DÉTERMINATION DES FONCTIONS ZÊTA DES COURBES D'ARTIN-SCHREIER

par

Thomas Bliem

Résumé. — Nous décrirons l'algorithme de A. Lauder et D. Wan pour déterminer la fonction zêta d'une courbe d'Artin-Schreier sur un corps fini. Cet algorithme utilise des méthodes d'analyse p-adique pour obtenir une complexité polynomiale.

Étant donné un polynôme g à coefficients dans un corps fini, on s'intéresse au nombre de zéros de g dans ce corps, ainsi que dans ses corps d'extension. Plus généralement, pour chaque variété algébrique V, définie sur un corps fini F_q, on veut étudier la suite $(N_k)_{k\in\mathbf{N}}$, où pour chaque entier positif k, $N_k := \#V(\mathbf{F}_{q^k})$ est le nombre de points F_{q^k}-rationnels sur V. On représente cette suite par une série formelle, la fonction zêta de V, donnée par

$$\mathrm{Z}(V,T) := \exp \sum_{k=1}^{\infty} \frac{N_k}{k} T^k \in \mathbf{Q}[[T]].$$

Depuis les travaux de B. Dwork, [**3**], sur les conjectures de Weil, on sait que la fonction zêta $\mathrm{Z}(V,T)$ de chaque V est une fraction rationnelle : $\mathrm{Z}(V,T) \in \mathbf{Q}(T)$. Plus précisément, elle s'écrit de la forme

$$\mathrm{Z}(V,T) = \frac{P(T)}{Q(T)},$$

où P, $Q \in 1 + T\mathbf{Z}[T]$ sont des polynômes à coefficients entiers et à terme constant 1. Cette « présentation finie » permet donc de traiter la fonction zêta sur l'ordinateur — en particulier, on peut se poser le problème de la déterminer par un algorithme, ce que nous ferons par la suite.

Regardons le cas d'une hypersurface affine donnée par un polynôme en n variables $g \in \mathbf{F}_q[X] := \mathbf{F}_q[X_1, \ldots, X_n]$. Chacune des nombres N_k se détermine de façon triviale en évaluant g en tous les points de $\mathbf{F}_{q^k}^n$. Si on connaît à priori des bornes supérieures d_P, d_Q pour les degrés de P et de Q, on peut en principe déterminer $\mathrm{Z}(V,T)$ avec l'algorithme suivant, que j'appellerai l'algorithme « naïf » dans la suite :

1. Déterminer N_k pour $k \in \{1, \ldots, d_P + d_Q\}$.
2. Se servant des N_k, développer la fonction zêta en série jusqu'à l'ordre $d_P + d_Q$.

3. De la définition $\mathrm{Z}(V,T) = P(T)/Q(T)$ on déduit la congruence $Q(T)\mathrm{Z}(V,T) \equiv P(T) \mod (T^{d_P+d_Q+1})$. Par comparaison de coefficients, on obtient donc $d_P + d_Q$ équations linéaires à coefficients entiers qui permettent de trouver les coefficients de P et de Q par l'algorithme de Gauß.

Pour une description un peu plus détaillée on peut consulter [**14**], co. 2.7.

En effet, dans [**2**], E. Bombieri a déterminé des bornes explicites pour les degrés de P et de Q en fonction du degré total de g et du nombre de variables n : $\deg P + \deg Q \leq (9 + 4\deg g)^{n+1}$ (cf. Wan, [**14**], th. 2.6), à fortiori $\deg P, \deg Q \leq (9 + 4\deg g)^{n+1}$. Le problème de la détermination de la fonction zêta peut donc être considéré trivial du point de vue mathématique — il reste néanmoins le point de vue algorithmique, c'est-à-dire que l'on peut chercher des algorithmes plus efficaces. Ceci est fort nécessaire : déjà le calcul de N_k prend $O(q^{nk})$ opérations dans $\mathbf{F}_{q^k}$, donc l'algorithme naïf est exponentiel en n et en $\deg g$ sans même considérer que le calcul dans $\mathbf{F}_{q^k}$ devient de plus en plus difficile pour des grands q et k.

L'algorithme de A. Lauder et D. Wan permet de traiter le cas d'une certaine classe de courbes beaucoup plus vite, c'est le cas des courbes d'Artin-Schreier que l'on introduira maintenant.

1. Définition des courbes d'Artin-Schreier

Soit $g \in \mathbf{F}_q[X,Z]$ de la forme $g(X,Z) = (Z^p - Z)f_2(X) - f_1(X)$ où p est la caractéristique de $\mathbf{F}_q$, $q = p^a$ et $f_1, f_2 \in \mathbf{F}_q[X]$ sont deux polynômes qui ne dépendent que de X et tels que $(f_1, f_2) = 1$. Alors f_1 et f_2 n'ont pas de zéro en commun, et on peut utiliser l'équation plus compacte

$$Z^p - Z = f(X),$$

où $f = f_1/f_2 \in \mathbf{F}_p(X)$ est une fraction rationnelle, pour décrire l'ensemble des zéros de g. (Avec la convention habituelle que $x/0 = \infty \neq y$ pour tout $x \in \bar{\mathbf{F}}_q^\times$ et $y \in \bar{\mathbf{F}}_q$.) Alors une *courbe d'Artin-Schreier* V est la courbe dans $\mathbf{A}^2$ définie par un tel g. On note $V^* := V \setminus \{X = 0\}$.

2. Réduction au calcul d'une fonction L

Soit V une courbe d'Artin-Schreier. Nous utiliserons la notation abrégé $\mathrm{tr}_k := \mathrm{tr}_{\mathbf{F}_{q^k}|\mathbf{F}_p} : \mathbf{F}_{q^k} \to \mathbf{F}_p$. Soit W la variété quasi affine définie sur $\mathbf{F}_q$ par l'équation $f(X) \neq \infty$ et $W^* := W \setminus 0$. On peut dénombrer les points de $V(\mathbf{F}_{q^k})$ plus facilement en les classant suivant leur première composante :

Lemme 2.1. — *Soit $k \in \mathbf{N}$ un entier positif. On considère la projection $V(\mathbf{F}_{q^k}) \to W(\mathbf{F}_{q^k})$ sur la première composante. Alors au dessus de chaque $x \in W(\mathbf{F}_{q^k})$ il y a p points si $\mathrm{tr}_k f(x) = 0$ et il n'y en a aucun sinon.*

Démonstration. — Notons $I := \{z^p - z : z \in \mathbf{F}_{q^k}\}$. D'après le théorème 90 de D. Hilbert, la suite

$$0 \longrightarrow I \longrightarrow \mathbf{F}_{q^k} \xrightarrow{\mathrm{tr}} \mathbf{F}_p \longrightarrow 0$$

est exacte. La condition $\mathrm{tr}_k f(x) = 0$ est donc nécessaire pour trouver des points au dessus de x. La caractéristique d'Euler-Poincaré pour l'application $A \mapsto \#A$ de la suite est donc 1, d'où $\#I = p^{ak-1}$. Soit K le noyau de l'application $z \mapsto z^p - z$, alors en regardant la caractéristique de la suite exacte

$$0 \longrightarrow K \longrightarrow \mathbf{F}_{q^k} \longrightarrow I \longrightarrow 0$$

on obtient que $\#K = p$, d'où le lemme. □

On note que ce lemme permet déjà d'améliorer l'algorithme naïf pour les courbes d'Artin-Schreier : Au lieu d'évaluer tous les $f(x, z)$, il suffit d'évaluer les $\mathrm{tr}_k f(x)$. Malheureusement, cet algorithme « pseudo-naïf » est encore de croissance exponentielle.

Le lemme nous permettra dans la suite de trouver une écriture de la fonction zêta utilisant des *sommes exponentielles*. Soit ζ_p une racine p-ième primitive de l'unité, $\psi : \mathbf{F}_p \to \mathbf{Q}(\zeta_p)^\times$ le caractère de $\mathbf{F}_p$ avec $\psi(1) = \zeta_p$. On note $\psi_k := \psi \circ \mathrm{tr}_k : \mathbf{F}_{q^k} \to \mathbf{Q}(\zeta_p)^\times$ les caractères des corps d'extension de $\mathbf{F}_q$ associés à ψ.

Soit alors

$$S_k(W, f) := \sum_{x \in W(\mathbf{F}_{q^k})} \psi_k(f(x)),$$

$$L(W, f, T) := \exp \sum_{k=1}^{\infty} \frac{S_k(W, f)}{k} T^k.$$

De manière analogue on définit des suites S_k et des fonctions L pour (W^*, f) et plus généralement pour toute variété définie sur un corps fini, munie d'une fonction régulière. Les endomorphismes de corps sont étendus sur l'anneau correspondant des séries entières en agissant coefficient par coefficient, et cette opération sera notée en notation exponentielle.

