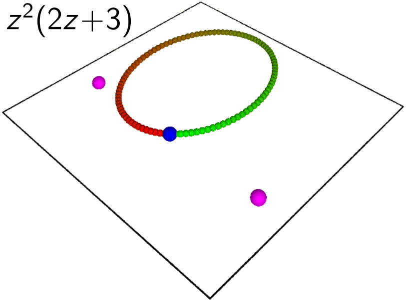
$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$

$|f^{-1}(\bullet)| < 3$

Operation der Monodromiegruppe



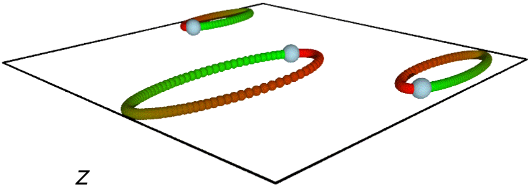
$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$



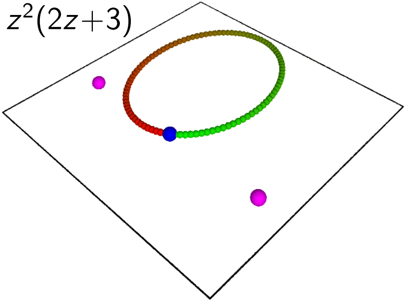
$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



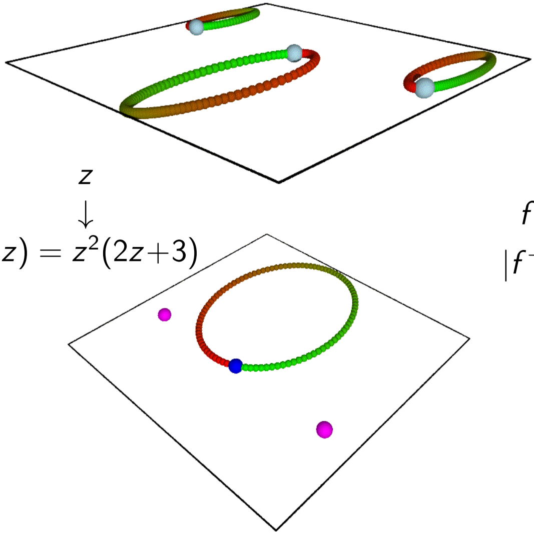
$$z \downarrow f(z) = z^2(2z+3)$$



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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

