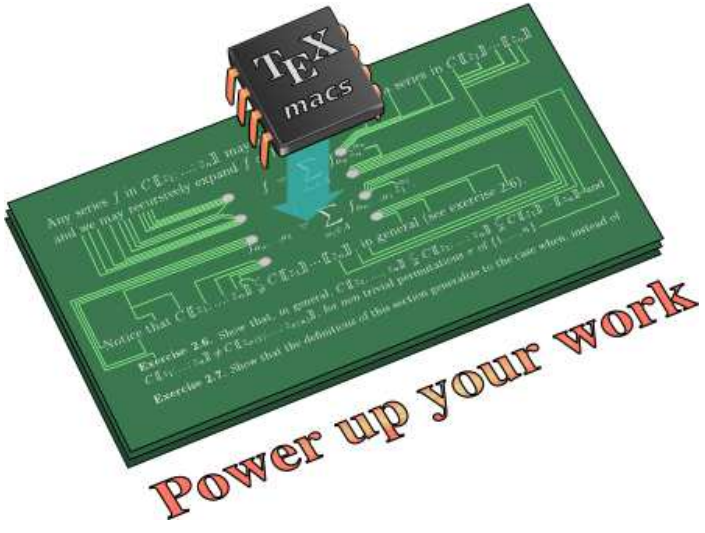
Autour du calcul numérique de groupes de Galois différentiels

Joris van der Hoeven

CNRS



Séminaire Différentiel

Palaiseau, 2 avril 2019

Le problème

$\mathbb{K} = \bar{\mathbb{Q}} \subseteq \mathbb{C}$ (ou sous corps de $\mathbb{C}$ avec $\mathbb{K} = \bar{\mathbb{K}}$ pour certains résultats)

Le problème

$\mathbb{K} = \bar{\mathbb{Q}} \subseteq \mathbb{C}$ (ou sous corps de $\mathbb{C}$ avec $\mathbb{K} = \bar{\mathbb{K}}$ pour certains résultats)

$$L \;=\; \partial^r + L_{r-1}(z)\,\partial^{r-1} + \cdots + L_0(z) \;\in\; \mathbb{K}(z)[\partial]$$

Le problème

$\mathbb{K} = \bar{\mathbb{Q}} \subseteq \mathbb{C}$ (ou sous corps de $\mathbb{C}$ avec $\mathbb{K} = \bar{\mathbb{K}}$ pour certains résultats)

$$L \;=\; \partial^r + L_{r-1}(z)\,\partial^{r-1} + \cdots + L_0(z) \;\in\; \mathbb{K}(z)[\partial]$$

système fondamental de solutions $\boldsymbol{h}$: $L(h_1) \;=\; \cdots \;=\; L(h_r) \;=\; 0$

Le problème

$\mathbb{K} = \bar{\mathbb{Q}} \subseteq \mathbb{C}$ (ou sous corps de $\mathbb{C}$ avec $\mathbb{K} = \bar{\mathbb{K}}$ pour certains résultats)

$$L = \partial^r + L_{r-1}(z)\,\partial^{r-1} + \cdots + L_0(z) \in \mathbb{K}(z)[\partial]$$

système fondamental de solutions $\boldsymbol{h}$: $L(h_1) = \cdots = L(h_r) = 0$

$$\mathcal{K} = \mathbb{K}(z)(h_1, \ldots, h_r) \mid \mathbb{K}(z) = \mathcal{F}$$

Le problème

$\mathbb{K} = \bar{\mathbb{Q}} \subseteq \mathbb{C}$ (ou sous corps de $\mathbb{C}$ avec $\mathbb{K} = \bar{\mathbb{K}}$ pour certains résultats)

$$L \;=\; \partial^r + L_{r-1}(z)\,\partial^{r-1} + \cdots + L_0(z) \;\in\; \mathbb{K}(z)[\partial]$$

système fondamental de solutions $\boldsymbol{h}$: $L(h_1) \;=\; \cdots \;=\; L(h_r) \;=\; 0$

$$\mathcal{K} \;=\; \mathbb{K}(z)(h_1, \ldots, h_r) \;\mid\; \mathbb{K}(z) \;=\; \mathcal{F}$$

Définition : groupe de Galois différentiel de L

Groupe $\mathcal{G}_{L,\boldsymbol{h}} = \mathcal{G}_{\mathcal{K}|\mathcal{F}}$ des automorphismes différentiels de $\mathcal{K}$ sur $\mathcal{F}$. Par l'action sur $\boldsymbol{h}$, c'est un sous groupe algébrique de $\mathsf{GL}_n(\mathbb{K})$. En faisant varier $\boldsymbol{h}$, ceci détermine $\mathcal{G}_L$ à conjugaison près.

Le problème

$\mathbb{K} = \bar{\mathbb{Q}} \subseteq \mathbb{C}$ (ou sous corps de $\mathbb{C}$ avec $\mathbb{K} = \bar{\mathbb{K}}$ pour certains résultats)

$$L \;=\; \partial^r + L_{r-1}(z)\,\partial^{r-1} + \cdots + L_0(z) \;\in\; \mathbb{K}(z)[\partial]$$

système fondamental de solutions $\boldsymbol{h}$: $L(h_1) \;=\; \cdots \;=\; L(h_r) \;=\; 0$

$$\mathcal{K} \;=\; \mathbb{K}(z)(h_1,\ldots,h_r) \;\mid\; \mathbb{K}(z) \;=\; \mathcal{F}$$

Définition : groupe de Galois différentiel de L

Groupe $\mathcal{G}_{L,\boldsymbol{h}} = \mathcal{G}_{\mathcal{K}|\mathcal{F}}$ des automorphismes différentiels de $\mathcal{K}$ sur $\mathcal{F}$. Par l'action sur $\boldsymbol{h}$, c'est un sous groupe algébrique de $\mathsf{GL}_n(\mathbb{K})$. En faisant varier $\boldsymbol{h}$, ceci détermine $\mathcal{G}_L$ à conjugaison près.

Question

Comment calculer $\mathcal{G}_L$?

Exemples

- $L = \partial - 1$,

  $h = (e^z)$

$$\sigma(e^z) = a e^z, \qquad a \neq 0$$

Exemples

- $L = \partial - 1$,

  $h = (e^z)$

$$\mathcal{G}_{L,h} = \{(a) : a \in \mathbb{K}^{\neq}\}$$

Exemples

- $L = \partial - 1$,

  $h = (e^z)$

$$\mathcal{G}_{L,h} = \{(a) : a \in \mathbb{K}^{\neq}\}$$

- $L = \partial^2 + z^{-1}\partial$

  $h = (\log z, 1)$

$$\sigma(1) = 1$$

Exemples

- $L = \partial - 1$,

  $h = (e^z)$

$$\mathcal{G}_{L,h} = \{(a) : a \in \mathbb{K}^{\neq}\}$$

- $L = \partial^2 + z^{-1}\partial$

  $h = (\log z, 1)$

$$\begin{aligned} \sigma(\log z) &= \log z + a, \qquad a \in \mathbb{K} \\ \sigma(1) &= 1 \end{aligned}$$

Exemples

- $L = \partial - 1$,

  $h = (e^z)$

$$\mathcal{G}_{L,h} = \{(a) : a \in \mathbb{K}^{\neq}\}$$

- $L = \partial^2 + z^{-1}\partial$

  $h = (\log z, 1)$

$$\mathcal{G}_{L,h} = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{K} \right\}$$

Exemples (suite)

- $L = \partial^2 + (1 + z^{-1})\,\partial + z^{-1}$ (« dérivée » de $h' + h = z^{-1}$)

  $h = (\frac{1}{z} + \frac{1}{z^2} + \frac{2}{z^3} + \frac{6}{z^4} + \cdots, \mathrm{e}^{-z})$

$$\sigma(\mathrm{e}^{-z}) \;=\; a\,\mathrm{e}^{-z}, \qquad a \;\in\; \mathbb{K}^{\neq}$$

Exemples (suite)