Proposition 2.2. — *La fonction zêta de chaque courbe d'Artin-Schreier V s'exprime en fonction de $L(W, f, T)$ et de $\mathrm{Z}(W, T)$:*

$$\mathrm{Z}(V, T) = \mathrm{Z}(W, T) \prod_{\sigma \in G(\mathbf{Q}(\zeta_p)|\mathbf{Q})} L(W, f, T)^\sigma.$$

On note qu'il est facile de déterminer $\mathrm{Z}(W, T)$ car le complément de W dans $\mathbf{A}^1$ est une variété de dimension 0 ; on a alors effectivement obtenu une réduction du problème au calcul de la fonction $L(W, f, T)$.

Démonstration. — D'après le lemme 2.1 on a

$$\begin{aligned} \#V(\mathbf{F}_{q^k}) &= \sum_{x \in W(\mathbf{F}_{q^k})} p \cdot \delta_{\mathrm{tr}_k f(x), 0} = \sum_{x \in W(\mathbf{F}_{q^k})} \sum_{b \in \mathbf{F}_p} \psi(b \,\mathrm{tr}_k f(x)) \\ &= \sum_{b \in \mathbf{F}_p} \sum_{x \in W(\mathbf{F}_{q^k})} \psi_k(bf(x)) = \sum_{b \in \mathbf{F}_p} S_k(W, bf), \end{aligned}$$

d'où

$$\mathrm{Z}(V, T) = \prod_{b \in F_p} L(W, bf, T).$$

Regardons alors les fonctions $L(W, bf, T)$. Pour $b = 0$ on obtient $S_k(W, 0) = \#W(\mathbf{F}_{q^k})$, alors $L(W, 0, T) = \mathrm{Z}(W, T)$. Pour $b \neq 0$ on obtient

$$\begin{aligned} S_k(W, bf) &= \sum_{x \in W(\mathbf{F}_{q^k})} \psi(b \operatorname{tr}_k f(x)) = \sum_{x \in W(\mathbf{F}_{q^k})} \psi(\operatorname{tr}_k f(x))^b \\ &= \sigma(S_k(W, f)), \end{aligned}$$

où $\sigma \in G(\mathbf{Q}(\zeta_p)|\mathbf{Q})$ est l'automorphisme induit par $\zeta \to \zeta^b$. Alors $L(W, bf, T) = L(W, f, T)^\sigma$, comme énoncé dans la formule. □

Pour des raisons techniques, il est souvent préférable d'exclure le point 0 et de travailler sur W^*. Cela ne pose pas de problème, car

$$L(W, f, T) = L(W^*, f, T) \cdot L(\mathbf{A}^0_{\mathbf{F}_q}, f, T),$$

et cette dernière fonction L se calcule à la main :

$$\begin{aligned} L(\mathbf{A}^0_{\mathbf{F}_q}, f, T) &= \exp \frac{\psi_k(f(0))}{k} T^k = \exp \frac{\psi_1(f(0))^k}{k} T^k \\ &= \mathrm{Z}(\mathbf{A}^0_{\mathbf{F}_q}, \psi_1(f(0))T) = \frac{1}{1 - \psi_1(f(0))T}. \end{aligned}$$

3. Une formule de trace pour les nombres S_k

Pour les calculs pratiques, on utilise l'observation suivante : Un entier $i \in \{0, \ldots, p^N - 1\}$ est uniquement déterminé par sa classe d'équivalence modulo (p^N). Nous voulons appliquer cette observation aux coefficients de la fonction zêta de V. Notre stratégie sera donc de

1. déterminer des bornes supérieures pour les coefficients de la fonction zêta et de
2. calculer $L(W, f, T)$ à une précision p-adique suffisante près pour trouver ces coefficients.

Effectivement, il existe une formule classique qui décrit $L(W, f, T)$ comme déterminant de Fredholm d'un certain opérateur complètement continu que nous étudions maintenant. Nous allons rapporter les résultats généraux en incluant seulement les démonstrations pour le cas plus facile où $f \in \mathbf{F}_q[X]$ est un polynôme.

Commençons par quelques définitions. Soit $\mathcal{O}$ l'anneau de valuation de $\mathbf{C}_p$. L'application de Teichmüller $\bar{\mathbf{F}}_p \to \mathcal{O}$, c'est-à-dire la section de $\mathcal{O} \to \bar{\mathbf{F}}_p$ dont l'image consiste uniquement en racines $(p^l - 1)$-ièmes de l'unité ($l \in \mathbf{N}$) et de 0, sera noté parfois ω, parfois $x \mapsto \hat{x}$. Valuation et valeur absolue sur $\mathbf{C}_p$ sont normalisés en sorte que $v(p) = 1$ et $|p| = 1/p$. Pour chaque nombre rationnel positif δ soit

$$A_\delta := \{z \in \mathbf{C}_p : |z| \leq p^\delta, |\hat{f}_2(z)| \geq p^{-\delta}\}.$$

(C'est le domaine D_{δ,δ,f_2} de D. Reich, [**10**].) Quand f est un polynôme, A_δ est simplement la boule fermée de rayon p^δ et de centre 0 dans $\mathbf{C}_p$, $A_\delta = \bar{B}_0(p^\delta)$. Soit $H(A_\delta)$ l'espace des éléments analytiques sur A_δ, muni de la norme $\|\xi\| := \sup_{z \in A_\delta} |\xi(z)|$. Le lemme suivant nous permet de considérer les éléments de $H(A_\delta)$ comme des séries formelles.

Lemme 3.1. — *Pour chaque nombre rationnel positif δ, soit $L(\delta)$ le sous-espace de $\mathbf{C}_p[[X]]$ composé des séries formelles $\xi = \sum_{i=0}^{\infty} b_i X^i$, telles que $v(b_i) - \delta i \to \infty$ $(i \to \infty)$, muni de la norme $\|\xi\| := p^{-\inf_i v(b_i)-\delta i}$. Alors le développement de Taylor en 0 est un isomorphisme isométrique*

$$H(\bar{B}_0(p^\delta)) \to L(\delta)$$

d'espaces de Banach sur $\mathbf{C}_p$.

Ce lemme est démontré par exemple dans l'introduction aux nombres p-adiques de Y. Amice, [**1**], § 4.1. Dans le cas où f est un polynôme, cas nous intéressant particulièrement, il fournit déjà la traduction désirée entre les fonctions et les séries. Dans le cas général, on doit encore appliquer le théorème de Mittag-Leffler, voir [**1**], th. 4.7.7, pour obtenir des objets formels. Compte tenu du lemme, nous n'allons pas systématiquement distinguer $H(\bar{B}_0(p^\delta))$ et $L(\delta)$, mais essayerons de changer la notation suivant l'aspect mis en avant.

Du point de vue algorithmique, il est avantageux de travailler avec des grands δ : du point de vue des séries formelles, un grand domaine de convergence se traduit par une convergence rapide des coefficients vers 0, alors il suffit de considérer des développements d'ordre petit pour atteindre une précision p-adique donnée. On note que ce n'est qu'une règle heuristique dans cette version-là : Le comportement de convergence ne change pas si on modifie un nombre fini arbitraire de coefficients. Nous introduisons pour cette raison encore le $\mathcal{O}$-module $\underline{L}(\delta)$ des éléments de $L(\delta)$ qui satisfont pour tout i à l'inégalité $v(b_i) \geq \delta i$. Les éléments de $L(\delta)$ seront dit avoir *taux de décroissance* δ et les éléments de $\underline{L}(\delta)$ seront dit avoir *taux de décroissance strict* δ.

Définition 3.2. — Une *tour de fonctions* sur W est une suite d'applications $g_k : W(\mathbf{F}_{q^k}) \to \mathbf{C}_p$ pour $k \in \mathbf{N}$. Une *représentation analytique* d'une tour de fonctions (g_k) est une fonction $G \in H(A_\delta)$ pour un $\delta > 0$ telle que pour tout $k \in \mathbf{N}, x \in W(\mathbf{F}_{q^k})$

$$g_k(x) = \prod_{i=0}^{k-1} G(\hat{x}^{q^i}).$$

On notera alors $G_k(z) := \prod_{i=0}^{k-1} G(z^{q^i})$ pour des $z \in A_\delta$. On définit ainsi des représentations analytiques des tours sur W^* ou plus généralement sur des sous-variétés arbitraires de $\mathbf{A}^1_k$ pour un corps fini k.

Un des exemples les plus importants est la représentation analytique suivante de la tour de caractères (ψ_k) sur $\mathbf{A}^1_{\mathbf{F}_q}$: Soit $\pi \in \mathbf{C}_p$ tel que $\pi^{p-1} = -p$ et que $\zeta_p \equiv 1 + \pi \mod (\pi^2)$.