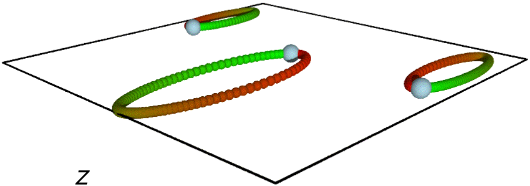


$$z \downarrow f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

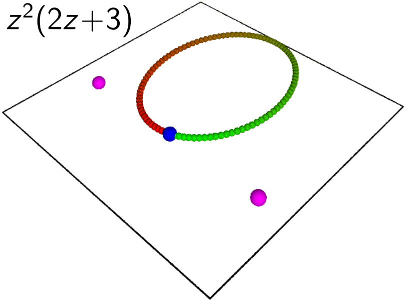
Operation der Monodromiegruppe



z

$\downarrow$

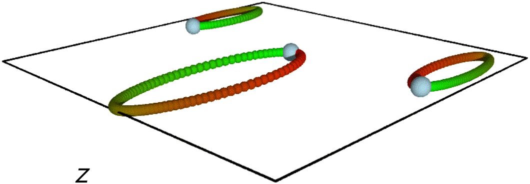
$f(z) = z^2(2z+3)$



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

$|f^{-1}(\bullet)| < 3$

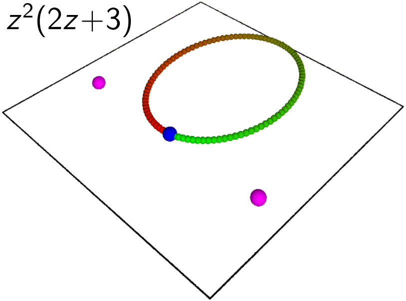
Operation der Monodromiegruppe



z

$\downarrow$

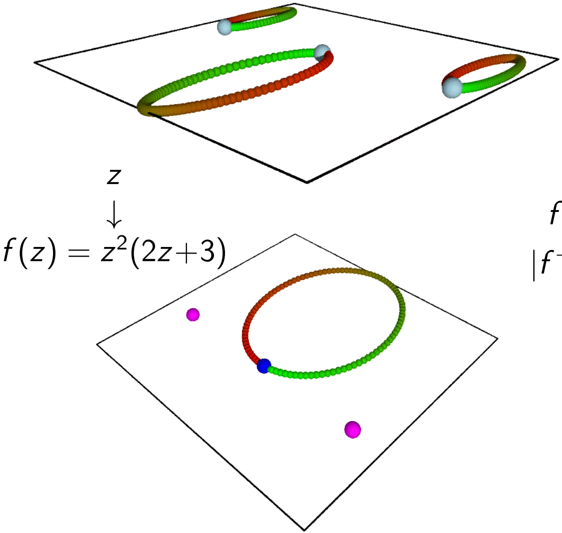
$f(z) = z^2(2z+3)$



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

$|f^{-1}(\bullet)| < 3$

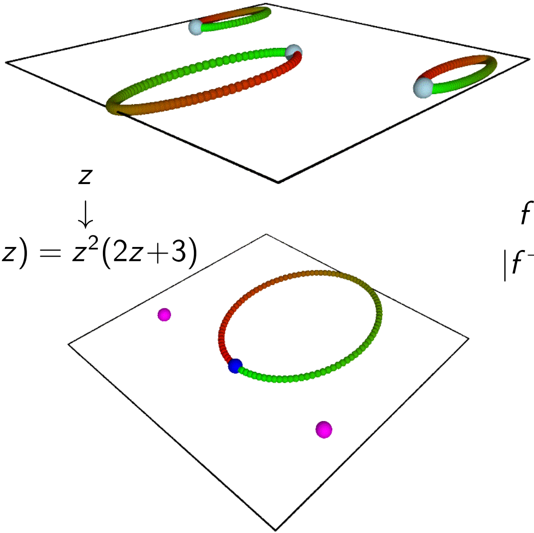
Operation der Monodromiegruppe



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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

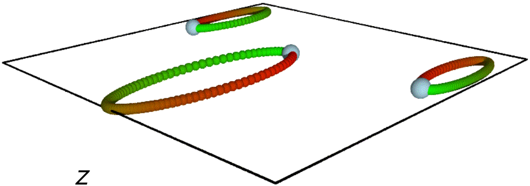


$$z \downarrow f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

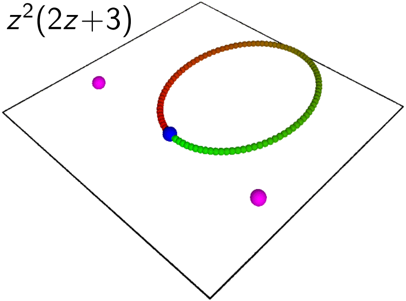
Operation der Monodromiegruppe



z

$\downarrow$

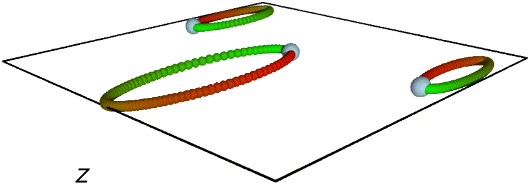
$f(z) = z^2(2z+3)$



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

$|f^{-1}(\bullet)| < 3$

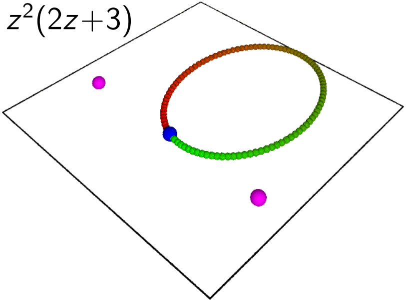
Operation der Monodromiegruppe



z

$\downarrow$

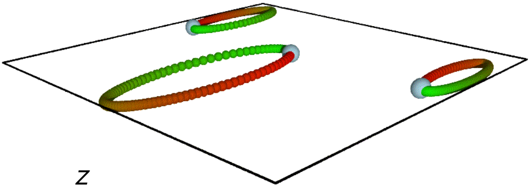
$f(z) = z^2(2z+3)$



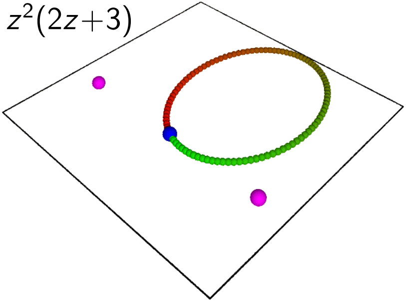
$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$