- $L = \partial^2 + (1 + z^{-1})\,\partial + z^{-1}$ (« dérivée » de $h' + h = z^{-1}$)

  $h = (\frac{1}{z} + \frac{1}{z^2} + \frac{2}{z^3} + \frac{6}{z^4} + \cdots, \mathrm{e}^{-z})$

$$\begin{aligned} \sigma(h_1) &= h_1 + b\,\mathrm{e}^{-z}, & b &\in \mathbb{K} \\ \sigma(\mathrm{e}^{-z}) &= a\,\mathrm{e}^{-z}, & a &\in \mathbb{K}^{\neq} \end{aligned}$$

Exemples (suite)

- $L = \partial^2 + (1 + z^{-1})\,\partial + z^{-1}$ (« dérivée » de $h' + h = z^{-1}$)

  $\boldsymbol{h} = (\frac{1}{z} + \frac{1}{z^2} + \frac{2}{z^3} + \frac{6}{z^4} + \cdots, \mathrm{e}^{-z})$

$$\mathcal{G}_{L,\boldsymbol{h}} = \left\{ \begin{pmatrix} 1 & b \\ 0 & a \end{pmatrix} : a \in \mathbb{K}^{\neq}, b \in \mathbb{K} \right\}$$

Exemples (suite)

- $L = \partial^2 + (1 + z^{-1})\,\partial + z^{-1}$ (« dérivée » de $h' + h = z^{-1}$)

  $\boldsymbol{h} = (\frac{1}{z} + \frac{1}{z^2} + \frac{2}{z^3} + \frac{6}{z^4} + \cdots, \mathrm{e}^{-z})$

$$\mathcal{G}_{L,\boldsymbol{h}} = \left\{ \begin{pmatrix} 1 & b \\ 0 & a \end{pmatrix} : a \in \mathbb{K}^{\neq}, b \in \mathbb{K} \right\}$$

- $L = A\,B$

  $\boldsymbol{h} = (B^{-1}\,\boldsymbol{h}_A, \boldsymbol{h}_B)$

$$\mathcal{G}_{L,\boldsymbol{h}} = \begin{pmatrix} \mathcal{G}_{A,\boldsymbol{h}_A} & * \\ 0 & \mathcal{G}_{B,\boldsymbol{h}_B} \end{pmatrix}$$

Exemples (suite)

- $L = \partial^2 + (1 + z^{-1})\,\partial + z^{-1}$ (« dérivée » de $h' + h = z^{-1}$)

  $\boldsymbol{h} = (\frac{1}{z} + \frac{1}{z^2} + \frac{2}{z^3} + \frac{6}{z^4} + \cdots, \mathrm{e}^{-z})$

$$\mathcal{G}_{L,\boldsymbol{h}} = \left\{ \begin{pmatrix} 1 & b \\ 0 & a \end{pmatrix} : a \in \mathbb{K}^{\neq}, b \in \mathbb{K} \right\}$$

- $L = A\,B$

  $\boldsymbol{h} = (B^{-1}\,\boldsymbol{h}_A, \boldsymbol{h}_B)$

$$\mathcal{G}_{L,\boldsymbol{h}} = \begin{pmatrix} \mathcal{G}_{A,\boldsymbol{h}_A} & * \\ 0 & \mathcal{G}_{B,\boldsymbol{h}_B} \end{pmatrix}$$

L se factorise $\iff$ $\mathcal{G}_L$ admet un sous espace invariant non trivial

Historique abrégée

1895, 1897. SCHLESINGER : théorème de densité (cas Fuchsien)

Historique abrégée

1895, 1897. SCHLESINGER : théorème de densité (cas Fuchsien)

1991. MARTINET–RAMIS : théorème de densité (cas général)

Historique abrégée

1895, 1897. SCHLESINGER : théorème de densité (cas Fuchsien)

1991. MARTINET–RAMIS : théorème de densité (cas général)

1986–1998. KOVACIC, SINGER, ULMER, VAN HOEIJ & WEIL, SINGER & COMPOINT, … : cas particuliers

Historique abrégée

1895, 1897. SCHLESINGER : théorème de densité (cas Fuchsien)

1991. MARTINET–RAMIS : théorème de densité (cas général)

1986–1998. KOVACIC, SINGER, ULMER, VAN HOEIJ & WEIL, SINGER & COMPOINT, … : cas particuliers

1998. Discussion avec Harm DERKSEN (et VAN HOEIJ) au MSRI…

Historique abrégée

1895, 1897. SCHLESINGER : théorème de densité (cas Fuchsien)

1991. MARTINET–RAMIS : théorème de densité (cas général)

1986–1998. KOVACIC, SINGER, ULMER, VAN HOEIJ & WEIL, SINGER & COMPOINT, … : cas particuliers

1998. Discussion avec Harm DERKSEN (et VAN HOEIJ) au MSRI…

2002. HRUSHOVSKI : algorithme basé sur « bornes sur le degré »

Historique abrégée

1895, 1897. SCHLESINGER : théorème de densité (cas Fuchsien)

1991. MARTINET–RAMIS : théorème de densité (cas général)

1986–1998. KOVACIC, SINGER, ULMER, VAN HOEIJ & WEIL, SINGER & COMPOINT, … : cas particuliers

1998. Discussion avec Harm DERKSEN (et VAN HOEIJ) au MSRI…

2002. HRUSHOVSKI : algorithme basé sur « bornes sur le degré »

2003. DERKSEN–JAENDEL–KOIRAN : algorithme algébrique

Historique abrégée

1895, 1897. SCHLESINGER : théorème de densité (cas Fuchsien)

1991. MARTINET–RAMIS : théorème de densité (cas général)

1986–1998. KOVACIC, SINGER, ULMER, VAN HOEIJ & WEIL, SINGER & COMPOINT, … : cas particuliers

1998. Discussion avec Harm DERKSEN (et VAN HOEIJ) au MSRI…

2002. HRUSHOVSKI : algorithme basé sur « bornes sur le degré »

2003. DERKSEN–JAENDEL–KOIRAN : algorithme algébrique

2005. VAN DER HOEVEN : algorithme numérique approximatif +

Historique abrégée

1895, 1897. SCHLESINGER : théorème de densité (cas Fuchsien)

1991. MARTINET–RAMIS : théorème de densité (cas général)

1986–1998. KOVACIC, SINGER, ULMER, VAN HOEIJ & WEIL, SINGER & COMPOINT, … : cas particuliers

1998. Discussion avec Harm DERKSEN (et VAN HOEIJ) au MSRI…

2002. HRUSHOVSKI : algorithme basé sur « bornes sur le degré »

2003. DERKSEN–JAENDEL–KOIRAN : algorithme algébrique

2005. VAN DER HOEVEN : algorithme numérique approximatif + théorème effectif de densité

Historique abrégée

1895, 1897. SCHLESINGER : théorème de densité (cas Fuchsien)

1991. MARTINET–RAMIS : théorème de densité (cas général)

1986–1998. KOVACIC, SINGER, ULMER, VAN HOEIJ & WEIL, SINGER & COMPOINT, … : cas particuliers

1998. Discussion avec Harm DERKSEN (et VAN HOEIJ) au MSRI…

2002. HRUSHOVSKI : algorithme basé sur « bornes sur le degré »

2003. DERKSEN–JAENDEL–KOIRAN : algorithme algébrique

2005. VAN DER HOEVEN : algorithme numérique approximatif + théorème effectif de densité

2016. BARKATOU–CLUZEAU–DI VIZIO–WEIL : algèbre de Lie de $\mathcal{G}_L$

Factorisation de l'opérateur L

1894. BEKE : facteurs d'ordre un

Factorisation de l'opérateur L

1894. BEKE : facteurs d'ordre un

1996. VAN HOEIJ : algorithme « local-global »

Factorisation de l'opérateur L

1894. BEKE : facteurs d'ordre un

1996. VAN HOEIJ : algorithme « local-global »

2004. CLUZEAU : algorithme « mod p »

Factorisation de l'opérateur L

1894. BEKE : facteurs d'ordre un

1996. VAN HOEIJ : algorithme « local-global »

2004. CLUZEAU : algorithme « mod p »

2005. VAN DER HOEVEN : algorithme « numérique » (mais complet)

$$L = AB \iff \mathcal{G}_L \cong \begin{pmatrix} \mathcal{G}_A & * \\ 0 & \mathcal{G}_B \end{pmatrix}$$

