Chinoiseries

par Jean-Marie Didry et Pierre-Yves Gaillard

Institut Élie Cartan, Université Henri Poincaré, didry@iecn.u-nancy.fr, gaillard@iecn.u-nancy.fr

RÉSUMÉ. *On se place sur l'anneau $\mathbb{C}[X]$. On donne des formules explicites pour le théorème chinois et on en montre diverses applications.*

MOTS-CLÉS : *théorème chinois, division euclidienne, décomposition en éléments simples, suites récurrentes de nombres complexes, exponentielle d'une matrice, équation différentielle ordinaire linéaire à coefficients constants.*

1 Préliminaires

Pour tout polynôme $P \in \mathbb{C}[X]$, où X est une indéterminée, et tout nombre complexe a notons $\mu(a, P)$ la multiplicité de a comme racine de P (avec la convention $\mu(a, 0) = +\infty$), et, pour tout couple (P, Q) tel que $P, Q \in \mathbb{C}[X], Q \neq 0$, définissons la **multiplicité de a comme racine de la fraction rationnelle** $f := P/Q$ comme étant l'entier

$$\mu(a, f) := \mu(a, P) - \mu(a, Q).$$

(Cet entier ne dépendant que de a et f, la définition a bien un sens.) Posons pour tout $a \in \mathbb{C}$

$$\mathbb{C}[X]_a := \{f \in \mathbb{C}(X) \mid \mu(a, f) \geq 0\}.$$

Une fraction rationnelle est dite **définie en** a si elle appartient à $\mathbb{C}[X]_a$. On vérifie $\mathbb{C}[X] \subset \mathbb{C}[X]_a$ et

$$f, g \in \mathbb{C}[X]_a \Rightarrow f + g,\ fg,\ f' \in \mathbb{C}[X]_a.$$

On pose pour tout $a \in \mathbb{C}, \mu \in \mathbb{N}$ et tout $f, g \in \mathbb{C}[X]_a$

$$f \equiv g \bmod (X - a)^\mu \iff f - g \in (X - a)^\mu\, \mathbb{C}[X]_a.$$

C'est évidemment une relation d'équivalence. Si $f_1, f_2, g_1, g_2 \in \mathbb{C}[X]_a$ et si $f_j \equiv g_j \bmod (X - a)^\mu$ pour $j = 1, 2$, alors

$$f_1 + f_2 \equiv g_1 + g_2, \quad f_1\, f_2 \equiv g_1\, g_2 \bmod (X - a)^\mu.$$

Pour $f \in \mathbb{C}(X)$ et $a \in \mathbb{C}$ on a

$$\mu(a, f) \neq 0 \Rightarrow \mu(a, f') = \mu(a, f) - 1.$$

Soit $f \in \mathbb{C}[X]_a$. L'implication ci-dessus entraîne

$$f \equiv 0 \bmod (X-a)^\mu \iff f^{(n)}(a) = 0 \; \forall \, n < \mu.$$

En particulier le **développement limité de f en a à l'ordre $\mu - 1$**

$$\mathrm{DL}_a^{\mu-1}(f) := \sum_{n=0}^{\mu-1} \frac{f^{(n)}(a)}{n!} \, (X-a)^n \tag{1}$$

est l'unique polynôme de degré $< \mu$ satisfaisant

$$\mathrm{DL}_a^{\mu-1}(f) \equiv f \bmod (X-a)^\mu.$$

Par suite on a pour $f, g \in \mathbb{C}[X]_a$

$$\mathrm{DL}_a^{\mu-1}(f+g) \equiv \mathrm{DL}_a^{\mu-1}(f) + \mathrm{DL}_a^{\mu-1}(g) \bmod (X-a)^\mu, \tag{2}$$

$$\mathrm{DL}_a^{\mu-1}(f\,g) \equiv \mathrm{DL}_a^{\mu-1}(f) \; \mathrm{DL}_a^{\mu-1}(g) \bmod (X-a)^\mu. \tag{3}$$

2 Théorème chinois

Fixons un polynôme non constant $D \in \mathbb{C}[X]$, notons Z l'ensemble de ses racines (on admet le théorème fondamental de l'algèbre) et posons $\mu_a := \mu(a, D)$ pour toute racine a de D.