$|f^{-1}(\bullet)| < 3$

Operation der Monodromiegruppe

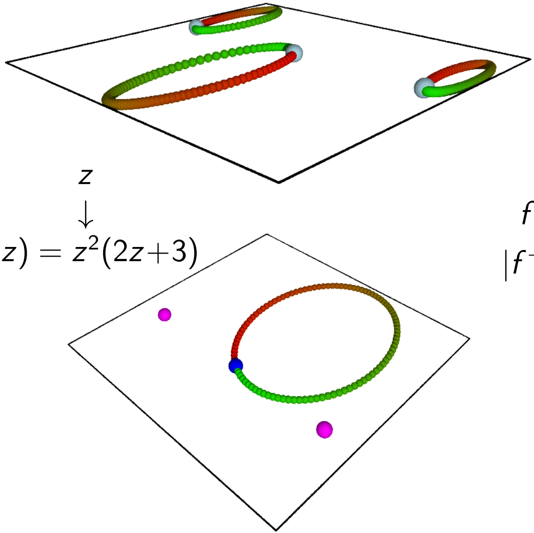


$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$



$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$
$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



z

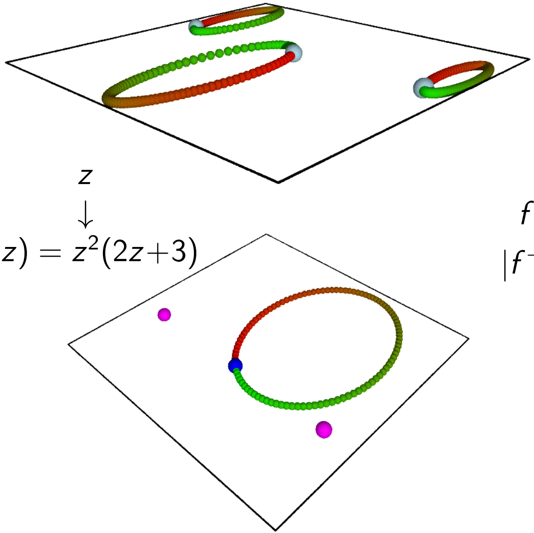
$\downarrow$

$f(z) = z^2(2z+3)$

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

$|f^{-1}(\bullet)| < 3$

Operation der Monodromiegruppe

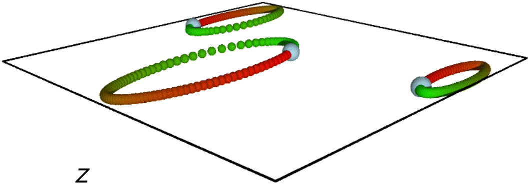


$$z \downarrow f(z) = z^2(2z+3)$$

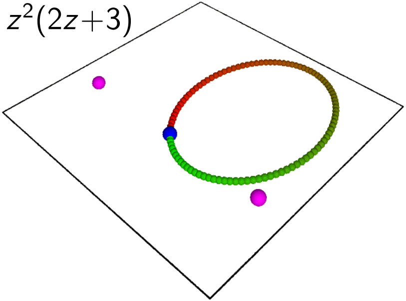
$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



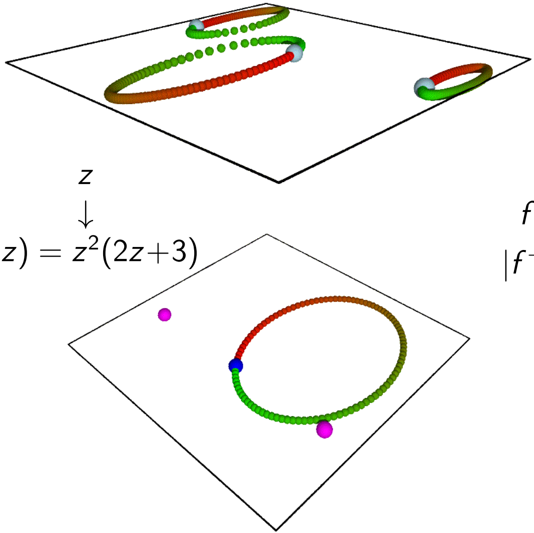
$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$



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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