Point non singulier $z = \alpha$. On peut prendre $h = h^{[\alpha]}$ unique telle que

$$\begin{pmatrix} h_1(\alpha) & \cdots & h_r(\alpha) \\ \vdots & & \\ h_1^{(r-1)}(\alpha) & \cdots & h_r^{(r-1)}(\alpha) \end{pmatrix} = \begin{pmatrix} 1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & 1 \end{pmatrix}.$$

Point non singulier $z=\alpha$. On peut prendre $h=h^{[\alpha]}$ unique telle que

$$\begin{pmatrix} h_1(\alpha) & \cdots & h_r(\alpha) \\ \vdots & & \\ h_1^{(r-1)}(\alpha) & \cdots & h_r^{(r-1)}(\alpha) \end{pmatrix} = \begin{pmatrix} 1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & 1 \end{pmatrix}.$$

Point singulier $z=\alpha$. Disons $\alpha=0$. On peut prendre

$$h_i = e^{P_i(\sqrt[\varrho]{1/z})}\, z^{\gamma_i} \left(h_{i,0}(\sqrt[\varrho]{z}) + \cdots + h_{i,r-1}(\sqrt[\varrho]{z})\,(\log z)^{r-1}\right)$$

$$\begin{aligned} P_i &\in \mathbb{K}\left[\sqrt[\varrho]{1/z}\right] \\ \gamma_i &\in \mathbb{K} \\ h_{i,0},\ldots,h_{i,r-1} &\in \mathbb{K}\left[\left[\sqrt[\varrho]{z}\right]\right] \end{aligned}$$

Point non singulier $z=\alpha$. On peut prendre $h=h^{[\alpha]}$ unique telle que

$$\begin{pmatrix} h_1(\alpha) & \cdots & h_r(\alpha) \\ \vdots & & \\ h_1^{(r-1)}(\alpha) & \cdots & h_r^{(r-1)}(\alpha) \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

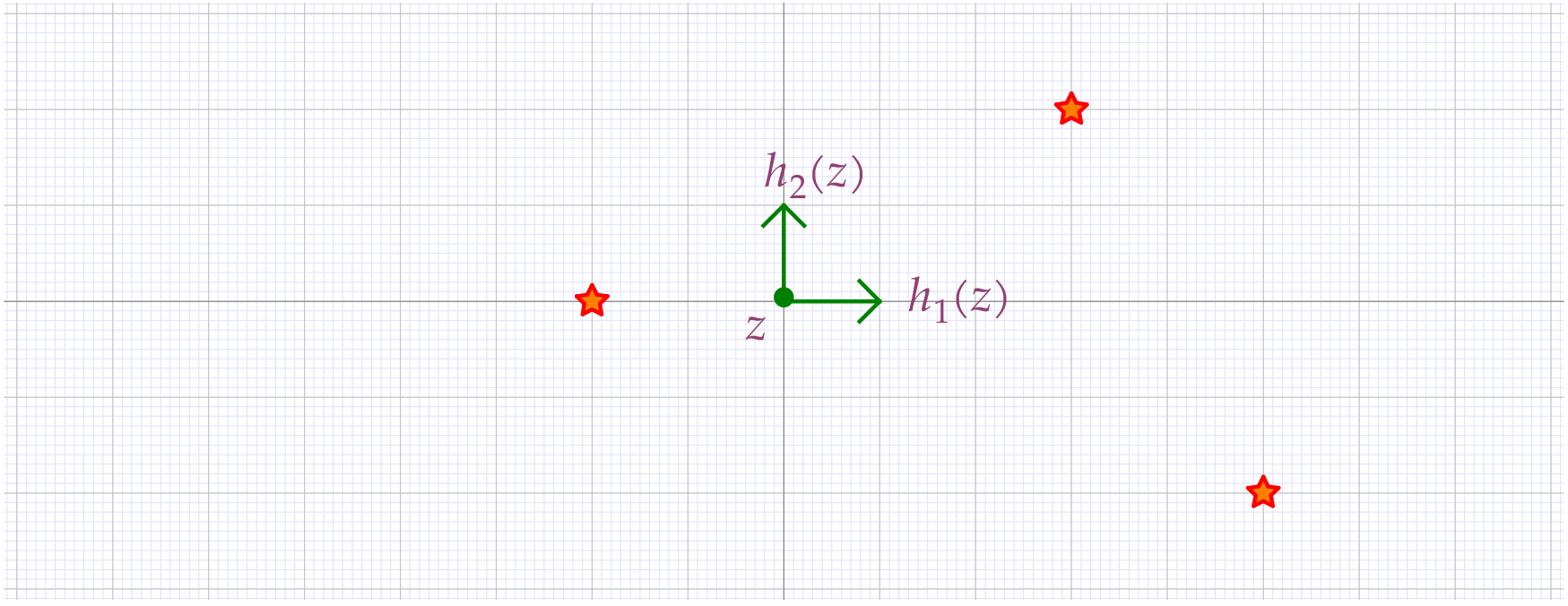
Point singulier $z=\alpha$. Disons $\alpha=0$. On peut prendre

$$h_i = \mathrm{e}^{P_i(\sqrt[\varrho]{1/z})}\, z^{\gamma_i} \left(h_{i,0}(\sqrt[\varrho]{z}) + \cdots + h_{i,r-1}(\sqrt[\varrho]{z})\,(\log z)^{r-1}\right)$$

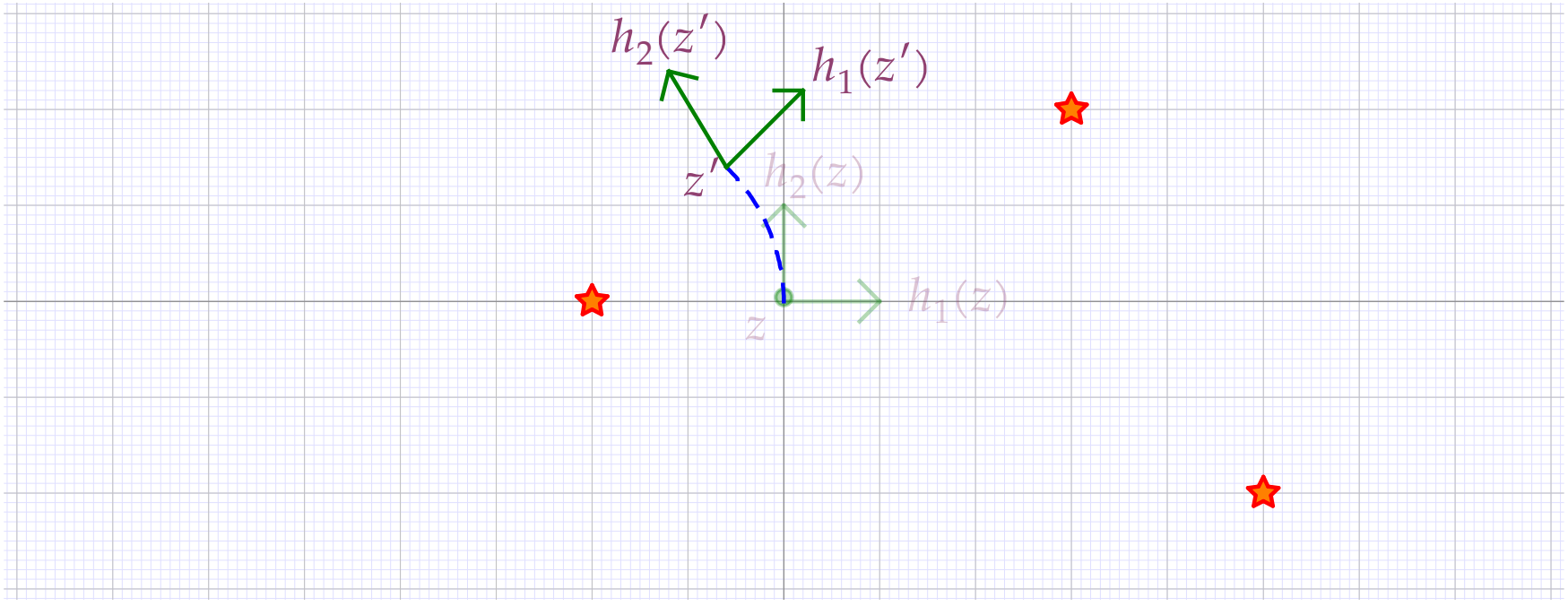
$$\begin{aligned} P_i &\in \mathbb{K}\left[\sqrt[\varrho]{1/z}\right] \\ \gamma_i &\in \mathbb{K} \\ h_{i,0},\ldots,h_{i,r-1} &\in \mathbb{K}\left[\left[\sqrt[\varrho]{z}\right]\right] \end{aligned}$$