Lemme 3.3. — *Soit θ la série formelle*

$$\theta := \exp \pi(X - X^p).$$

Alors, pour chaque $\delta < (p-1)/p^2$: $\theta \in \underline{L}(\delta)$ et la fonction correspondante à θ sur $H(\bar{B}_0(p^\delta))$ est une représentation analytique de $(\psi \circ \mathrm{tr}_{\mathbf{F}_{p^l}|\mathbf{F}_p})_{l \in \mathbf{N}}$ définie sur $\mathbf{A}^1_{\mathbf{F}_p}$.

Le lemme est démontré par ex. dans [**8**], § 4.1. Pour obtenir une représentation analytique de (ψ_k) sur $\mathbf{A}^1_{\mathbf{F}_q}$, on peut par changement de variable $l = ak + s$ prendre $\theta_1(z) := \prod_{s=0}^{a-1} \theta(z^{p^s})$. Du taux de décroissance strict de θ on déduit que $\theta_1 \in H(\bar{B}_0(p^\delta))$ et que sa série est dans $\underline{L}(\delta)$ pour

$$\delta < \frac{p-1}{p^{a-1}p^2} = \frac{p-1}{p^{a+1}}. \tag{1}$$

(On note que ce procédé fonctionne en général pour une extension du corps de définition et que la construction est transitive.) Si a est grand, le domaine de convergence s'est beaucoup réduit, ce qui est désavantageux pour les algorithmes. Nous allons trouver au paragraphe 6 une solution à ce problème.

Utilisant la fonction θ, on peut construire une représentation analytique de la tour $(\psi_k \circ f)$:

Proposition 3.4. — *La formule* $G(z) := \theta_1(\hat{f}(z)) \cdot \exp \pi(\hat{f}(z)^q - \hat{f}(z^q))$ *définit une fonction* $G \in H(A_\delta)$ *pour un* $\delta > 0$ *et* G *est une représentation analytique de la tour* $(\psi_k \circ f)$ *sur* W^**, c'est-à-dire*

$$\psi_k(f(x)) = \prod_{i=0}^{k-1} G(\hat{x}^{q^i}) = G_k(\hat{x})$$

pour tout entier positif k *et tout* $x \in W^*(\mathbf{F}_{q^k})$.

Pour une démonstration voir Ph. Robba, [**11**], formules (6.3.1) et (6.3.6). Pour le cas où $f = \sum_{j=0}^{d} a_j X^j$ est un polynôme, on peut trouver une représentation analytique plus facilement :

Proposition 3.5. — *Dans le cas où* f *est un polynôme de degré* d*, la formule*

$$G(z) := \prod_{j=0}^{d} \theta_1(\hat{a}_j z^j) = \prod_{j=0}^{d} \prod_{s=0}^{a-1} \theta((\hat{a}_j z^j)^{p^s}).$$

définit une fonction $G \in H(A_\delta)$ *pour* $\delta < \frac{p-1}{dp^{a+1}}$*, dont la série correspondante est un élément de* $\underline{L}(\delta)$*. La fonction* G *est une représentation analytique de la tour* $(\psi_k \circ f)$ *sur* W *et a fortiori sur* W^*.

Démonstration. — Pour $x \in W(\mathbf{F}_{q^k}) = \mathbf{F}_{q^k}$

$$\begin{aligned} \psi_k(f(x)) &= \psi_k(\sum_{j=0}^{d} a_j x^j) = \prod_{j=0}^{d} \psi_k(a_j x^j) \\ &= \prod_{j=0}^{d} \theta_k(\hat{a}_j \hat{x}^j) = \prod_{j=0}^{d} \prod_{i=0}^{k-1} \theta_1((\hat{a}_j \hat{x}^j)^{q^i}). \end{aligned}$$

Dans la dernière expression, l'argument de θ_1 s'écrit $(\hat{a}_j \hat{x}^j)^{q^i} = \hat{a}_j (\hat{x}^{q^i})^j$. Il reste alors à démontrer que G est de taux de décroissance strict δ pour $\delta < \frac{p-1}{dp^{a+1}}$. Cela provient du fait que les coefficients $\hat{a}_j$ de $\hat{f}$ sont des entiers et du lemme 3.3. □

Corollaire 3.6. — *Les nombres S_k s'obtiennent par la formule p-adique*

$$S_k(W^*, f) = \sum_{z \in \omega(W^*(\mathbf{F}_{q^k}))} G_k(z).$$

Si f est un polynôme, on peut aussi remplacer W^* par W.

La formule de trace de D. Reich permet alors d'exprimer $S_k(W^*, f)$ comme trace d'un certain opérateur complètement continu sur un certain espace de Banach p-adique que nous allons introduire maintenant. Pour une introduction à la théorie des tels opérateurs on peut consulter l'article [**12**] de J.-P. Serre.

Fixons pour la suite un δ tel que $G \in H(A_{\delta/q})$, c'est-à-dire

$$\delta < \frac{p-1}{dp} \tag{2}$$

d'après la proposition 3.5. Les fonctions de $H(A_{\delta/q})$ agissent sur $H(A_{\delta/q})$ par multiplication, et l'endomorphisme correspondant à ξ sera toujours noté ξ. Soit $\Psi : H(A_{\delta/q}) \to H(A_\delta)$ l'opérateur donné par

$$\Psi\xi(z) := q^{-1} \sum_{w^q = z} \xi(w).$$

Dans le cas où f est un polynôme, $A_\delta = \bar{B}_0(p^\delta)$, on note que l'opération de Ψ sur les séries formelles est donné par $\Psi(\sum_{i=0}^\infty b_i X^i) = \sum_{i=0}^\infty b_{qi} X^i$. Nous considérons maintenant

$$\alpha := \Psi \circ G \circ \mathrm{res} : H(A_\delta) \to H(A_{\delta/q}) \to H(A_{\delta/q}) \to H(A_\delta).$$

La restriction res est complètement continue (Serre, [**12**], § 3, co. de la pr. 4) et G et Ψ sont continus, alors α est complètement continu et possède donc une trace.

Théorème 3.7. — *Les nombres S_k s'obtiennent par la formule de trace*

$$S_k(W^*, f) = (q^k - 1) \operatorname{tr} \alpha^k.$$

Démonstration. — La formule de trace de D. Reich, [**10**], § c, th. 4, constate que

$$\operatorname{tr} \alpha^k = (q^k - 1)^{-1} \sum_{z \in \omega(W^*(\mathbf{F}_{q^k}))} G_k(z)$$

pour tout $k \in \mathbf{N}$. Reich démontre en effet une version de la formule pour plusieurs variables et il utilise l'hypothèse que la partie homogène de degré maximal du polynôme définissant W^* soit sans facteur carré. Mais d'après le remarque de Ph. Robba, [**11**], p. 232, on n'a pas besoin de cette condition dans notre cas d'une seule variable. Alors le théorème est une conséquence directe du corollaire 3.6.

Traitons à la main le cas où f est un polynôme. Alors $\omega(W^*(\mathbf{F}_{q^k}))$ est simplement le groupe μ_{q^k-1} des (q^k-1)-ièmes racines de l'unité. Pour les calculs explicites, il sera plus pratique de travailler avec des séries formelles. Si on choisit des éléments η, μ avec $v(\eta) = \delta, v(\mu) = \delta/q$, alors les familles $(\eta^i X^i), (\mu^i X^i)$ sont des bases orthonormales de $L(\delta), L(\delta/q)$. On devrait alors calculer les puissances de la matrice de α dans ces bases pour calculer la trace. Mais les éléments diagonaux des puissances de la matrice de α restent les mêmes si on multiplie chaque élément de base par une constante. (Pour

la matrice elle-même c'est évident, pour les puissances c'est obtenu par un calcul explicite.) Alors pour faciliter le calcul regardons la matrice M dans la « pseudo-base » (X^i). Pour plus d'explications on peut lire l'appendice A. Alors un calcul explicite démontre que

$$M = (g_{qi-j})_{i,j}\,, \tag{3}$$

où les g_i sont les coefficients de la série G.

Alors pour $k = 1$:

$$\begin{aligned} S_1(W^*, f) &= \sum_{z\in\mu_{q-1}} G(z) = \sum_{z\in\mu_{q-1}} \sum_{i=0}^{\infty} g_i z^i \\ &= \sum_{i=0}^{\infty} g_i \sum_{z\in\mu_{q-1}} z^i = \sum_{j=0}^{\infty} g_{(q-1)j}(q-1) \\ &= (q-1)\operatorname{tr}\alpha. \end{aligned}$$

Pour le cas général on remplace Ψ par Ψ^k et G par G_k pour obtenir

$$S_k(W^*, f) = \prod_{z\in\mu_{q^k-1}} G_k(z) = (q^k-1)\operatorname{tr}\Psi^k \circ G_k.$$

On utilise le fait que $G \circ \Psi = \Psi \circ G(X^q)$. Alors en regroupant les Ψ vers la gauche dans α^k on obtient $\alpha^k = (\Psi\circ G)^k = \Psi^k \circ G \circ G(X^q) \circ \cdots \circ G(X^{q^{k-1}}) = \Psi^k \circ G_k$, d'où le théorème. □

4. Une formule de déterminant pour la fonction L

La formule de trace pour les $S_k(W^*, f)$ permet immédiatement de donner une formule de déterminant pour $L(W^*, f, T)$. Pour chaque endomorphisme complètement continu Φ notons $\det(1 - T\Phi)$ son déterminant de Fredholm.