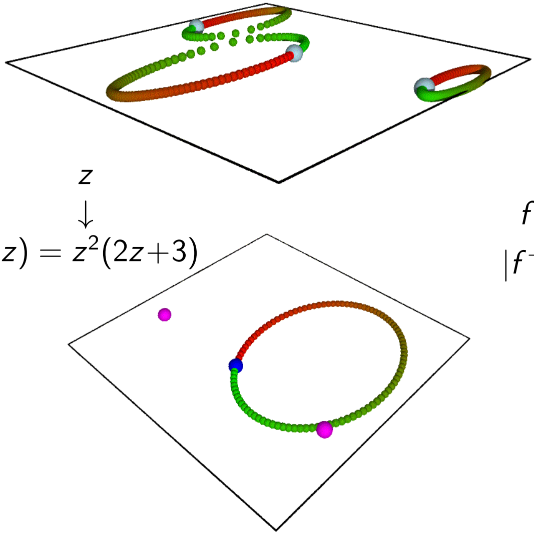
$$z \downarrow$$

$$f(z) = z^2(2z+3)$$

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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe

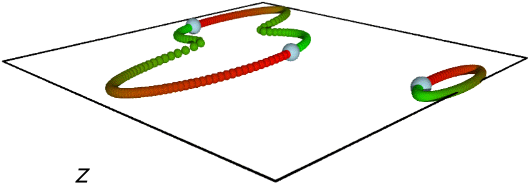


$$z \downarrow f(z) = z^2(2z+3)$$

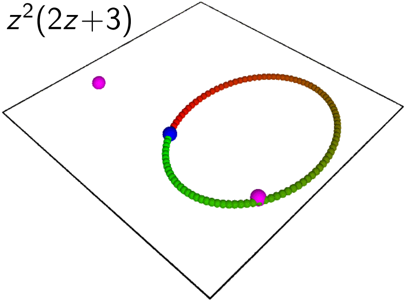
$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



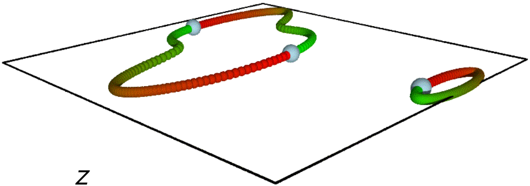
$$z \downarrow f(z) = z^2(2z+3)$$



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

$|f^{-1}(\bullet)| < 3$

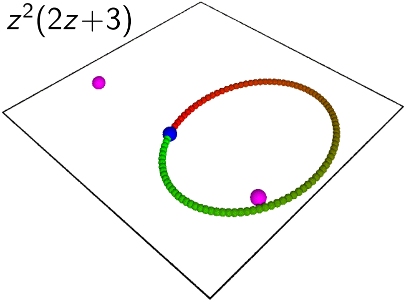
Operation der Monodromiegruppe



z

$\downarrow$

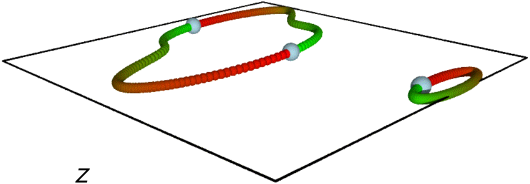
$f(z) = z^2(2z+3)$



$f^{-1}(\textcolor{blue}{\bullet}) = \{\textcolor{lightblue}{\bullet}, \textcolor{lightblue}{\bullet}, \textcolor{lightblue}{\bullet}\}$

$|f^{-1}(\textcolor{magenta}{\bullet})| < 3$

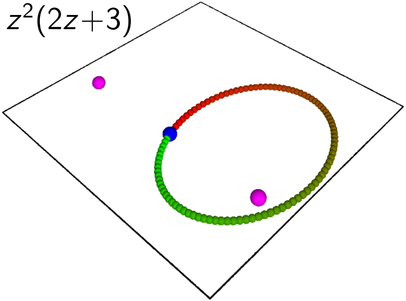
Operation der Monodromiegruppe



z

$\downarrow$

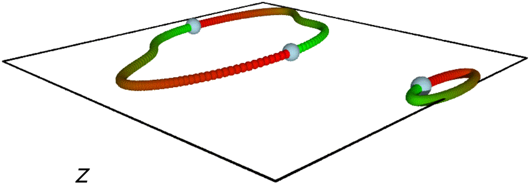
$f(z) = z^2(2z+3)$



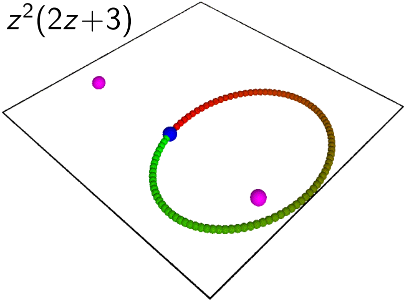
$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$