L est Fuchsien si $P_i=0$, $\gamma_i\in\mathbb{K}$ et $\varrho=1$ (pour toute singularité $\alpha\in\mathbb{K}\cup\{\infty\}$)

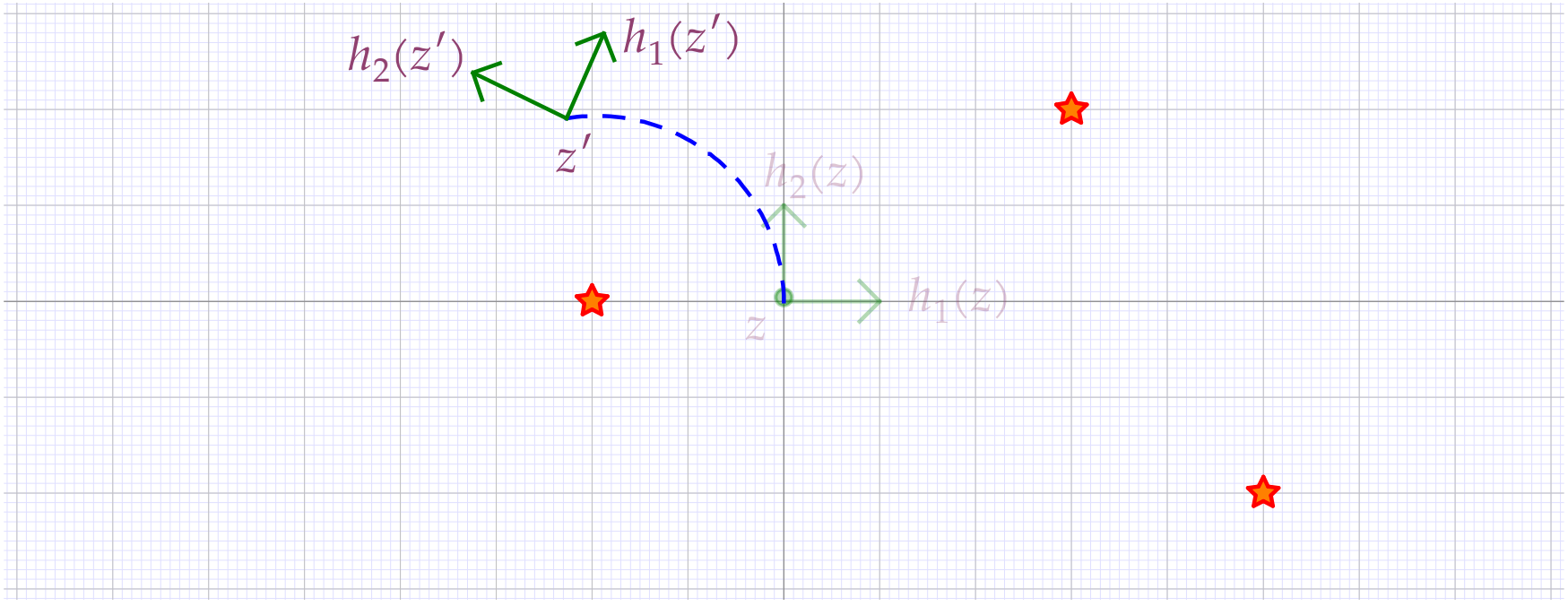
Monodromie



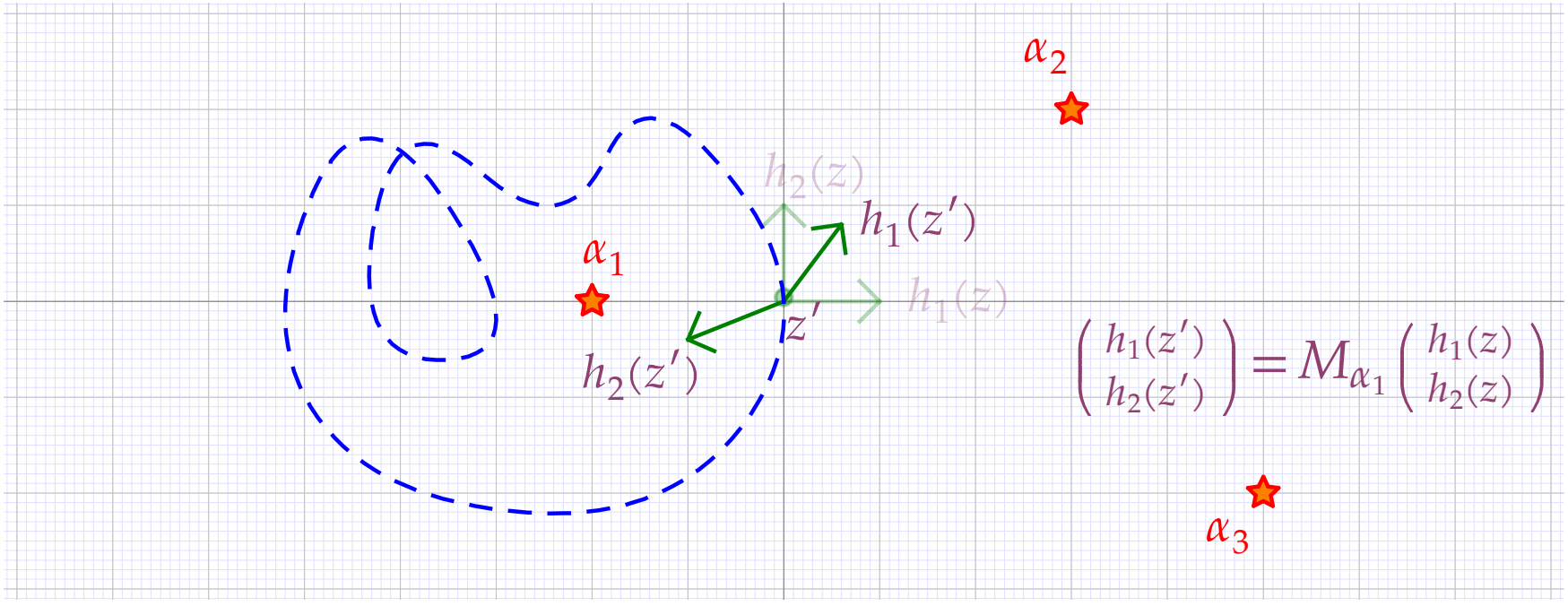
Monodromie



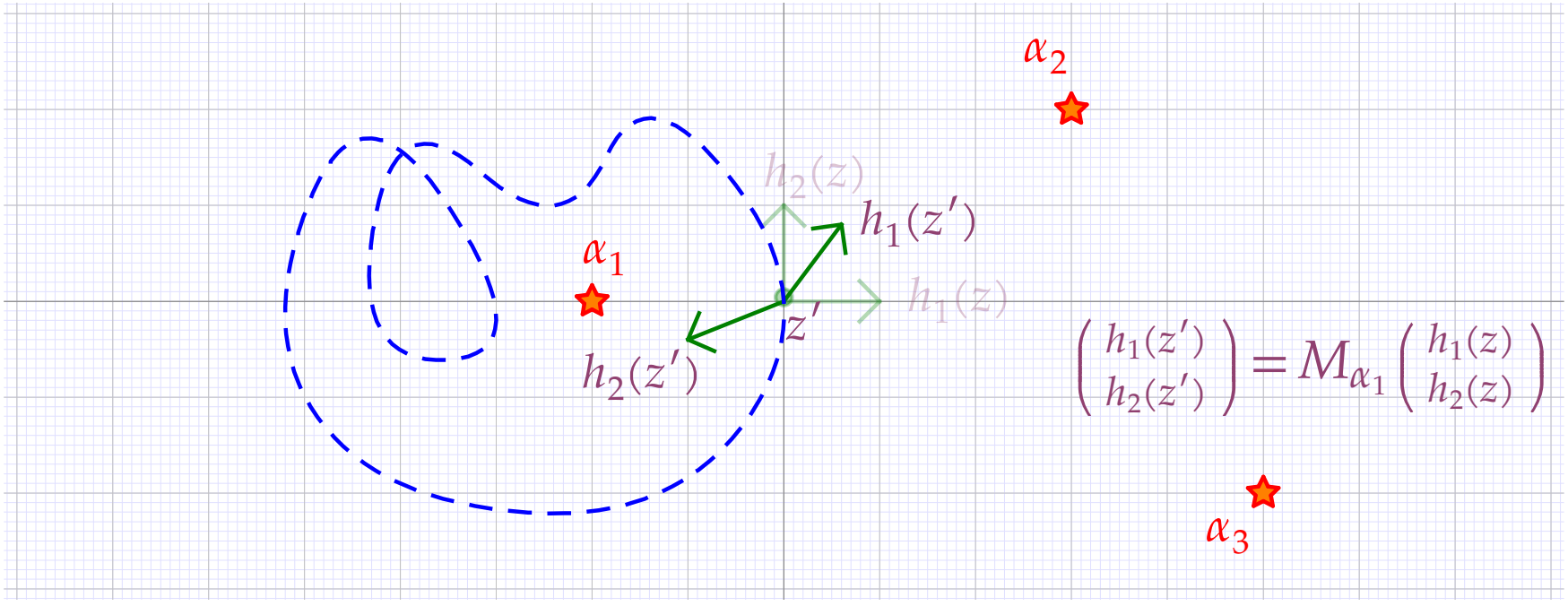
Monodromie



Monodromie


α_2
$h_2(z)$
$h_1(z')$
α_1
$h_1(z)$
z'
$h_2(z')$
$\begin{pmatrix} h_1(z') \\ h_2(z') \end{pmatrix} = M_{\alpha_1} \begin{pmatrix} h_1(z) \\ h_2(z) \end{pmatrix}$
α_3

Monodromie



Théorème (SCHLESINGER)

Soient $M_{\alpha_1},\dots,M_{\alpha_s} \in \mathrm{GL}_r(\mathbb{C})$ les matrices de monodromie autour des singularités d'un opérateur L Fuchsien. Soit $\mathcal{G} = \langle M_{\alpha_1},\dots,M_{\alpha_s}\rangle$ le plus petit sous groupe algébrique de $\mathrm{GL}_r(\mathbb{C})$ qui contient $M_{\alpha_1},\dots,M_{\alpha_s}$. Alors $\mathcal{G}_{L,h} = \mathcal{G} \cap \mathrm{GL}_r(\mathbb{K})$.

Matrices exponentiels

Induites par automorphismes σ exponentiels $\sigma\left(\mathrm{e}^{P(\sqrt[\varrho]{1/z})}\right) = \lambda\,\mathrm{e}^{P(\sqrt[\varrho]{1/z})}$

Théorème de densité (cas général)

Matrices exponentiels

Induites par automorphismes σ exponentiels $\sigma\left(\mathrm{e}^{P(\sqrt[\varrho]{1/z})}\right) = \lambda\,\mathrm{e}^{P(\sqrt[\varrho]{1/z})}$

Matrices de Stokes

$$\tilde{h} = \frac{1}{z} + \frac{1}{z^2} + \frac{2}{z^3} + \frac{6}{z^4} + \cdots$$

Théorème de densité (cas général)

Matrices exponentiels

Induites par automorphismes σ exponentiels $\sigma\left(\mathrm{e}^{P(\sqrt[\varrho]{1/z})}\right) = \lambda\,\mathrm{e}^{P(\sqrt[\varrho]{1/z})}$