Proposition 4.1. — *La fonction L de (W^*, f) s'écrit*

$$L(W^*, f, T) = \frac{\det(1 - T\alpha)}{\det(1 - Tq\alpha)}.$$

Démonstration. — Dans [**12**], § 5, co. 3 de la pr. 7, Serre à démontré que pour tout endomorphisme complètement continu Φ

$$\det(1 - T\Phi) = \exp \sum_{k=1}^{\infty} \frac{-\operatorname{tr}\Phi^k}{k} T^k. \tag{4}$$

Dans notre situation d'après le théorème 3.7 :

$$\begin{aligned} L(W^*, f, T) &= \exp \sum_{k=1}^{\infty} \frac{S_k(W^*, f)}{k} T^k = \exp \sum_{k=1}^{\infty} \frac{(q^k - 1) \operatorname{tr} \alpha^k}{k} T^k \\ &= \left(\exp \sum_{k=1}^{\infty} \frac{\operatorname{tr} \alpha^k}{k} (qT)^k \right) \cdot \left(\exp \sum_{k=1}^{\infty} \frac{-\operatorname{tr} \alpha^k}{k} T^k \right) \\ &= \det(1 - Tq\alpha)^{-1} \cdot \det(1 - T\alpha), \end{aligned}$$

ce qui est la formule énoncée. (Strictement, pour justifier la notation, on doit démontrer que $\det(1 - T(q\alpha)) = \det(1 - (qT)\alpha)$, ce qui se fait par un calcul similaire à celui que nous venons de faire.) □

5. Application algorithmique de la formule de déterminant

Regardons maintenant comment on peut utiliser la formule de déterminant pour calculer explicitement des fonctions zêta. Nous considérons le cas où f est un polynôme de degré d tel que $(d, p) = 1$. Nous supposons en outre que $p > 2$. La condition sur le degré n'est pas une restriction, car, par le procédé décrit dans [**6**], § 2.2, no. 4, on peut trouver pour tout polynôme $\tilde{f}$ un polynôme f tel que les courbes d'Artin-Schreier associées sont isomorphes et que $(\deg f, p) = 1$. On sait que $L(W, f, T)$ est un polynôme de degré $d - 1$, purement de poids 1 ([**6**], p. 36). D'après le lemme 2.2, la fonction zêta de V se décompose

$$\mathrm{Z}(V, T) = \frac{P(T)}{1 - qT},$$

où $P(T) = \prod_{\sigma \in G(\mathbf{Q}(\zeta_p)|\mathbf{Q})} L(W, f, T)^\sigma \in \mathbf{Z}[T]$ est un polynôme de degré $(p-1)(d-1)$, purement de poids 1. En regardant l'écriture factorisée de P on voit que ses coefficients b_k satisfont à l'inégalité $|b_k|_\infty \leq C^2_{(p-1)(d-1)} \sqrt{q}^k \leq 2^{(p-1)(d-1)} p^{(p-1)(d-1)a/2} \leq p^{(p-1)(d-1)(1+a/2)}$. Soit alors $N := \lfloor (p-1)(d-1)(1 + a/2) + 1 \rfloor$, où pour chaque nombre rationnel r, $\lfloor r \rfloor$ est l'entier qui satisfait à $\lfloor r \rfloor \leq r < \lfloor r \rfloor + 1$. C'est, d'après l'observation du début du paragraphe 3, à la précision p-adique p^N près que nous devons les calculer.

Notre stratégie est donc de calculer $\det(1 - T\alpha)$ à p^N près. Comme la matrice $M = (m_{ij})$ de α ne contient que des entiers p-adiques, il suffit de la calculer à p^N près. D'après le taux de décroissance strict de G, proposition 3.5, et de notre connaissance le la matrice $M = (m_{ij})$ de α, formule (3) :

$$v(m_{ij}) \geq \frac{p-1}{dp^{a-1}}(qi - j), \tag{5}$$

bien sûr $m_{ij} = 0$ si $qi - j < 0$. Les coefficients intéressants sont donc ceux situés dans la bande

$$0 \leq qi - j \leq dp^{a+1}(d-1)(1 + a/2) =: C.$$

La matrice M se présente alors comme indiqué dans la figure 1. Pour calculer la trace de M ainsi que la trace de ses puissances, il suffit de calculer les composantes m_{ij}

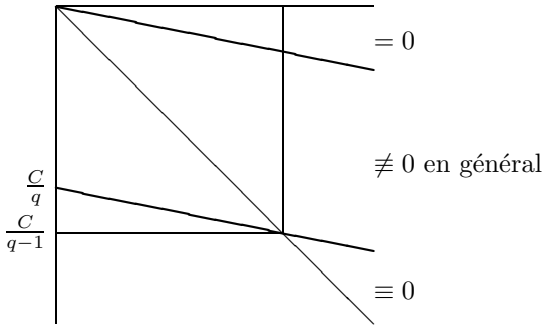

FIGURE 1. Schéma de la matrice M

avec $i, j \leq C/(q-1)$ à p^N près. Comme le déterminant de Fredholm est déterminé par ces traces, ces m_{ij} suffisent aussi pour le calculer à notre précision désirée près.

Estimons maintenant le temps nécessaire pour effectuer l'algorithme. Bien que nous ayons travaillé dans $\mathbf{C}_p$, tous les résultats intermédiaires sont des éléments de $\mathbf{Z}_p[\zeta_{q-1}, \pi]$, où ζ_{q-1} est une racine $(q-1)$-ième primitive de l'unité, qui est utilisée pour exprimer les relèvements de Teichmüller des coefficients de f. Tous les calculs peuvent êtres effectués dans l'anneau $\mathbf{Z}_p[\zeta_{q-1}, \pi]/(p^N) =: B$.

Faisons d'abord un sommaire des complexités des opérations de base que nous allons utiliser, d'après [**8**], § 3.2.2, le. 5, et [**6**], § 8.1. Tous les temps doivent être mesurés en opérations élémentaires de bits : comme nous voulons estimer le temps en fonction de d, a et p, le calcul dans tout anneau naturel à considérer est variable lui-aussi, donc une indication en tels opérations ne serait pas significative. Pour éviter les facteurs logarithmiques dans la notation O, étant donné des fonctions réelles r, s nous écrivons $r = \tilde{O}(s)$ si $r = O(s \log(s+1))$. Les opérations dans B peuvent être réalisés en $\tilde{O}(Nap)$ et l'application de Teichmüller peut être calculée en $O(N^2(a \log p)^3)$. Les polynômes dans $B[X]$ de degré ∂ peuvent être multipliés en $\tilde{O}(\partial)$ opérations dans B, soit $\tilde{O}(\partial \cdot Nap)$ opérations élémentaires. Les matrices dans $B^{(m,m)}$ peuvent être multipliées en $O(m^3)$ opérations dans B, soit $\tilde{O}(m^3 \cdot Nap)$ opérations élémentaires, déjà avec l'algorithme standard.

L'algorithme, étant donné un polynôme f, fonctionne comme suit :

1. Déterminer la série G à p^N près ;
2. calculer M à p^N près ;
3. déterminer le polynôme $L(W^*, f, T)$ à p^N près ;
4. déterminer le polynôme $L(W, f, T) = (1 - \psi_1(a_0)T)^{-1} L(W^*, f, T)$ à p^N près ;
5. sortir la fraction rationnelle $\mathrm{Z}(V, T) = (1 - qT)^{-1} \prod_{\sigma \in G(\mathbf{Q}(\zeta_p)|\mathbf{Q})} L(W, f, T)^\sigma$.

Pour effectuer la *première étape*, on doit multiplier les $O(da)$ polynômes

$$\theta((\hat{a}_j X^j)^{p^s}) \bmod (p^N)$$

pour $j = 0, \ldots, d$ et $s = 0, \ldots, a-1$. Les degrés de ces polynômes sont bornés par $C = O(d^2 a p^{a+1})$. Alors l'ensemble de la multiplication prend

$$\tilde{O}(da \cdot d^2 a p^{a+1} \cdot Nap) = \tilde{O}(d^4 a^4 p^{a+3})$$

opérations élémentaires. Comme le temps du calcul des $\theta((\hat{a}_j X^j)^{p^s}) \bmod (p^N)$ est majoré par cette multiplication, c'est le temps nécessaire pour cette étape. Pour plus de détails, voir [**8**], § 6.3.1, le. 30.