$|f^{-1}(\bullet)| < 3$

Operation der Monodromiegruppe



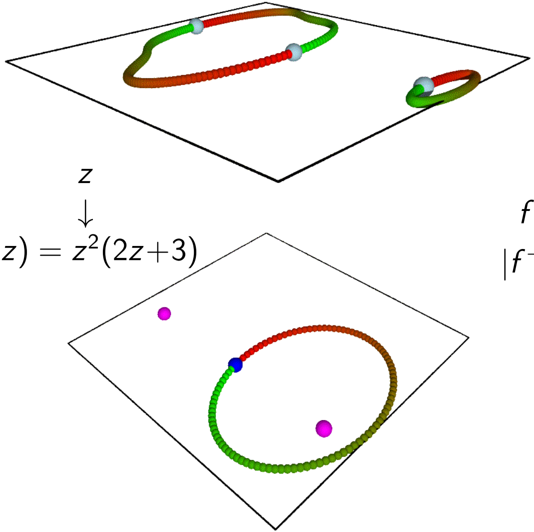
$$z \downarrow f(z) = z^2(2z+3)$$



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

$$|f^{-1}(\bullet)| < 3$$

Operation der Monodromiegruppe



z

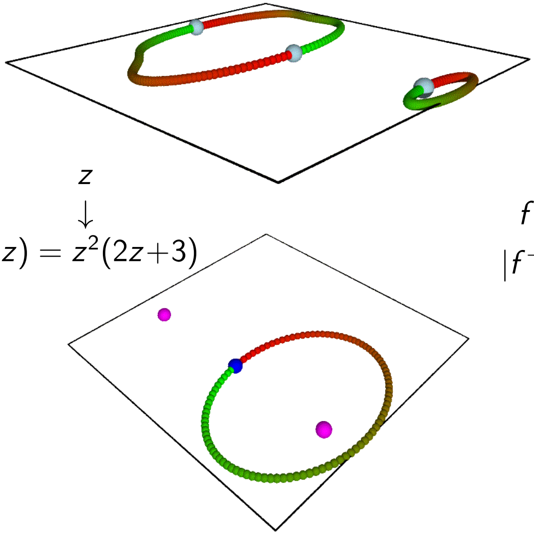
$\downarrow$

$f(z) = z^2(2z+3)$

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

$|f^{-1}(\bullet)| < 3$

Operation der Monodromiegruppe

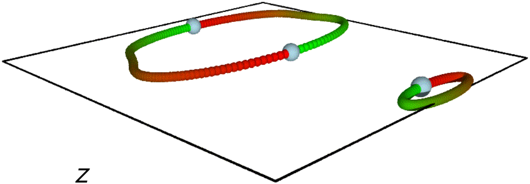


$$z \downarrow f(z) = z^2(2z+3)$$

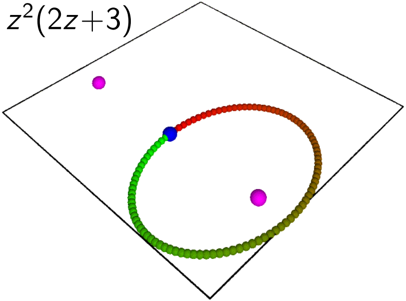
$$f^{-1}(\bullet) = \{\bullet, \bullet, \bullet\}$$ (blue dot; light blue dots)

$$|f^{-1}(\bullet)| < 3$$ (magenta dot)

Operation der Monodromiegruppe



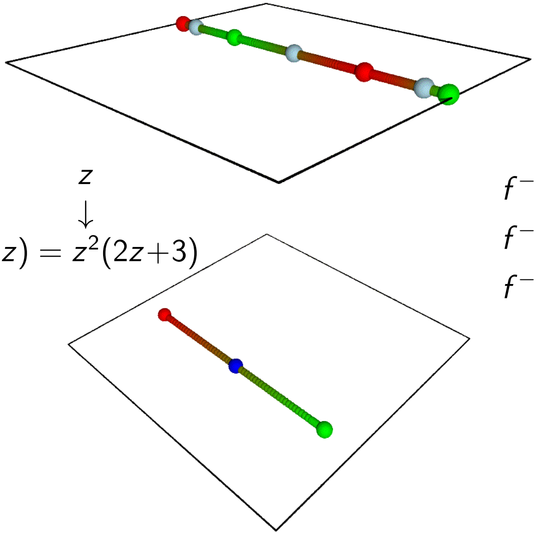
$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$



$$f^{-1}(\color{blue}\bullet) = \{\color{lightblue}\bullet, \color{lightblue}\bullet, \color{lightblue}\bullet\}$$