Matrices de Stokes

$$\tilde{h} \;=\; \frac{1}{z}+\frac{1}{z^2}+\frac{2}{z^3}+\frac{6}{z^4}+\cdots$$

$$\hat{h}(\zeta) \;=\; (\tilde{\mathcal{B}}h)(\zeta) \;=\; 1+\zeta+\zeta^2+\zeta^3+\cdots \;=\; \frac{1}{1-\zeta}$$

Théorème de densité (cas général)

Matrices exponentiels

Induites par automorphismes σ exponentiels $\sigma\left(\mathrm{e}^{P(\sqrt[\varrho]{1/z})}\right) = \lambda\,\mathrm{e}^{P(\sqrt[\varrho]{1/z})}$

Matrices de Stokes

$$\tilde{h} \;=\; \frac{1}{z} + \frac{1}{z^2} + \frac{2}{z^3} + \frac{6}{z^4} + \cdots$$

$$\hat{h}(\zeta) \;=\; (\tilde{\mathcal{B}}h)(\zeta) \;=\; 1 + \zeta + \zeta^2 + \zeta^3 + \cdots \;=\; \frac{1}{1-\zeta}$$

$$h(z) \;=\; (\mathcal{L}_\theta \hat{h})(z) \;=\; \int_0^{\mathrm{e}^{\mathrm{i}\theta}\infty} \frac{\mathrm{e}^{-z\zeta}}{1-\zeta}\,\mathrm{d}\zeta$$

Théorème de densité (cas général)

Matrices exponentiels

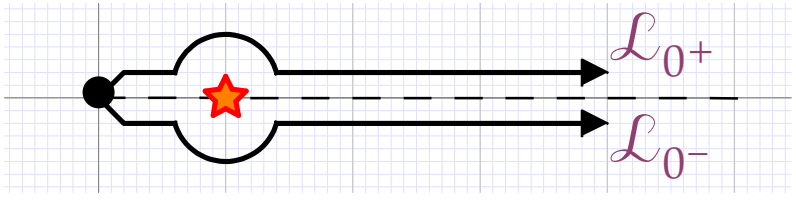
Induites par automorphismes σ exponentiels $\sigma\left(\mathrm{e}^{P(\sqrt[\varrho]{1/z})}\right) = \lambda\,\mathrm{e}^{P(\sqrt[\varrho]{1/z})}$

Matrices de Stokes

$$\tilde{h} \;=\; \frac{1}{z} + \frac{1}{z^2} + \frac{2}{z^3} + \frac{6}{z^4} + \cdots$$

$$\hat{h}(\zeta) \;=\; (\tilde{\mathcal{B}}h)(\zeta) \;=\; 1 + \zeta + \zeta^2 + \zeta^3 + \cdots \;=\; \frac{1}{1-\zeta}$$

$$h(z) \;=\; (\mathcal{L}_\theta \hat{h})(z) \;=\; \int_0^{\mathrm{e}^{\mathrm{i}\theta}\infty} \frac{\mathrm{e}^{-z\zeta}}{1-\zeta}\,\mathrm{d}\zeta$$



« Monodromie » de $\hat{h}$ en $\zeta = 1$

Théorème de densité (cas général, suite)