Pour la *deuxième étape*, il n'y a rien à faire — elle est seulement inclue dans l'algorithme pour faciliter la compréhension.

Pour la *troisième étape*, nous utilisons encore le fait que le déterminant de Fredholm s'exprime par les traces des puissances de M. Grâce à notre connaissance de $\deg L(W, f, T)$, il nous suffit de calculer ces puissances jusqu'à M^{d-1}. Cela fait $O(d)$ multiplications de matrices de taille $C/(q-1) = O(d^2 ap)$, soit un temps total de

$$\tilde{O}(d \cdot (d^2 ap)^3 \cdot Nap) = \tilde{O}(d^8 a^5 p^5)$$

opérations élémentaires. Le déterminant de Fredholm de $q\alpha$ est simplement $\det(1 - Tq\alpha) = \det(1 - (qT)\alpha)$, et ne nécessite donc pas de calcul supplémentaire. On note que nous avons utilisé ici que $\det(1 - Tq\alpha)$ est à coefficients entiers pour ne pas perdre de précision lors de la division. C'est pour cette condition que nous avons supposé que $p > 2$ — elle se démontre alors par un calcul direct. Pour rattraper le cas $p = 2$, on peut déterminer une borne inférieure $-c$ des valeurs de ces coefficients et déterminer $\det(1 - T\alpha)$ à la précision p^{N+c} augmentée de c. (Comme des déterminants de Fredholm sont des fonctions entières, une telle borne existe nécessairement.)

Pour la *quatrième et cinquième étape*, le temps nécessaire est majoré par le temps des étapes déjà prises en compte.

La complexité totale de l'algorithme est donc

$$\tilde{O}(d^8 a^5 p^{\max\{5, a+3\}}),$$

alors pour des petites valeurs de a nous sommes arrivés à un algorithme polynomial. Une amélioration pour obtenir un algorithme polynomial en a sera présentée au paragraphe 7.

6. Une décomposition de α

On peut améliorer la vitesse de l'algorithme en utilisant une décomposition de α que nous étudierons maintenant. Nous allons seulement considérer dans ce paragraphe le cas où f est un polynôme, $f = \sum_{j=0}^{d} a_j X^j$, pour le cas général on peut consulter [**7**] et [**11**], § 6. Soit $\tau \in G(\mathbf{C}_p | \mathbf{Q}_p)$ un relèvement de l'automorphisme de Frobenius $x \mapsto x^p$ de $\bar{\mathbf{F}}_p$ avec $\tau(\pi) = \pi$.

Proposition 6.1. — *Soit $\tilde{G}(z) := \prod_{j=0}^{d} \theta(\hat{a}_j z^j)$. Alors $\tilde{G} \in H(A_\delta)$ pour $\delta < \frac{p-1}{dp^2}$, et la série correspondante est un élément de $\underline{L}(\delta)$ pour de tels δ. Puis*

$$G(z) = \prod_{s=0}^{a-1} \tilde{G}^{\tau^s}(z^{p^s})$$

pour tout z avec $v(z) < \frac{p-1}{dp^{a+1}}$.

On note que l'action de τ sur $\mathbf{Q}_p(\zeta_{q-1}, \pi)$ est déterminé par les données et que c'est dans ce corps où se trouvent les coefficients de $\tilde{G}$.

Démonstration. — L'estimation du taux de décroissance strict est immédiate d'après celle de θ dans lemme 3.3. L'égalité se démontre par le calcul suivant avec les séries formelles correspondantes :

$$\begin{aligned}\prod_{s=0}^{a-1} \tilde{G}^{\tau^i}(X^{p^s}) &= \prod_{s=0}^{a-1}\prod_{j=0}^{d} \theta(\hat{a}_j X^{jp^s})^{\tau^s} = \prod_{j=0}^{d}\prod_{s=0}^{a-1} \theta^{\tau^s}(\tau^s(\hat{a}_j) X^{jp^s}) \\ &= \prod_{j=0}^{d}\prod_{s=0}^{a-1} \theta((\hat{a}_j X^j)^{p^s}) = G(X),\end{aligned}$$

où le passage à la deuxième ligne est justifié par les faits suivants : Les coefficients de θ sont des éléments de $\mathbf{Q}_p(\pi)$, d'où $\theta^\tau = \theta$. L'action de τ sur les $\hat{a}_j$ est donné par $\tau(\hat{a}_j) = \hat{a}_j^p$ parce que c'est par définition l'action dans le corps résiduel et que l'ensemble μ_{q-1} des racines $(q-1)$-ièmes de l'unité est invariant par τ. □

Pour chaque série formelle $\xi = \sum_{i=0}^{\infty} b_i X^i$ à coefficients dans $\mathbf{C}_p$ posons

$$\tilde{\Psi}\xi := \sum_{i=0}^{\infty} \tau^{-1}(b_{pi}) X^i.$$

Pour chaque espace vectoriel M sur $\mathbf{C}_p$ on note $M^{\tau^{-1}}$ l'espace conjugué, c'est-à-dire l'espace sur lequel les scalaires agissent via $c * \xi := \tau^{-1}(c)\xi$. Alors pour tout nombre rationnel positif δ, $\tilde{\Psi}$ est un opérateur linéaire $H(A_{\delta/p}) \to H(A_\delta)^{\tau^{-1}}$. Il sera parfois plus convenable de regarder $\tilde{\Psi}$ comme opérateur τ^{-1}-linéaire $H(A_{\delta/p}) \to H(A_\delta)$, c'est-à-dire qui satisfait à $\tilde{\Psi}(c\xi) = \tau^{-1}(c)\tilde{\Psi}(\xi)$ pour tout $c \in \mathbf{C}_p$ et $\xi \in H(A_{\delta/p})$. Nous considérons maintenant

$$\tilde{\alpha} := \tilde{\Psi} \circ \tilde{G} \circ \mathrm{res} : H(A_\delta) \to H(A_{\delta/p}) \to H(A_{\delta/p}) \to H(A_\delta)^{\tau^{-1}}.$$

C'est un endomorphisme complètement continu d'après l'argument déjà utilisé pour α.

Lemme 6.2. — *Si δ satisfait à (2), alors α et $\tilde{\alpha}$ sont définies et*

$$\alpha = \tilde{\alpha}^a$$

sur l'ensemble des éléments de $L(\delta)$ dont les coefficients sont dans $\mathbf{Q}_p(\zeta_{q-1}, \pi)$.

On note qu'il n'y a pas d'espoir que l'égalité soit valable pour tous les éléments de $H(A_\delta)$: α est linéaire tandis que $\tilde{\alpha}^a$ est τ^{-a}-linéaire.

Démonstration. — Toutes les égalités sont sous-entendues valables pour les séries à coefficients dans $\mathbf{Q}_p(\zeta_{q-1}, \pi)$. La formule

$$\tilde{\Psi} \circ \tilde{G}(X^p) = \tilde{G}^{\tau^{-1}} \circ \tilde{\Psi} \tag{6}$$

se démontre en observant que ses deux membres sont τ^{-1}-linéaires et en l'évaluant explicitement sur les monômes.

Cette formule nous servira à voir que pour tout entier positif b

$$\tilde{\Psi}^b \circ \prod_{s=0}^{b-1} \tilde{G}^{\tau^i}(X^{p^i}) = (\tilde{\Psi} \circ \tilde{G})^b, \tag{7}$$

qui se spécialise dans l'énoncé en $b = a$ d'après la proposition 6.1 et du fait que $\tilde{\Psi}^a = \Psi$. La formule (7) est triviale pour $b = 1$. Pour $b > 1$ on applique (6) pour obtenir

$$\tilde{\Psi}^b \circ \prod_{s=0}^{b-1} \tilde{G}^{\tau^i}(X^{p^i}) = \left(\tilde{\Psi}^{b-1} \circ \prod_{s=0}^{b-2} \tilde{G}^{\tau^i}(X^{p^i}) \right) \circ \left(\Psi \circ \tilde{G} \right)$$

et on procède par récurrence. □

7. Application algorithmique de la décomposition

Le but de ce paragraphe est d'améliorer l'algorithme du paragraphe 5 pour obtenir une croissance polynomiale en a. Nous continuons, comme dans ce paragraphe, à supposer que f est un polynôme de degré d tel que $(d, p) = 1$ et que $p > 2$. Notre stratégie est d'utiliser une version de matrices du lemme 6.2 pour trouver la matrice M de α plus facilement. Soit alors $\tilde{M} = (\tilde{m}_{ij})$ la matrice de $\tilde{\alpha}$ par rapport à la pseudo-base (X^i). Comme l'application $\tilde{\alpha}$ n'est pas linéaire, M ne se calcule pas directement comme puissance a-ième de $\tilde{M}$, mais d'après la formule suivante :

Lemme 7.1. — *La matrice M s'écrit en fonction de $\tilde{M}$ comme*

$$M = \prod_{s=0}^{a-1} \tilde{M}^{\tau^{-s}},$$

où τ^{-1} agit sur $\tilde{M}$ composante par composante.