$$|f^{-1}(\color{magenta}\bullet)| < 3$$

Operation der Monodromiegruppe



z

$\downarrow$

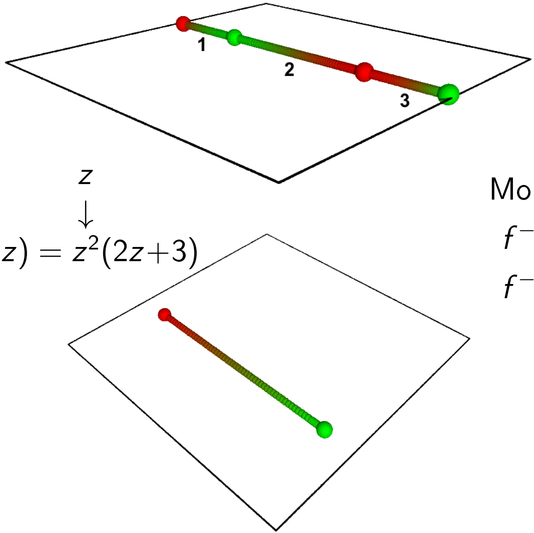
$f(z) = z^2(2z+3)$

$$f^{-1}({\color{blue}\bullet}) = \{{\color{lightblue}\bullet}, {\color{lightblue}\bullet}, {\color{lightblue}\bullet}\}$$

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

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

Operation der Monodromiegruppe



$$z$$
$$\downarrow$$
$$f(z) = z^2(2z+3)$$

$$\mathrm{Mon}(f) = <\textcolor{red}{(2\,3)}, \textcolor{green}{(1\,2)}>$$
$$f^{-1}(\textcolor{red}{\bullet}) = \{\textcolor{red}{\bullet}, \textcolor{red}{\bullet}\}$$
$$f^{-1}(\textcolor{green}{\bullet}) = \{\textcolor{green}{\bullet}, \textcolor{green}{\bullet}\}$$

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

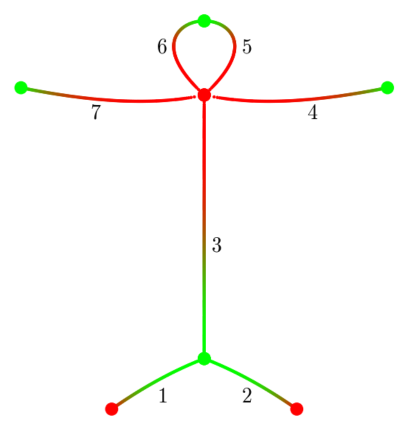
Rationale Funktion

$f(z) \in \mathbb{C}(z)$, Grad n, kritische Werte $0, 1$ und ∞

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

Bipartiter Graph

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



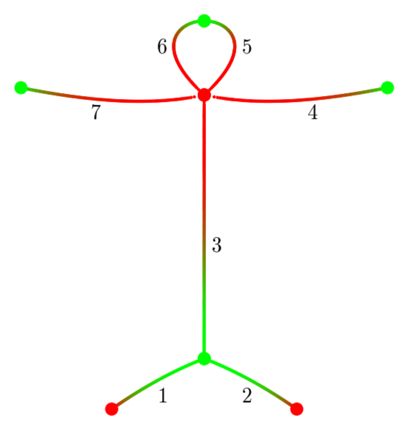
Rationale Funktion

$f(z) \in \mathbb{C}(z)$, Grad n, kritische Werte $0, 1$ und ∞

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

Bipartiter Graph

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



Rationale Funktion

$f(z) \in \mathbb{C}(z)$, Grad n, kritische Werte $0, 1$ und ∞

Erzeuger von Mon(f)

$$\sigma = (1\,2\,3)(5\,6)$$
$$\tau = (3\,4\,5\,6\,7)$$
$$\sigma\tau = (1\,2\,3\,4\,6\,7)$$

Klassifikation der Monodromiegruppen

$f(z) \in \mathbb{C}(z)$ vom Grad n mit r kritischen Werten

- $\text{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_{r-1}>$
- $\sum_{i=1}^{r}$ Anzahl der Zykel von $\sigma_i = (r-2)n + 2$

mit $\sigma_r = \sigma_1 \cdot \sigma_2 \cdots \sigma_{r-1}$.

Klassifikation der Monodromiegruppen

$f(z) \in \mathbb{C}(z)$ vom Grad n mit r kritischen Werten

- $\mathrm{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_{r-1}>$
- $\sum_{i=1}^{r}$ Anzahl der Zykel von $\sigma_i = (r-2)n + 2$

mit $\sigma_r = \sigma_1 \cdot \sigma_2 \cdots \sigma_{r-1}$.