Accéléro-sommation d'Écalle

$$\begin{array}{ccccccccc}
\tilde{h} & & & & & & & & h \\
\downarrow{\scriptstyle \tilde{\mathcal{B}}_{z_1}} & & & & & & & & \uparrow{\scriptstyle \hat{\mathcal{L}}^{\theta_p}_{z_p}} \\
\hat{h}_1 & \xrightarrow[\hat{\mathcal{A}}^{\theta_1}_{z_1\to z_2}]{} & \hat{h}_2 & \longrightarrow & \cdots & \longrightarrow & \hat{h}_{p-1} & \xrightarrow[\hat{\mathcal{A}}^{\theta_{p-1}}_{z_{p-1}\to z_p}]{} & \hat{h}_n
\end{array}$$

Théorème de densité (cas général, suite)

Accéléro-sommation d'Écalle

$$\begin{array}{ccccccccc}
\tilde{h} & & & & & & & & h \\
\downarrow{\scriptstyle \tilde{\mathcal{B}}_{z_1}} & & & & & & & & \uparrow{\scriptstyle \hat{\mathcal{L}}^{\theta_p}_{z_p}} \\
\hat{h}_1 & \xrightarrow[\hat{\mathcal{A}}^{\theta_1}_{z_1\to z_2}]{} & \hat{h}_2 & \longrightarrow & \cdots & \longrightarrow & \hat{h}_{p-1} & \xrightarrow[\hat{\mathcal{A}}^{\theta_{p-1}}_{z_{p-1}\to z_p}]{} & \hat{h}_n
\end{array}$$

Théorème (MARTINET–RAMIS)

Les matrices de monodromie, exponentielles, et de Stokes génèrent le groupe de Galois différentiel de L en tant que groupe algébrique (défini sur $\mathbb{C}$).

Théorème de densité (cas général, suite)

Accéléro-sommation d'Écalle

$$\begin{array}{ccccccccc} \tilde{h} & & & & & & & & h \\ \downarrow{\scriptstyle \tilde{\mathcal{B}}_{z_1}} & & & & & & & & \uparrow{\scriptstyle \hat{\mathcal{L}}^{\theta_p}_{z_p}} \\ \hat{h}_1 & \xrightarrow[\hat{\mathcal{A}}^{\theta_1}_{z_1\to z_2}]{} & \hat{h}_2 & \longrightarrow & \cdots & \longrightarrow & \hat{h}_{p-1} & \xrightarrow[\hat{\mathcal{A}}^{\theta_{p-1}}_{z_{p-1}\to z_p}]{} & \hat{h}_n \end{array}$$

Théorème (Martinet–Ramis)

Les matrices de monodromie, exponentielles, et de Stokes génèrent le groupe de Galois différentiel de L en tant que groupe algébrique (défini sur $\mathbb{C}$).

Théorème (van der Hoeven)

On peut calculer un nombre fini de matrices de monodromie, exponentielles, et de Stokes, tel que ces matrices génèrent $\mathcal{G}_L$ en tant que groupe algébrique.

Les entrées de ces matrices sont des nombres complexes calculables.

Théorème (CHUDNOVSKY², VAN DER HOEVEN)

Pour $\mathbb{K} = \bar{\mathbb{Q}}$ et en prenant un point de base non singulier dans $\mathbb{K}$, on peut approximer en temps $O(n \log^3 n)$ les matrices de monodromie de L autour de chaque singularié avec une erreur d'au plus 2^{-n}.

Théorème (CHUDNOVSKY², VAN DER HOEVEN)

Pour $\mathbb{K} = \bar{\mathbb{Q}}$ et en prenant un point de base non singulier dans $\mathbb{K}$, on peut approximer en temps $O(n \log^3 n)$ les matrices de monodromie de L autour de chaque singularié avec une erreur d'au plus 2^{-n}.

Théorème (VAN DER HOEVEN)

Pour $\mathbb{K} = \bar{\mathbb{Q}}$, on peut approximer en temps $O(n \log^4 n)$ les matrices de Stokes du théorème de densité avec une erreur d'au plus 2^{-n}.

Factorisation de L

1. Calculer des générateurs $M_1, \ldots, M_m \in \mathsf{GL}_r(\mathbb{C}^{\mathrm{calc}})$ de $\mathcal{G}_L$

Factorisation de L

1. Calculer des générateurs $M_1, \ldots, M_m \in \mathsf{GL}_r(\mathbb{C}^{\mathrm{calc}})$ de $\mathcal{G}_L$
2. Fixer une précision p de calcul pour les « tests à zéro »

Factorisation de L

1. Calculer des générateurs $M_1, \ldots, M_m \in \mathsf{GL}_r(\mathbb{C}^{\mathrm{calc}})$ de $\mathcal{G}_L$
2. Fixer une précision p de calcul pour les « tests à zéro »
3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$

Factorisation de L

1. Calculer des générateurs $M_1, \ldots, M_m \in \mathsf{GL}_r(\mathbb{C}^{\mathrm{calc}})$ de $\mathcal{G}_L$
2. Fixer une précision p de calcul pour les « tests à zéro »
3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$
4. Si un tel espace V n'existe pas, alors retourner $\perp$

Factorisation de L

1. Calculer des générateurs $M_1, \ldots, M_m \in \mathsf{GL}_r(\mathbb{C}^{\mathrm{calc}})$ de $\mathcal{G}_L$
2. Fixer une précision p de calcul pour les « tests à zéro »
3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$
4. Si un tel espace V n'existe pas, alors retourner $\perp$
5. À partir de V, reconstruire une factorisation $L = A\,B$ « candidat »

Factorisation de L

1. Calculer des générateurs $M_1, \ldots, M_m \in \mathsf{GL}_r(\mathbb{C}^{\mathrm{calc}})$ de $\mathcal{G}_L$
2. Fixer une précision p de calcul pour les « tests à zéro »
3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$
4. Si un tel espace V n'existe pas, alors retourner $\perp$
5. À partir de V, reconstruire une factorisation $L = A\,B$ « candidat »
6. Si $L = A\,B$, alors retourner (A, B)

Factorisation de L

1. Calculer des générateurs $M_1, \ldots, M_m \in \mathsf{GL}_r(\mathbb{C}^{\mathrm{calc}})$ de $\mathcal{G}_L$
2. Fixer une précision p de calcul pour les « tests à zéro »
3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$
4. Si un tel espace V n'existe pas, alors retourner $\perp$
5. À partir de V, reconstruire une factorisation $L = A\,B$ « candidat »
6. Si $L = A\,B$, alors retourner (A, B)
7. Doubler la précision et retourner à l'étape 3

Zoom sur l'étape 3

1. Calculer des générateurs $M_1, \ldots, M_m \in \mathrm{GL}_r(\mathbb{C}^{\mathrm{calc}})$ de $\mathcal{G}_L$
2. Fixer une précision p de calcul pour les « tests à zéro »
3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$
4. Si un tel espace V n'existe pas, alors retourner $\perp$
5. À partir de V, reconstruire une factorisation $L = AB$ « candidat »
6. Si $L = AB$, alors retourner (A, B)
7. Doubler la précision et retourner à l'étape 3

Zoom sur l'étape 3

3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$

Zoom sur l'étape 3

3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$

- V invariant sous $M_1, \ldots, M_m \iff V$ invariant sous $\mathbb{A} := \mathbb{C}[M_1, \ldots, M_m]$

Zoom sur l'étape 3

3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$

- V invariant sous $M_1, \ldots, M_m \iff V$ invariant sous $\mathbb{A} := \mathbb{C}[M_1, \ldots, M_m]$
- **Scindage** : $\mathbb{C}^r = E_1 \oplus \cdots \oplus E_k$ avec $\pi_{E_1}, \ldots, \pi_{E_k} \in \mathbb{C}[M_1, \ldots, M_m]$

Zoom sur l'étape 3

3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$

- V invariant sous $M_1, \ldots, M_m \iff V$ invariant sous $\mathbb{A} := \mathbb{C}[M_1, \ldots, M_m]$
- **Scindage** : $\mathbb{C}^r = E_1 \oplus \cdots \oplus E_k$ avec $\pi_{E_1}, \ldots, \pi_{E_k} \in \mathbb{C}[M_1, \ldots, M_m]$
- Calculer un scindage avec k maximal :
  - Pour $A \in \mathbb{C}[M_1, \ldots, M_m]$ « aléatoire », prendre une base de E_i pour laquelle $\pi_{E_i} \circ A \circ \pi_{E_i}$ est sous forme normale de Jourdan
  - Si $\pi_{E_i} \circ A \circ \pi_{E_i}$ n'est pas « monopotente », on peut raffiner le scindage