Démonstration. — D'après le lemme 6.2, la matrice M de α est celle de $\tilde{\alpha}^k$. Pour chaque matrice N notons $[N]$ l'application τ^{-1}-linéaire de matrice N. Alors regardant les images des éléments X^i on voit que

$$[N_1] \circ [N_2] = [N_1 N_2^{\tau^{-1}}]$$

pour chaque paire de matrices (N_1, N_2), identité dont on dérive le lemme par récurrence. □

La matrice $\tilde{M}$ elle-même est donnée par $\tilde{m}_{ij} = \tilde{g}_{pi-j}$ où $\tilde{G} =: \sum_{i=0}^{\infty} \tilde{q}_i X^i$. On procède donc comme qu'au paragraphe 5 avec les modifications suivantes : L'estimation (5) s'écrit maintenant d'après la proposition 6.1

$$v(\tilde{m}_{ij}) \geq \frac{p-1}{dp^2}(pi - j). \tag{8}$$

Les coefficients intéressants sont donc ceux situés dans la bande

$$0 \leq pi - q \leq dp^2(d-1)(1 + a/2) =: \tilde{C}.$$

Il suffit alors de calculer les composantes $\tilde{m}_{ij}$ avec $i, j \leq \tilde{C}/(p-1)$ à p^N près.

L'algorithme, étant donné un polynôme f, fonctionne comme suit :

1. Déterminer la série $\tilde{G}$ à p^N près ;
2. calculer $\tilde{M}$ à p^N près ;
3. déterminer M à p^N près ;
4. déterminer le polynôme $L(W^*, f, T)$ à p^N près ;
5. déterminer le polynôme $L(W, f, T) = (1 - \psi_1(a_0)T)^{-1} L(W^*, f, T)$ à p^N près ;
6. sortir la fraction rationnelle $\mathrm{Z}(V, T) = (1 - qT)^{-1} \prod_{\sigma \in G(\mathbf{Q}(\zeta_p)|\mathbf{Q})} L(W, f, T)^\sigma$.

Pour effectuer la *première étape*, on doit multiplier les $O(d)$ polynômes

$$\theta(\hat{a}_j X^j) \bmod (p^N)$$

pour $j = 0, \ldots, d$. Les degrés de ces polynômes sont bornés par $\tilde{C} = O(d^2 a p^2)$. Alors l'ensemble la multiplication prend

$$\tilde{O}(d \cdot d^2 a p^2 \cdot Nap) = \tilde{O}(d^4 a^3 p^4)$$

opérations élémentaires. Comme le temps du calcul des $\theta(\hat{a}_j X^j) \bmod (p^N)$ est majoré par cette multiplication, c'est le temps nécessaire pour cette étape.

Pour la *deuxième étape*, il n'y a rien à faire — elle est seulement inclue dans l'algorithme pour faciliter la compréhension.

Pour la *troisième étape*, d'après [**8**], § 6.3.1, le. 32, le temps décisif est celui de la multiplication des matrices, soit

$$\tilde{O}((d^2 ap)^3 \cdot Nap) = \tilde{O}(d^7 a^5 p^5)$$

opérations élémentaires.

La *quatrième étape* est égale à la troisième étape de l'algorithme du paragraphe 5, et prend donc un temps total de

$$\tilde{O}(d \cdot (d^2 ap)^3 \cdot Nap) = \tilde{O}(d^8 a^5 p^5)$$

opérations élémentaires.

Pour la *cinquième et sixième étape*, le temps nécessaire est majoré par le temps des étapes déjà prises en compte.

La complexité totale de l'algorithme est donc

$$\tilde{O}(d^8 a^5 p^5),$$

c'est-à-dire nous avons obtenu un algorithme polynomial en p, a et d. Le but des paragraphes suivants sera de réduire les exposants.

8. Passage à l'homologie

Le but de ce paragraphe est d'interpréter la formule de déterminant de la proposition 4.1 comme la caractéristique d'Euler-Poincaré d'un certain complexe et de déduire une formule évaluable plus efficacement en passant à l'homologie. Nous continuerons à supposer que f est un polynôme, et de plus que $f(0) = 0$. Nous n'avons pas besoin dans ce paragraphe des conditions sur d et p.

Soit $\mathcal{A}$ la catégorie des endomorphismes complètement continus d'espaces de Banach sur un corps local K, dont, pour deux objets $u : A \to A$ et $v : B \to B$, les morphismes sont les applications linéaires continues $E : A \to B$ telles que le diagramme

$$\begin{array}{ccc} A & \xrightarrow{E} & B \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} \\ A & \xrightarrow{E} & B \end{array}$$

soit commutatif. Le fait que $u \mapsto \det(1-Tu)$ soit une application d'Euler-Poincaré sur $\mathcal{A}$ à valeurs dans $K[[T]]$ n'est alors qu'une autre interprétation du lemme 2 dans [**12**], § 5 de J.-P. Serre. On note que l'argument de Serre utilise le fait que la valuation de K soit discrète — nous pouvons quand même utiliser ce résultat, car les endomorphismes que nous considérons s'obtiennent des endomorphismes des espaces de Banach sur $\mathbf{Q}_p(\zeta_{q-1}, \pi)$ en tenseurisant avec $\mathbf{C}_p$.

Construisons alors une application linéaire continue $D : L(\delta) \to L(\delta)$, telle que

$$\begin{array}{ccccccc} 0 & \longrightarrow & L(\delta) & \xrightarrow{D} & L(\delta) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle q\alpha} & & \downarrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & L(\delta) & \xrightarrow{D} & L(\delta) & \longrightarrow & 0 \end{array}$$

soit un diagramme commutatif dans la catégorie des espaces de Banach, c'est-à-dire un complexe dans la catégorie des endomorphismes. Pour Ψ au lieu de α, un tel opérateur est donné par le lemme suivant, qui se démontre par un calcul direct :

Lemme 8.1. — *Soit E l'opérateur différentiel $E = X \circ \frac{d}{dX}$. Alors*

$$E \circ q\Psi = \Psi \circ E.$$

Pour le passage de Ψ à α, observons que Ψ, α et E s'étendent naturellement en des endomorphismes de $\mathbf{C}_p[[X]]$. On suppose dans un premier temps que $\alpha = R^{-1} \circ \Psi \circ R$ est conjugué à Ψ par un automorphisme R de $\mathbf{C}_p[[X]]$. Alors pour $D := R^{-1} \circ E \circ R$:

$$\begin{aligned} \alpha \circ D &= R^{-1} \circ \Psi \circ E \circ R = q\ R^{-1} \circ E \circ \Psi \circ R \\ &= q\ D \circ \alpha. \end{aligned}$$

Tout ce qui nous reste à faire est alors de trouver un R convenable, et de démontrer que $L(\delta)$ est invariant par l'opérateur D obtenu ainsi.

Lemme 8.2. — *Soit $R := \exp \pi \hat{f}$. Alors $\alpha = R^{-1} \circ \Psi \circ R$.*

On note que nous avons utilisé la condition que $f(0) = 0$ pour donner un sens à $\exp \pi \hat{f}$.

Démonstration. — La série R s'écrit

$$\begin{aligned} R = \exp \pi \hat{f} &= \prod_{j=0}^{d} \exp \pi \hat{a}_j X^j = \prod_{j=0}^{d} \exp \sum_{l=0}^{\infty} \pi((\hat{a}_j X^j)^{p^l} - (\hat{a}_j X^j)^{p^{l+1}}) \\ &= \prod_{j=0}^{d} \prod_{l=0}^{\infty} \theta((\hat{a}_j X^j)^{p^l}). \end{aligned}$$

Dans la démonstration de la proposition 6.1, nous avons vu que

$$G = \prod_{j=0}^{d} \prod_{s=0}^{a-1} \theta((\hat{a}_j X^j)^{p^s}),$$

et donc $G(X) = R(X)/R(X^q)$ puisque $\hat{a}_j^q = \hat{a}_j$ pour tout j :

$$\begin{aligned} G(X) \cdot R(X^q) &= \prod_{j=0}^{d} \prod_{s=0}^{a-1} \prod_{k=0}^{\infty} \theta((\hat{a}_j X^j)^{p^s}) \theta((\hat{a}_j X^j)^{p^{ak}}) \\ &= \prod_{j=0}^{d} \prod_{s=0}^{a-1} \prod_{k=0}^{\infty} \theta((\hat{a} X^j) p^{ak+s}) = R(X) \end{aligned}$$

par changement de variable $l = ak+s$. On en déduit que $\alpha = \Psi \circ G = \Psi \circ R(X^q)^{-1} \circ R = R^{-1} \circ \Psi \circ R$. □