Beispiele für Monodromiegruppen

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

Klassifikation der Monodromiegruppen

$f(z) \in \mathbb{C}(z)$ vom Grad n mit r kritischen Werten

- $\mathrm{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_{r-1}>$
- $\sum_{i=1}^{r}$ Anzahl der Zykel von $\sigma_i = (r-2)n + 2$

mit $\sigma_r = \sigma_1 \cdot \sigma_2 \cdots \sigma_{r-1}$.

Beispiele für Monodromiegruppen

$f(z)$	r	$\mathrm{Mon}(f)$
z^n	2	$<(1\,2\,\ldots\,n)>$ zyklisch
$f(\cos\phi) = \cos n\phi$	3	Diedergruppe der Ordnung $2n$

Klassifikation der Monodromiegruppen

$f(z) \in \mathbb{C}(z)$ vom Grad n mit r kritischen Werten

- $\mathrm{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_{r-1}>$
- $\sum_{i=1}^{r}$ Anzahl der Zykel von $\sigma_i = (r-2)n + 2$

mit $\sigma_r = \sigma_1 \cdot \sigma_2 \cdots \sigma_{r-1}$.

Beispiele für Monodromiegruppen

$f(z)$	r	$\mathrm{Mon}(f)$
z^n	2	$<(1\,2\,\ldots\,n)>$ zyklisch
$f(\cos\phi) = \cos n\phi$	3	Diedergruppe der Ordnung $2n$
„zufällig“	$2(n-1)$	$\mathrm{Sym}(n)$

Klassifikation der Monodromiegruppen

$f(z) \in \mathbb{C}(z)$ vom Grad n mit r kritischen Werten

- $\mathrm{Mon}(f) = <\sigma_1, \sigma_2, \ldots, \sigma_{r-1}>$
- $\sum_{i=1}^{r}$ Anzahl der Zykel von $\sigma_i = (r-2)n + 2$

mit $\sigma_r = \sigma_1 \cdot \sigma_2 \cdots \sigma_{r-1}$.

Beispiele für Monodromiegruppen

$f(z)$	r	$\mathrm{Mon}(f)$
z^n	2	$<(1\,2\,\ldots\,n)>$ zyklisch
$f(\cos\phi) = \cos n\phi$	3	Diedergruppe der Ordnung $2n$
„zufällig“	$2(n-1)$	$\mathrm{Sym}(n)$
?	3	$\mathrm{GL}(3,2)$ einfach, Ordnung 168

Klassifikation der Monodromiegruppen

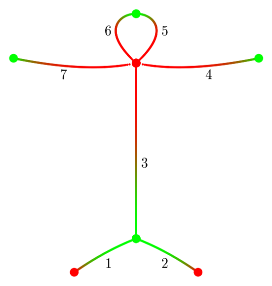
Großprojekt

Bestimme die möglichen Monodromiegruppen rationaler Funktionen.

- Wesentliche Fortschritte:
  - Guralnick-Thompson Vermutung gelöst: Außer Alt(n) nur endlich viele nicht abelsche Kompositionfaktoren.
  - Bekannt für Polynome
- Alles beruht auf der *Klassifikation der endlichen einfachen Gruppen*, einem Satz mit einem Beweis auf 15.000 Seiten!