Théorème 1 (Théorème chinois) *Soit $(P_a)_{a \in Z} \subset \mathbb{C}[X]$ une famille de polynômes. Alors l'unique solution $R \in \mathbb{C}[X]$ de degré $< \deg D$ des congruences*

$$R \equiv P_a \bmod (X-a)^{\mu_a} \quad \textit{pour tout } a \in Z.$$

est donnée par la **formule de Taylor-Gauss** *(voir [1])*

$$\boxed{R(X) = \sum_{a \in Z} \mathrm{DL}_a^{\mu_a - 1}\!\left(P_a(X) \, \frac{(X-a)^{\mu_a}}{D(X)} \right) \frac{D(X)}{(X-a)^{\mu_a}}} \tag{4}$$

En particulier si les P_a sont tous égaux à P, alors R est le reste de la division euclidienne de P par D, tandis que la partie singulière de la décomposition de

P/D en éléments simples est donnée par la **première formule de Serret** *(voir [1])*

$$\boxed{\mathrm{Sing}\left(\frac{P}{D}\right) = \sum_{a\in Z} \mathrm{DL}_a^{\mu_a-1}\!\left(P(X)\,\frac{(X-a)^{\mu_a}}{D(X)}\right)\frac{1}{(X-a)^{\mu_a}}} \tag{5}$$

Soit Q le quotient de la division euclidienne de P par D, et soit q son degré. Alors Q est donnée par la **deuxième formule de Serret** *(voir [1]) :*

$$\boxed{Q(X^{-1}) = \mathrm{DL}_0^q(f(X^{-1})\,X^q)\,X^{-q}} \tag{6}$$

Preuve. Si $a, b \in Z$ et si δ désigne le symbole de Kronecker, alors on a, en vertu du paragraphe 1,

$$\delta_{ab}\,P_a(X) = \delta_{ab}\,\left(P_a(X)\frac{(X-a)^{\mu_a}}{D(X)}\right)\,\frac{D(X)}{(X-a)^{\mu_a}}$$

$$\equiv \mathrm{DL}_a^{\mu_a-1}\!\left(P_a(X)\frac{(X-a)^{\mu_a}}{D(X)}\right)\frac{D(X)}{(X-a)^{\mu_a}} \bmod (X-b)^{\mu_b}.$$

Cela implique (4) et (5). Montrons (6). Définissons le **degré** d'une fraction rationnelle g non nulle comme étant le degré du numérateur moins celui du dénominateur ; en particulier

$$\deg g = -\mu(0, g(X^{-1})). \tag{7}$$

Ceci dit, posons $Q_0(X) := \mathrm{DL}_0^q(f(X^{-1})\,X^q)$ où $f := P/D$. D'après le paragraphe 1 il existe une fraction rationnelle g définie en 0 satisfaisant

$$f(X^{-1})\,X^q = Q_0(X) + X^{q+1}g(X),$$

et donc

$$P(X) = D(X)\,X^q Q_0(X^{-1}) + X^{-1}g(X^{-1})\,D(X).$$

Comme $g(X^{-1})$ est de degré ≤ 0 par (7), cela prouve (6). QED

Fixons une racine a de D, désignons par B l'ensemble des autres racines, pour toute application $u : B \to \mathbb{N}, b \mapsto u_b$, notons $|u|$ la somme des u_b.

Théorème 2 *Le coefficient de $(X-a)^k$ dans $\mathrm{DL}_a^{\mu_a-1}(\frac{(X-a)^{\mu_a}}{D(X)})$ est*

$$c_{a,k} := (-1)^k \sum_{\substack{u\in\mathbb{N}^B \\ |u|=k}} \prod_{b\in B} \binom{\mu_b - 1 + u_b}{\mu_b - 1} \frac{1}{(a-b)^{\mu_b+u_b}} \quad .$$

Preuve. Il suffit de multiplier les développements limités

$$\mathrm{DL}_a^{\mu_a-1}\left(\frac{1}{(X-b)^{\mu_b}}\right) = \sum_{n=0}^{\mu_a-1} \binom{\mu_b-1+n}{\mu_b-1} \frac{(-1)^n(X-a)^n}{(a-b)^{\mu_b+n}} \quad .$$

CQFD

Le polynôme R du théorème 1 est alors $\displaystyle\sum_{\substack{a\in Z\\ k+n<\mu_a}} \frac{c_{a,k}\, P_a^{(n)}(a)}{n!}\,(X-a)^{k+n}$.