Zoom sur l'étape 3

3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$

- V invariant sous $M_1, \ldots, M_m \iff V$ invariant sous $\mathbb{A} := \mathbb{C}[M_1, \ldots, M_m]$
- **Scindage** : $\mathbb{C}^r = E_1 \oplus \cdots \oplus E_k$ avec $\pi_{E_1}, \ldots, \pi_{E_k} \in \mathbb{C}[M_1, \ldots, M_m]$
- Calculer un scindage avec k maximal :
  - Pour $A \in \mathbb{C}[M_1, \ldots, M_m]$ « aléatoire », prendre une base de E_i pour laquelle $\pi_{E_i} \circ A \circ \pi_{E_i}$ est sous forme normale de Jourdan
  - Si $\pi_{E_i} \circ A \circ \pi_{E_i}$ n'est pas « monopotente », on peut raffiner le scindage
- On a $\mathbb{A} = \begin{pmatrix} \mathbb{A}_{1,1} & \cdots & \mathbb{A}_{1,m} \\ \vdots & & \vdots \\ \mathbb{A}_{m,1} & \cdots & \mathbb{A}_{m,m} \end{pmatrix}$ avec $\mathbb{A}_{i,j} = \pi_{E_i} \circ \mathbb{A} \circ \pi_{E_j}$, $\mathbb{A}_{i,i} - \lambda_i$ nilpotente sur E_i

Zoom sur l'étape 3

3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$

- V invariant sous $M_1, \ldots, M_m \iff V$ invariant sous $\mathbb{A} := \mathbb{C}[M_1, \ldots, M_m]$
- **Scindage** : $\mathbb{C}^r = E_1 \oplus \cdots \oplus E_k$ avec $\pi_{E_1}, \ldots, \pi_{E_k} \in \mathbb{C}[M_1, \ldots, M_m]$
- Calculer un scindage avec k maximal :
  - Pour $A \in \mathbb{C}[M_1, \ldots, M_m]$ « aléatoire », prendre une base de E_i pour laquelle $\pi_{E_i} \circ A \circ \pi_{E_i}$ est sous forme normale de Jourdan
  - Si $\pi_{E_i} \circ A \circ \pi_{E_i}$ n'est pas « monopotente », on peut raffiner le scindage
- On a $\mathbb{A} = \begin{pmatrix} \mathbb{A}_{1,1} & \cdots & \mathbb{A}_{1,m} \\ \vdots & & \vdots \\ \mathbb{A}_{m,1} & \cdots & \mathbb{A}_{m,m} \end{pmatrix}$ avec $\mathbb{A}_{i,j} = \pi_{E_i} \circ \mathbb{A} \circ \pi_{E_j}$, $\mathbb{A}_{i,i} - \lambda_i$ nilpotente sur E_i
- Pour tout i, prendre $v \in E_i \cap \ker(\mathbb{A}_{i,i} - \lambda_i)$ et tester si $\mathrm{Inv}_{\mathbb{A}}(v) \subsetneq \mathbb{C}^r$

Zoom sur l'étape 3

3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$

- V invariant sous $M_1, \ldots, M_m \iff V$ invariant sous $\mathbb{A} := \mathbb{C}[M_1, \ldots, M_m]$
- **Scindage** : $\mathbb{C}^r = E_1 \oplus \cdots \oplus E_k$ avec $\pi_{E_1}, \ldots, \pi_{E_k} \in \mathbb{C}[M_1, \ldots, M_m]$
- Calculer un scindage avec k maximal :
  - Pour $A \in \mathbb{C}[M_1, \ldots, M_m]$ « aléatoire », prendre une base de E_i pour laquelle $\pi_{E_i} \circ A \circ \pi_{E_i}$ est sous forme normale de Jourdan
  - Si $\pi_{E_i} \circ A \circ \pi_{E_i}$ n'est pas « monopotente », on peut raffiner le scindage
- On a $\mathbb{A} = \begin{pmatrix} \mathbb{A}_{1,1} & \cdots & \mathbb{A}_{1,m} \\ \vdots & & \vdots \\ \mathbb{A}_{m,1} & \cdots & \mathbb{A}_{m,m} \end{pmatrix}$ avec $\mathbb{A}_{i,j} = \pi_{E_i} \circ \mathbb{A} \circ \pi_{E_j}$, $\mathbb{A}_{i,i} - \lambda_i$ nilpotente sur E_i
- Pour tout i, prendre $v \in E_i \cap \ker(\mathbb{A}_{i,i} - \lambda_i)$ et tester si $\mathrm{Inv}_{\mathbb{A}}(v) \subsetneq \mathbb{C}^r$
- Si $\mathrm{Inv}_{\mathbb{A}}(v) \subsetneq \mathbb{C}^r$ pour un i, alors retourner $\mathrm{Inv}_{\mathbb{A}}(v)$; sinon, retourner $\perp$

Zoom sur l'étape 5

1. Calculer des générateurs $M_1, \ldots, M_m \in \mathrm{GL}_r(\mathbb{C}^{\mathrm{calc}})$ de $\mathcal{G}_L$
2. Fixer une précision p de calcul pour les « tests à zéro »
3. Déterminer un sous espace invariant V non trivial pour $M_1, \ldots, M_m$
4. Si un tel espace V n'existe pas, alors retourner $\perp$
5. À partir de V, reconstruire une factorisation $L = A\,B$ « candidat »
6. Si $L = A\,B$, alors retourner (A, B)
7. Doubler la précision et retourner à l'étape 3

Zoom sur l'étape 5

5. À partir de V, reconstruire une factorisation $L = A\,B$ « candidat »

Zoom sur l'étape 5

5. À partir de V, reconstruire une factorisation $L = A\,B$ « candidat »

- $V \longrightarrow$ base $\varphi_1, \ldots, \varphi_k \in \mathbb{C}^{\mathrm{calc}}[[z]]$ de $\ker B$ en un point non singulier

Zoom sur l'étape 5

5. À partir de V, reconstruire une factorisation $L = A\,B$ « candidat »

- $V \longrightarrow$ base $\varphi_1, \ldots, \varphi_k \in \mathbb{C}^{\mathrm{calc}}[[z]]$ de $\ker B$ en un point non singulier
- Reconstruire $B = \mathrm{ppcm}(\partial - \varphi_1'/\varphi_1, \ldots, \partial - \varphi_k'/\varphi_k) \in \mathbb{C}^{\mathrm{calc}}[[z]][\partial]$

Zoom sur l'étape 5

5. À partir de V, reconstruire une factorisation $L = A\,B$ « candidat »

- $V \longrightarrow$ base $\varphi_1, \ldots, \varphi_k \in \mathbb{C}^{\mathrm{calc}}[[z]]$ de $\ker B$ en un point non singulier
- Reconstruire $B = \mathrm{ppcm}(\partial - \varphi_1'/\varphi_1, \ldots, \partial - \varphi_k'/\varphi_k) \in \mathbb{C}^{\mathrm{calc}}[[z]][\partial]$
- Reconstruire $B \in \mathbb{C}^{\mathrm{calc}}(z)[\partial]$

Zoom sur l'étape 5

5. À partir de V, reconstruire une factorisation $L = A\,B$ « candidat »

- $V \longrightarrow$ base $\varphi_1, \ldots, \varphi_k \in \mathbb{C}^{\mathrm{calc}}[[z]]$ de $\ker B$ en un point non singulier
- Reconstruire $B = \mathrm{ppcm}(\partial - \varphi_1'/\varphi_1, \ldots, \partial - \varphi_k'/\varphi_k) \in \mathbb{C}^{\mathrm{calc}}[[z]][\partial]$
- Reconstruire $B \in \mathbb{C}^{\mathrm{calc}}(z)[\partial]$
- Reconstruire $B \in \bar{\mathbb{Q}}(z)[\partial]$ utilisant LLL