Vom Dessin zur rationalen Funktion

Bipartiter Graph



Ansatz

$$f(z) - 0 = \frac{(z-1)^5(z^2+az+b)}{z}$$

$$f(z) - 1 = \frac{(z-c)^3(z-d)^2(z^2+ez+g)}{z}$$

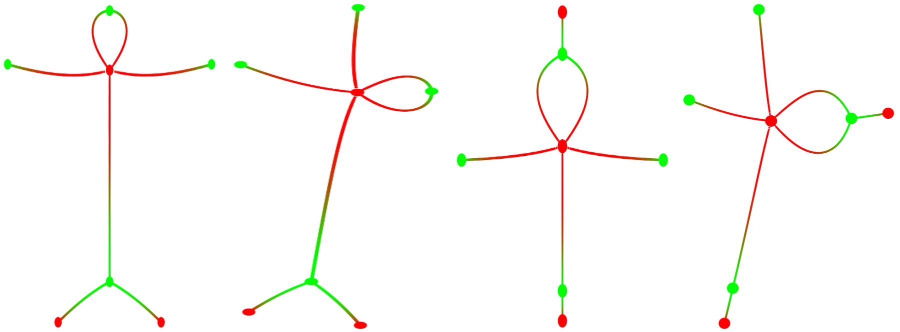
Lösung

Koeffizientenvergleich: Polynomiales System in $\{a, b, c, d, e, g\}$

Vom Dessin zur rationalen Funktion

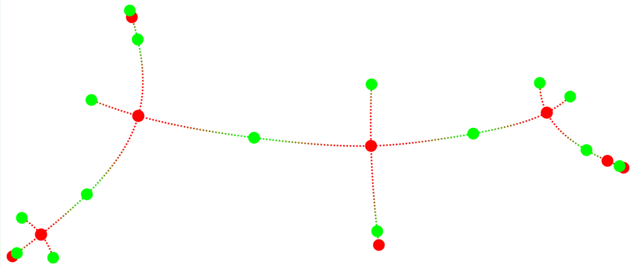
Problem

- Ansatz berücksichtigt nur Eckenvalenzen des Dessins, daher viele „falsche“ Lösungen.
- Polynomiale Systeme nur bis etwa Grad $n = 10$ lösbar.



Vom Dessin zur rationalen Funktion

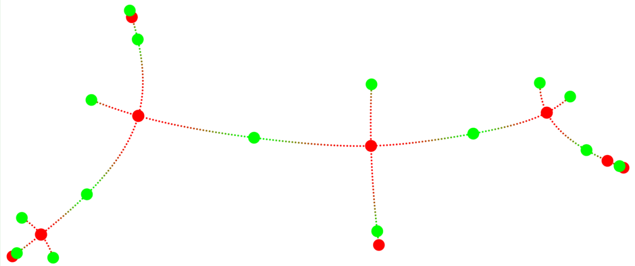
Herausforderung



$n = 23$
Mathieugruppe M_{23}
$f(z) =?$

Vom Dessin zur rationalen Funktion

Herausforderung

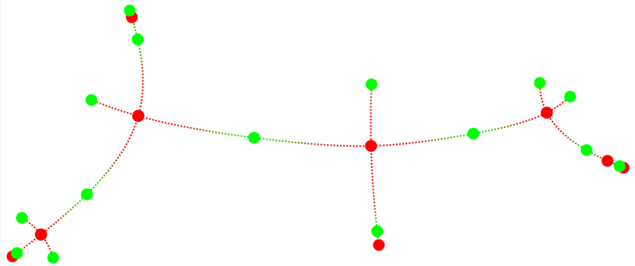


$n = 23$
Mathieugruppe M_{23}
$f(z) = ?$

- (Matiyasevich 1998) Numerische Approximation durch Deformation, danach algebraische Koeffizienten erkennen.

Vom Dessin zur rationalen Funktion

Herausforderung

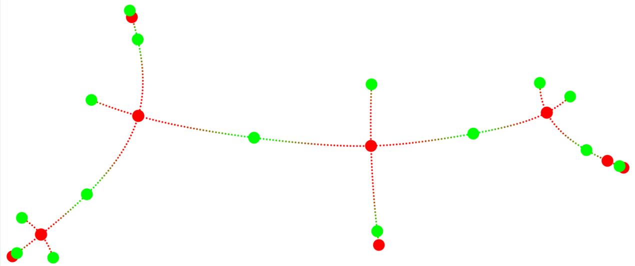


$n = 23$
Mathieugruppe M_{23}
$f(z) = ?$

- (Matiyasevich 1998) Numerische Approximation durch Deformation, danach algebraische Koeffizienten erkennen.
- (Elkies 2013) Lösung über Primkörper $\mathbb{F}_p$, danach p-adisch liften zu Lösung in $\mathbb{Q}_p$, danach algebraische Koeffizienten erkennen.

Vom Dessin zur rationalen Funktion

Herausforderung



$n = 23$
Mathieugruppe M_{23}
$f(z) = ?$

- (Matiyasevich 1998) Numerische Approximation durch Deformation, danach algebraische Koeffizienten erkennen.
- (Elkies 2013) Lösung über Primkörper $\mathbb{F}_p$, danach p-adisch liften zu Lösung in $\mathbb{Q}_p$, danach algebraische Koeffizienten erkennen.
- (M. 2015) Anderer Ansatz mit formalen Potenzreihen und direkte exakte Lösung.

Algebraische Definition der Monodromiegruppe

Beliebiger Körper K statt $\mathbb{C}$

$\mathrm{Mon}(f)$ für $f(z) \in K(z)$, zum Beispiel für K endlich?

$$\mathrm{Mon}(f) = \mathrm{Gal}(f(z) - t/K(t))$$

Stimmt für $K = \mathbb{C}$ mit der geometrisch definierten Gruppe überein.