Définissons alors $D := R^{-1} \circ E \circ R$. Le fait que $L(\delta)$ est invariant par D est immédiat en observant que D s'écrit

$$D = X \circ \frac{d}{dX} + \pi X \frac{d\hat{f}}{dX}$$

de D, écriture de toute façon plus pratique pour l'application algorithmique. Précisons le choix de δ : Depuis (2) nous avons supposé que $\delta < \frac{p-1}{dp}$ pour que $L(\delta)$ soit invariant par α. Supposons maintenant en plus que

$$\delta \leq \frac{1}{d(p-1)} \tag{9}$$

pour que $\pi X \frac{d\hat{f}}{dX} \in \underline{L}(\delta)$ et que $\underline{L}(\delta)$ soit invariant par D. Soient H_1 l'endomorphisme de $\ker D$ induit par $q\alpha$, H_0 l'endomorphisme de $L/D(L(\delta))$ induit par α. Alors de la théorie des applications d'Euler-Poincaré nous avons immédiatement obtenu que $L(W^*, f, T) = \det(1 - TH_0)/\det(1 - TH_1)$. Effectivement, $\ker D = 0$, alors :

Proposition 8.3. — *La fonction L de (W^*, f) s'écrit*

$$L(W^*, f, T) = \det(1 - TH_0).$$

Démonstration. — Il faut voir que $D = X \circ \frac{d}{dX} + \pi X \frac{d\hat{f}}{dX}$ est injectif, c'est-à-dire que la seule solution F de l'équation différentielle

$$\frac{dF}{dX} = -\frac{d\pi\hat{f}}{dX}F \tag{10}$$

dans L est 0. Cherchons d'abord les solutions de (10) dans $\mathbf{C}_p[[X]]$. D'après le théorie des équations différentielles linéaires d'ordre 1, ce sont les multiples de $\exp -\pi\hat{f}$. Mais $\exp -\pi\hat{f} \notin L$, donc la seule solution dans L est 0. □

On peut de manière analogue introduire la fonction $\tilde{H}_0$ qui vérifie l'égalité $\tilde{H}_0^a = H_0$ pour les séries à coefficients dans $\mathbf{Q}_p(\zeta_{q-1}, \pi)$.

9. Application algorithmique de l'homologie

Le but de ce paragraphe est d'améliorer l'algorithme du paragraphe 7 en passant à l'homologie. Nous supposons, comme dans ce paragraphe, que f est un polynôme de degré d tel que $(d, p) = 1$ et que $p > 2$; puis, comme au paragraphe 8, nous supposons que $f(0) = 0$. Les conditions (2) et (9) sur δ sont donc vérifiées par le choix

$$\delta := \frac{1}{d(p-1)},$$

que l'on fixe pour la suite.

L'endomorphisme α agit par restriction sur le $\mathcal{O}$-module $\underline{L}(\delta)$. En fait, comme les coefficients de G sont des éléments de $\mathbf{Z}_p[\zeta_{q-1}, \pi]$, on peut regarder l'action sur le $\mathbf{Z}_p[\zeta_{q-1}, \pi]$-module libre $\mathcal{L}$ de base

$$\left(\pi^{\lceil i(p-1)\delta \rceil} X^i\right)_{i \in \mathbf{N}_0} = \left(\pi^{\lceil i/d \rceil} X^i\right)_{i \in \mathbf{N}_0}, \tag{11}$$

où pour chaque nombre rationnel r, $\lceil r \rceil$ est l'entier qui satisfait à $\lceil r \rceil - 1 < r \leq \lceil r \rceil$. Ces restrictions de α préservent le déterminant de Fredholm.

D'après [**6**], § 5, le. 7.1, un système de représentants de $\mathcal{L}/D(\mathcal{L})$ est le sous-module engendré par $1, \pi X, \ldots, \pi X^{d-1}$; le représentant d'un élément de $\mathcal{L}/D(\mathcal{L})$ dans ce module sera appelé la *forme normale* de cet élément. On vérifie directement que

$$\pi^{\lceil i/d \rceil} X^i = D((d\hat{a}_d)^{-1} \pi^{\lceil i/d \rceil - 1} X^{i-d}) + r,$$

où

$$\begin{aligned} r &= -\left(X\frac{d}{dX} + \pi \sum_{j=0}^{d-1} j\hat{a}_j X^j\right)((d\hat{a}_d)^{-1}\pi^{\lceil i/d \rceil - 1} X^{i-d}) \\ &= -(d\hat{a}_d)^{-1}\pi^{\lceil i/d \rceil - 1}(i-d)X^{i-d} - (d\hat{a}_d)^{-1}\pi^{\lceil i/d \rceil} \sum_{j=1}^{d-1} j\hat{a}_j X^{i-d+j}. \end{aligned}$$

Cette formule peut servir à réduire des polynômes dans $\mathcal{L}$ en forme normale, en enlevant successivement les termes de plus grand degré. Pour les calculs pratiques, ainsi que pour la réduction des séries, nous observons dans la formule de réduction que l'ordre de tous les coefficients de la forme normale de bX^i est au moins $v(b) - \frac{i}{d(p-1)}$.

En combinant cela avec notre connaissance sur les valeurs des coefficients des $\tilde{\alpha}(X^i)$, (8), on voit que les termes de grand ordre n'ont pas d'influence à la forme normale à une précision p-adique limité près. En fait, pour atteindre une précision de p^N de la forme normale, il suffit de de calculer les $\tilde{\alpha}$ sur les éléments de base à $p^{4(N+1)}$ près. (Le calcul est explicité dans [**6**], §7.1, le. 27.)

L'algorithme, étant donné un polynôme f, fonctionne comme suit :

1. Déterminer la série $\tilde{G}$ à $p^{4(N+1)}$ près ;
2. calculer la matrice $\tilde{M}'$ de $\tilde{H}_0$ à p^N près ;
3. déterminer la matrice M' de H_0 à p^N près ;
4. déterminer le polynôme $L(W^*, f, T)$ à p^N près ;
5. déterminer le polynôme $L(W, f, T) = (1 - \psi_1(a_0)T)^{-1}L(W^*, f, T)$ à p^N près ;
6. sortir la fraction rationnelle $\mathrm{Z}(V, T) = (1 - qT)^{-1} \prod_{\sigma \in G(\mathbf{Q}(\zeta_p)|\mathbf{Q})} L(W, f, T)^\sigma$.

Pour effectuer la *première étape*, on doit multiplier les $O(d)$ polynômes

$$\theta(\hat{a}_j X^j) \bmod (p^{4(N+1)})$$

pour $j = 0, \ldots, d$. Les degrés de ces polynômes sont bornés par $\tilde{C}' = O(d^2ap^2)$. Alors toute la multiplication prend

$$\tilde{O}(d \cdot d^2ap^2 \cdot Nap) = \tilde{O}(d^4a^3p^4)$$

opérations élémentaires. Comme le calcul des $\theta(\hat{a}_j X^j) \bmod (p^{4(N+1)})$ est majoré par cette multiplication, c'est le temps nécessaire pour cette étape.

La *deuxième étape* nécessite le calcul de $\tilde{\alpha}$ pour les d éléments de la base de $\mathcal{L}/D(\mathcal{L})$ et la réduction en forme normale. Le degré initial de $\tilde{\alpha} \bmod (p^{4(N+1)})$ est $O(Ndp)$, et chaque étape de la réduction nécessite $O(d)$ opérations dans $\mathbf{Z}_p[\zeta_{q-1}, \pi]/(p^{4(N+1)})$. Ça fait un total de

$$\tilde{O}(d \cdot Ndp \cdot d \cdot Nap) = \tilde{O}(d^5a^3p^4)$$

opérations élémentaires.

Pour la *troisième étape*, d'après [**8**], § 6.3.1, le. 32, le temps décisif est celui de la multiplication des matrices, soit

$$\tilde{O}(d^3 \cdot Nap) = \tilde{O}(d^4a^2p^2)$$

opérations élémentaires.

La *quatrième étape*, d'après [**6**], § 8.2, fo. (32) prend

$$\tilde{O}(d^5a^2p^2)$$

opérations élémentaires.

Pour la *cinquième et sixième étape*, le temps nécessaire est majoré par le temps des étapes déjà prises en compte.

La complexité totale de l'algorithme est donc

$$\tilde{O}(d^5a^3p^4).$$

Appendice A
L'espace $\mathcal{H}^\dagger(A)$

L'objectif de ce paragraphe est de clarifier les phénomènes qui apparaissent quand on considère des opérateurs qui agissent naturellement sur plusieurs espaces $H(A_\delta)$ avec δ rationnel positif. Cela permet d'une part de mieux comprendre la notion de « pseudo-base » introduite dans le paragraphe 3, et d'autre part de faciliter le passage à l'étude des articles [**7**] de Lauder et Wan et [**11**] de Ph. Robba, qui utilisent un certain espace $\mathcal{H}^\dagger(A)$.