3 Suites récurrentes

Soit encore D un polynôme non constant de $\mathbb{C}[X]$ et q son degré. Soit $\mathbb{C}^{\mathbb{N}}$ l'ensemble des suites de nombres complexes ; soit Δ l'opérateur de décalage qui à la suite $u \in \mathbb{C}^{\mathbb{N}}$ associe la suite $\Delta u \in \mathbb{C}^{\mathbb{N}}$ définie par $(\Delta u)_t = u_{t+1}$; soit $f \in \mathbb{C}^{\mathbb{N}}$; soient $c_0, \ldots, c_{q-1} \in \mathbb{C}$; soit y l'unique élément de $\mathbb{C}^{\mathbb{N}}$ satisfaisant

$$D(\Delta)\, y = f, \quad y_n = c_n \text{ pour tout } n < q\ ;$$

pour $(n,t) \in \mathbb{N}^2$ notons $g_n(t)$ le coefficient de X^n dans le reste de la division euclidienne de X^t par D.

Théorème 3 *Si $t \geq q$ alors* $y_t = \displaystyle\sum_{n<q} c_n\, g_n(t) + \sum_{k<t} g_{q-1}(t-1-k)\, f_k$.

La preuve de ce résultat est similaire à (et légèrement plus facile que) celle du Théorème 5 plus bas.

4 Fonctions de matrices

Soient Λ_0 l'ensemble des applications de $\mathbb{N}\times\mathbb{C}$ dans $\mathbb{C}$ et f un élément de Λ_0. Convenons de noter $f^{(n)}(a)$ [resp. $\mathrm{DL}_a^{\mu-1}(f)$] l'image d'un couple (n,a) par f [resp. le polynôme défini par (1)]. Tout polynôme P peut-être vu comme l'élément $(n,a) \mapsto P^{(n)}(a)$ de Λ_0. Il est parfois commode de désigner par $f(X)$ l'élément f de Λ_0. Étant donnés $f, g \in \Lambda_0$ on vérifie qu'il existe un unique élément $f+g$ [resp. fg] de Λ_0 satisfaisant (2) [resp. (3)] pour tout $a \in \mathbb{C}$ et tout $\mu \in \mathbb{N}^*$. Si a, μ et f sont comme ci-dessus et si g est une fraction rationnelle définie en a, alors on note $\mathrm{DL}_a^{\mu-1}(fg)$ l'unique polynôme de degré $< \mu$ tel que (3). Les opérations que l'on vient de définir sur Λ_0 prolongent les opérations correspondantes sur les polynômes.

Le théorème chinois (Théorème 1) nous invite à définir le reste $\mathcal{R}(f,D)$ de la division euclidienne d'un élément f de Λ_0 par le polynôme D fixé au début du paragraphe 2 comme étant le polynôme

$$\boxed{\mathcal{R}(f,D)(X) := \sum_{a\in Z} \mathrm{DL}_a^{\mu_a-1}\!\left(f(X)\,\frac{(X-a)^{\mu_a}}{D(X)}\right)\frac{D(X)}{(X-a)^{\mu_a}}} \tag{8}$$

C'est l'unique polynôme de degré $< \deg D$ satisfaisant

$$\mathrm{DL}_a^{\mu_a-1}(\mathcal{R}(f,D)) = \mathrm{DL}_a^{\mu_a-1}(f) \quad \forall\, a \in Z. \tag{9}$$

Si Q est un polynôme non nul, alors on a

$$\mathcal{R}(\mathcal{R}(f,DQ),D) = \mathcal{R}(f,D). \tag{10}$$

En effet, en désignant par ν_a la multiplicité de $a \in Z$ comme racine de Q, nous obtenons en vertu de (9) pour tout $a \in Z$

$$\mathrm{DL}_a^{\mu_a+\nu_a-1}(\mathcal{R}(f,DQ)) = \mathrm{DL}_a^{\mu_a+\nu_a-1}(f)$$

et donc *a fortiori*

$$\mathrm{DL}_a^{\mu_a-1}(\mathcal{R}(f,DQ)) = \mathrm{DL}_a^{\mu_a-1}(f),$$

ce qui, compte tenu de (9) et du théorème chinois, implique (10). En particulier si A est une matrice p fois p à coefficients complexes annulée par D, alors la matrice

$$f(A) := \mathcal{R}(f,D)(A)$$

ne dépend pas du choix du polynôme annulateur D, et nous obtenons pour tout $f, g \in \Lambda_0$