Groupe Galois différentiel

Idée : calculer $\mathcal{G}$ comme variété sous la forme

$$\mathcal{G} = \mathcal{F}\mathrm{e}^{\mathcal{L}} \qquad (\forall N \in \mathcal{F},\ N\mathrm{e}^{\mathcal{L}} = \mathrm{e}^{\mathcal{L}}N)$$

$\mathcal{F}$: ensemble fini contenant 1

$\mathcal{L}$: algèbre de Lie donnée par une base

Idée : calculer $\mathcal{G}$ comme variété sous la forme

$$\begin{aligned} \mathcal{G} &= \mathcal{F}\mathrm{e}^{\mathcal{L}} \qquad (\forall N \in \mathcal{F},\ N\mathrm{e}^{\mathcal{L}} = \mathrm{e}^{\mathcal{L}} N) \\ \mathcal{F} &: \text{ ensemble fini contenant } 1 \\ \mathcal{L} &: \text{ algèbre de Lie donnée par une base} \end{aligned}$$

Ingredients :

1. Calcul de $\langle M \rangle$ pour une simple matrice M
2. Tester si $M \in \mathcal{F}\mathrm{e}^{\mathcal{L}}$ pour $\mathcal{F}$ et $\mathcal{L}$ donnés

Groupe Galois différentiel : l'algorithme

Étape 1. [Initialisation]

Calculer $\langle M_i \rangle = \mathcal{F}_i \mathrm{e}^{\mathcal{L}_i}$ pour tout $i \in \{1, \ldots, m\}$

$\mathcal{F} := \mathcal{F}_1 \cup \cdots \cup \mathcal{F}_m$

$\mathcal{L} := \mathsf{Lie}(\mathcal{L}_1 + \cdots + \mathcal{L}_m)$

Étape 2. [Clôture]

Tant qu'il existe un $N \in \mathcal{F} \setminus \{1\}$ avec $N\,\mathcal{L}\,N^{-1} \not\subseteq \mathcal{L}$

$\mathcal{L} := \mathsf{Lie}(\mathcal{L} + N\,\mathcal{L}\,N^{-1})$

Tant qu'il existe un $N \in \mathcal{F} \setminus \{1\}$ avec $N \in \mathrm{e}^{\mathcal{L}}$, faire $\mathcal{F} := \mathcal{F} \setminus \{N\}$

Tant qu'il existe un $N \in \mathcal{F}^2$ avec $N \notin \mathcal{F}\mathrm{e}^{\mathcal{L}}$ faire

Calculer $\langle N \rangle = \mathcal{F}' \mathrm{e}^{\mathcal{L}'}$

Si $\mathcal{L}' \not\subseteq \mathcal{L}$, alors $\mathcal{L} := \mathsf{Lie}(\mathcal{L} + \mathcal{L}')$, quitter la boucle, repéter l'étape 2

Sinon, $\mathcal{F} := \mathcal{F} \cup \{N\}$

Retourner $\mathcal{F}\mathrm{e}^{\mathcal{L}}$

Représentation compacte des éléments dans $\mathcal{H} = \mathcal{G}/\mathrm{e}^{\mathcal{L}}$

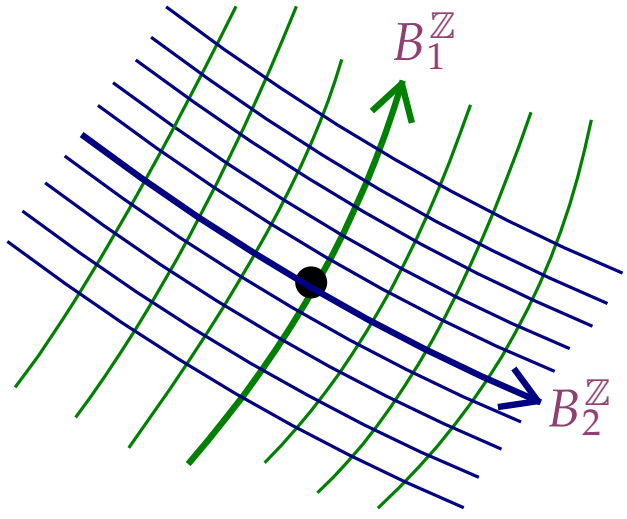
- Réduire au cas où $\mathcal{G} \subseteq \mathrm{Norm}(\mathrm{e}^{\mathcal{L}})^o$
- Premier élément $M = B_1 = \mathrm{e}^X$ de « la base » avec
  - $M\,\mathrm{e}^{\mathcal{L}} \in \mathcal{H}$
  - $M\,\mathrm{e}^{\mathcal{L}}$ génère $(\mathrm{e}^{\mathbb{C}X} \cap \mathcal{G})\,/\,\mathrm{e}^{\mathcal{L}}$
  - M admet un ordre q maximal avec ces propriétés
- Posons $\mathcal{H}' := \{N \in \mathcal{H} : [M,N] = 0\}$, $\mathcal{L}' := \mathcal{L} \oplus \mathbb{C}\,X$, tels que

$$\mathcal{H} \;=\; \{1, \ldots, M^{q-1}\}\,(\mathcal{H}'\,/\,\mathrm{e}^{\mathcal{L}'}).$$

- Autres éléments $B_2, \ldots, B_b$ de la base par récurrence, avec

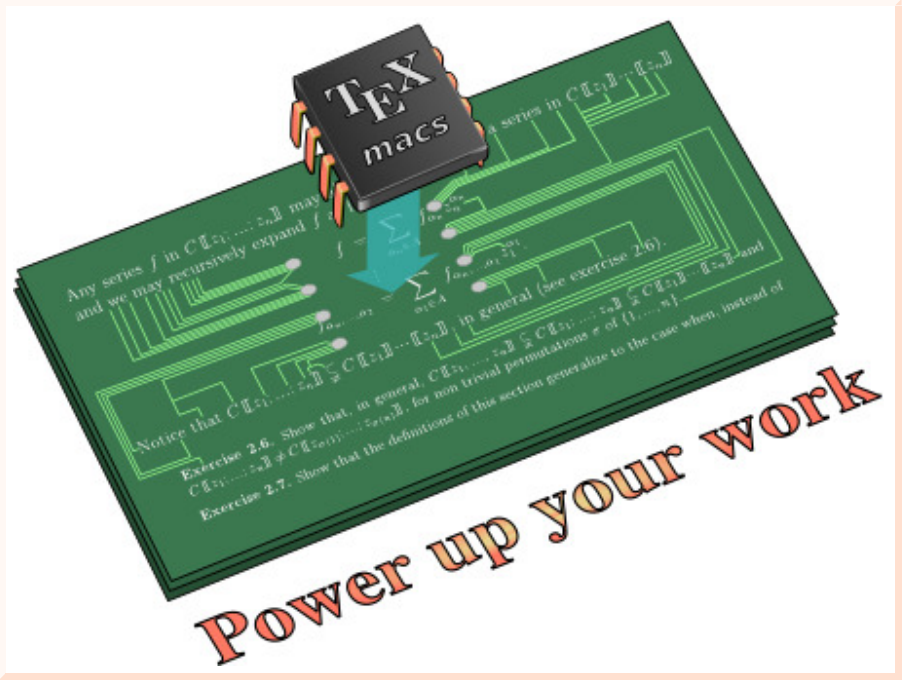
$$\|B_1\|_{\mathcal{L}} \;\leqslant\; \cdots \;\leqslant\; \|B_b\|_{\mathcal{L}}$$

Réduction de réseaux non commutative



- Si $[B_i, B_j] = 0$, alors réduire en utilisant LLL.
- Si $[B_i, B_j] \neq 0$, alors $\|[B_i, B_j]\|_{\mathcal{L}} = O(\|B_i\|_{\mathcal{L}} \|B_j\|_{\mathcal{L}}) \rightsquigarrow$ nouveaux éléments

Merci !



http://www.TEXMACS.org