Soit toujours $A_\delta = \bar{B}_0(p^\delta)$ pour simplicité. Il y a alors une identification naturelle de $H(A_\delta)$ avec l'espace $L(\delta)$ des séries formelles à coefficients dans $\mathbf{C}_p$ avec un taux de convergence de δ, voir lemme 3.1. On se fixe pour chaque δ un $\eta_\delta \in \mathbf{C}_p$ tel que $v(\eta_\delta) = \delta$. Alors une base orthonormale de $L(\delta)$ est donnée par

$$\left(\eta_\delta^i X^i\right)_{i\in\mathbf{N}_0}. \tag{12}$$

On note que ces bases ne sont pas canoniques, car il n'y a pas de choix naturel pour les η_δ. Pour $\delta' < \delta$, l'application naturelle sera toujours notée res, bien que dans l'interprétation des séries il s'agit plutôt d'une inclusion que d'une restriction. Soit $\mathcal{H}^\dagger(A) := \varinjlim H(A_\delta)$. Du point de vue des séries formelles, $\mathcal{H}^\dagger(A) = \bigcup L(\delta)$.

Définition A.1. — Une *famille admissible* est une famille $(\Phi_\delta)_{0<\delta\leq\Delta}$ d'opérateurs complètement continus sur $H(A_\delta)$, tels que pour chaque paire $0 < \delta' < \delta \leq \Delta$ le diagramme

$$\begin{array}{ccc} L(\delta) & \xrightarrow{\Phi_\delta} & L(\delta) \\ \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\ L(\delta') & \xrightarrow{\Phi_{\delta'}} & L(\delta') \end{array}$$

est commutatif. Un *opérateur admissible* sur $\mathcal{H}^\dagger(A)$ est un opérateur Φ induit par une famille admissible.

Un calcul explicite démontre le lemme suivant :

Lemme A.2. — *Soit $(\Phi_\delta)_{0<\delta\leq\Delta}$ une famille admissible. Pour chaque δ soit $(m_{ij}^{(\delta)})$ la matrice de Φ_δ par rapport à la base orthonormale* (12)*. Alors pour chaque paire $0 < \delta, \delta' \leq \Delta$ et chaque i, j*

$$m_{ij}^{(\delta')} = \left(\frac{\eta_\delta}{\eta_{\delta'}}\right)^{i-j} m_{ij}^{(\delta)}.$$

Du lemme A.2 on déduit que la trace de Φ_δ^k pour $k \in \mathbf{N}$ et le déterminant de Fredholm de Φ_δ sont indépendantes de δ. Puis, si un opérateur admissible est défini par deux familles admissibles, ces familles coïncident à des changements de Δ près.

Définition A.3. — Soit Φ un opérateur admissible sur $\mathcal{H}^\dagger(A)$. Alors on définit les traces et le déterminant de Fredholm

$$\operatorname{tr}\Phi^k := \operatorname{tr}\Phi_\delta^k, \quad \det(1 - T\Phi) := \det(1 - T\Phi_\delta)$$

pour un élément Φ_δ d'une famille admissible arbitraire induisant Φ.

Il n'est donc pas nécessaire de travailler dans les espaces $H(A_\delta)$, mais on peut restreindre la discussion à $\mathcal{H}^\dagger(A)$ — ce qui est préférable parce que l'on n'est pas obligé de donner un Δ explicite. Dans la littérature on trouve souvent la notion des opérateurs nucléaires sur $\mathcal{H}^\dagger(A)$ auxquels on peut établir un lien comme suit :

Proposition A.4. — *Chaque opérateur admissible sur $\mathcal{H}^\dagger(A)$ est nucléaire.*

On va utiliser la définition d'un opérateur nucléaire de [**9**], c'est-à-dire Φ est dit nucléaire si pour chaque valeur propre $\lambda \neq 0$ il existe une décomposition $\mathcal{H}^\dagger(A) = N \oplus F$ telle que N et F sont invariants par Φ, N est l'espace caractéristique de λ, $N = \bigcup_k \ker(\Phi - \lambda)^k$, et est de dimension finie, et que $\Phi - \lambda$ est bijectif sur F ; puis on exige que les valeurs propres non nulles forment soit un ensemble fini, soit une suite convergente vers 0.

Démonstration. — L'outil principal est la proposition 12 de Serre, [**12**], § 7, qui établit un lien entre les deux notions pour chaque $H(A_\delta)$. Ce qui nous reste à faire est alors le passage à la limite inductive. Soit Φ un opérateur admissible sur $\mathcal{H}^\dagger(A)$, et soit λ une valeur propre de Φ. Alors λ est aussi une valeur propre de Φ_δ pour un $\delta > 0$. D'après la proposition citée, $H(A_\delta)$ se décompose en $H(A_\delta) = N_{\lambda,\delta} \oplus F_{\lambda,\delta}$, ainsi que chaque $H(A_{\delta'})$ pour $\delta' < \delta$. Ces $N_{\lambda,\delta'}$ et $F_{\lambda,\delta'}$ forment des suites croissantes. Posons $N_\lambda := \bigcup N_{\lambda,\delta'}$, $F_\lambda := \bigcup F_{\lambda,\delta'}$. Effectivement, tous les $N_{\lambda,\delta'}$ sont de même dimension finie, donc égaux. Les espaces N_λ et F_λ sont invariants par Φ et $\mathcal{H}^\dagger(A) = N \oplus F$, et toutes les propriétés exigées sont immédiates. La suite des valeurs propres converge vers 0, parce que le déterminant de Fredholm est une fonction entière, qui n'a donc qu'un nombre fini de zéros dans chaque domaine bornée. □

Étant donné que le δ choisi dans la représentation d'un opérateur admissible n'a pas d'influence sur le déterminant de Fredholm qui nous intéresse, il est superflu de devoir le trouver, ainsi que l'élément η_δ qui nous a servi à définir une base de $H(A_\delta)$. Définissons alors $\eta_0 := 1$ et $m_{ij}^{(0)}$ par la formule du lemme A.2. Alors la matrice $M := (m_{ij}^{(0)})$ peut toujours servir à calculer le déterminant de Fredholm de Φ, et en plus elle est plus pratique. Ceci explique l'introduction ad hoc de la « pseudo-base » dans la démonstration du théorème 3.7. Il faut quand même se rendre compte que les matrices obtenues ainsi ne sont pas des matrices habituelles par rapport à des bases orthonormales : Par exemple, le critère [**12**], § 3, co. de la pr. 4, pour reconnaître une application complètement continue en regardant sa matrice ne fonctionne pas dans nos exemples.

Références

[1] Y. Amice – *Les nombres p-adiques*, Le mathématicien, no. 14, Presses Universitaires de France, 1975.

[2] E. Bombieri – "On exponential sums in finite fields, II", *Inventiones math.* **47** (1978), p. 29–39.

[3] B. Dwork – "On the rationality of the zeta function of an algebraic variety", *Amer. j. math.* **82** (1960), p. 631–648.

[4] ———, "On the zeta function of a hypersurface", *Publ. math. IHES* **12** (1962), p. 5–68.

[5] N. Koblitz – *p-adic numbers, p-adic analysis, and zeta-functions*, Graduate texts in mathematics, no. 58, Springer, 1977.

[6] A. G. B. Lauder & D. Wan – "Computing zeta functions of Artin-Schreier curves over finite fields", *LMS j. computat. math.* **5** (2002), p. 34–55.

[7] ———, "Computing zeta functions of Artin-Schreier curves over finite fields II", prépublication, 2002.

[8] ———, "Counting points on varieties over finite fields of small characteristic", prépublication, 2002.

[9] M. van der Put – "The cohomology of Monsky and Washnitzer", *Mém. SMF (nouv. sér.)* **23** (1986), p. 33–59.

[10] D. Reich – "A p-adic fixed point formula", *Amer. j. math.* **91** (1969), p. 835–850.

[11] Ph. Robba – "Index of p-adic differential operators: III. Application to twisted exponential sums", *Astérisque* **119–120** (1984), p. 191–266.

[12] J.-P. Serre – "Endomorphismes complètement continus des espaces de Banach p-adiques", *Publ. math. IHES* **12** (1962), p. 69–85.

[13] ———, "Majoration de sommes exponentielles", *Astérisque* **41–42** (1977), p. 111–126.

[14] D. Wan – "Algorithmic theory of zeta functions over finite fields", prépublication, 2002.

---

25 juin 2003

Thomas Bliem, Institut Fourier, Université de Grenoble I • *E-mail :* tbliem@gmx.de