$$(f+g)(A) = f(A) + g(A), \quad (fg)(A) = f(A)\,g(A).$$

Notons Λ l'ensemble des applications

$$f : \mathbb{N}\times\mathbb{R}\times\mathbb{C} \to \mathbb{C}, \quad (n,t,a) \to f^{(n)}(t,a)$$

telles que $t \mapsto f^{(n)}(t,a)$ est C^∞ pour tout $(n,a) \in \mathbb{N}\times\mathbb{C}$. Définissons $\frac{\partial}{\partial t} : \Lambda \to \Lambda$ par

$$\left(\frac{\partial f}{\partial t}\right)^{(n)}(t,a) := \frac{d}{dt}\, f^{(n)}(t,a),$$

et pour $f \in \Lambda, t \in \mathbb{R}$ notons $f(t,X)$ l'élément $(n,a) \mapsto f^{(n)}(t,a)$ de Λ_0.

Si $f \in \Lambda$ satisfait $\frac{\partial f}{\partial t} = F(t,f)$, où F est une application quelconque de $\mathbb{R}\times\Lambda$ dans Λ, et si A est comme ci-dessus, alors $f(t,A)$ est solution de l'équation différentielle ordinaire $\frac{d}{dt}\, f(t,A) = F(t,f(t,A))$.

5 Matrice exponentielle

En particulier, vu que l'élément f de Λ défini par $f^{(n)}(t,a) := t^n\, e^{at}$ satisfait

$$\frac{\partial f}{\partial t} = Xf, \quad f(0,X) = 1,$$

on a $\frac{d}{dt}\ f(t,A) = A\ f(t,A)$ et $f(0,A) = 1$ pour toute matrice carrée A annulée par D, d'où l'on déduit, en posant $e^{tX} := f(t,X)$,

Théorème 4 *La matrice exponentielle donnée par la* **formule de Wedderburn** *(voir [1])*

$$\boxed{e^{tA} := \mathcal{R}(e^{tX}, D)(A)} \tag{11}$$

[voir (8)] dépend différentiablement de t et satisfait $\frac{d}{dt}\ e^{tA} = A\ e^{tA}, e^{0A} = 1$.

6 Équation différentielle

L'unique solution $y(t)$ de l'équation différentielle

$$D\left(\frac{d}{dt}\right) y(t) = f(t), \quad y^{(n)}(0) = y_n\ \forall\ n < q := \deg D, \tag{12}$$

où $f : \mathbb{R} \to \mathbb{C}$ est une fonction continue et $y_n \in \mathbb{C}$ pour $0 \le n < q$, s'exprime simplement en terme de $g_0(t), \ldots, g_{q-1}(t)$, où $g_n(t)$ est le coefficient de X^n dans $\mathcal{R}(e^{tX}, D)$:

Théorème 5 *On a la* **formule de Collet** *(voir [1])*

$$\boxed{\begin{array}{c} \mathcal{R}(e^{tX}, D) = \displaystyle\sum_{n<q} g_n(t)\, X^n \implies \\[2ex] y(t) = \displaystyle\sum_{n<q} y_n\ g_n(t) + \int_0^t g_{q-1}(t-x)\ f(x)\ dx \end{array}} \tag{13}$$

[Pour $D(X) = X^q$ on retrouve la formule de Taylor avec reste intégral.]

Preuve. En posant $v_n := y^{(n-1)}$, $v_{0n} := y_{n-1}$ pour $1 \le n \le q$, et en désignant par e_q le dernier vecteur de la base canonique de $\mathbb{C}^q$, l'équation (12) prend la forme

$$v'(t) = A\ v(t) + f(t)\ e_q, \quad v(0) = v_0$$

où A est une matrice q fois q annulée par D. On a donc

$$v(t) = e^{tA} v_0 + \int_0^t f(x)\, e^{(t-x)A} e_q\, dx.$$

Si pour toute matrice B on note $[B]_{ij}$ son coefficient en position (i, j) et $[B]_i$ sa i-ème ligne, on obtient

$$y(t) = [e^{tA}]_1\, v_0 + \int_0^t [e^{(t-x)A}]_{1q}\, f(x)\, dx.$$

Un calcul facile donne $[A^n]_{1j} = \delta_{n+1,j}$ pour $n < q$, et le Théorème 5 résulte du Théorème 4. CQFD

Les commentaires de Richard Antetomaso, Frédéric Campana, Jacques Choné, Jean-Pierre Ferrier et Pierre Marchand nous ont été très utiles.

[1] http ://www.iecn.u-nancy.fr/˜gaillard/0

5 janv. 2006