Fonctions zêta de variétés algébriques sur des corps finis

Gabriel Bartlett

12 décembre 2022

Maîtres de stage :
Prof. Alan Lauder
Bernard Le Stum

Table des matières

Introduction

Ce rapport présente le travail effectué lors du stage de recherche de fin de deuxième année à l'École Normale Supérieure de Rennes, réalisé au Mathematical Institude, University of Oxford, sous la direction de Prof. Alan Lauder, et de Bernard Le Stum.

Le sujet de ce rapport, les fonctions zêta de variétés algébriques sur des corps finis, est un thème central de théorie des nombres. Il fait intervenir des outils de domaines mathématiques variés, tels l'analyse p-adique, et les questions d'homologie. Il fait en particulier l'objet de plusieurs décennies de recherche en théorie des nombres, motivées notamment par les conjectures de Weil.

Ce rapport élabore les bases de cette théorie, ainsi que la démonstration du théorème de la trace de Dwork. Le rapport contient aussi quelques résultats admis sur les fonction L.

1 Définitions et propriétés de base

Nous allons introduire dans cette partie les définitions de bases qui serviront notamment à énoncer et démontrer le théorème de la trace de Dwork.

1.1 Fonctions Zêta

Dans toute la suite on fixe un entier $n \in \mathbf{N}$.

1.1.1 Hypersurfaces

Soit k un corps infini.

Notons $\mathbf{A}^n(k)$ l'espace affine de dimension n sur k. Notons $\mathbf{P}^n(k)$ l'espace projectif de dimension n sur k, ie l'ensemble $\mathbf{A}^{n+1}(k) \setminus \{0\}/\sim$, où $\sim$ est la relation d'équivalence sur $\mathbf{A}^{n+1}(k) \setminus \{0\}$ définie par

$$x \sim x' \iff \exists \lambda \in k^* \text{ tel que } \lambda * x = x'$$

Notons la classe de $x \in \mathbf{A}^{n+1}(k) \setminus \{0\}$, $\bar{x} = [x_0, \ldots, x_n] \in \mathbf{P}^n(k)$.

Définition 1 (Variété (algébrique) affine)**.** Un ensemble $V \subset \mathbf{A}^n(k)$ est une *variété (algébrique) affine* s'il existe des polynômes $P_1, \ldots, P_m \in k[X_1, \ldots, X_n]$ tels que

$$V = \{x \in \mathbf{A}^n(k) \mid \forall i \in [\![1, m]\!], P_i(x) = 0\}$$

Nous noterons aussi $V = V(P_1, \ldots, P_m)$. Dans la suite nous traiterons essentiellement le cas où V est engendré par un seul polynôme f. Nous appelons un tel ensemble un *hypersurface affine*, et nous noterons $V(P) = \mathcal{H}_P$.

Définition 2 (Variété (algébrique) projective)**.** Soient $P_1, \ldots, P_m \in k[X_0, \ldots, X_n]$ des polynômes *homogènes*. La *variété projective* définie par $P_1, \ldots, P_m$ est l'ensemble

$$\tilde{V}(P_1, \ldots, P_m) = \{\bar{x} \in \mathbf{P}^n(k) \mid P_1(x) = \cdots = P_m(x) = 0\} \subset \mathbf{P}^n(k)$$

On définit l'hypersurface projectives $\tilde{\mathcal{H}}_P$ de façon analogue.

Remarque. Ces ensembles sont bien définis. Vérifions cela dans le cas des hypersurface projectives. Soit $x \in \mathbf{A}^{n+1}(k)$ tel que $P(x) = 0$ et soit $\lambda \in k^*$. Alors $P(\lambda x) = \lambda^{\deg(P)} P(x) = 0$. Donc $\forall x' \in \bar{x}, P(x') = 0$.

Pour $P \in k[X_1, \ldots, X_n]$, on pourra considérer le *polynôme homogénéisé* de P que l'on notera $\tilde{P} \in k[X_0, \ldots, X_n]$ défini ainsi :

$$\tilde{P} = X_0^{\deg(P)} P\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right)$$

$\tilde{P}$ est alors un polynôme homogène. On peut donc considérer son hypersurface projective $\tilde{\mathcal{H}}_{\tilde{P}}$. C'est sur cet espace que porterons les conjectures de Weil.

Exemple 1. Prenons $k = \mathbf{R}$, $n = 2$ et $P = X_1 X_2^2 + X_1^2 + 1$. Alors

$$\tilde{P} = X_1 X_2^2 + X_0 X_1^2 + X_0^3 \in \mathbf{R}[X_0, X_1, X_2]$$

Remarque. On peut rendre la notation d'une hypersurface plus précise en notant le corps concerné, ie $\mathcal{H}_P(P)$ (resp. $\tilde{\mathcal{H}}_P(k)$). Ainsi, on peut définir l'hypersurface de P sur une extension k' de k en considérant P comme un polynôme sur k'. On notera en effet, pour toute extension k' de k,

$$\mathcal{H}_P(k') = \{x \in \mathbf{A}^n(k') \mid P(x) = 0\}$$

On fera de même pour les variété algébriques en général.

Remarque. L'espace $\mathcal{H}_P(k)$ dépend aussi de l'entier n mais celui-ci sera implicite et fixé dans la suite.

Remarque. Le fait que k soit infini assure que tout ensemble de $\mathbf{A}^n(k)$ ne soit pas forcément une variété algébrique. Nous allons cependant employer l'abus de notation $V((P_1, \ldots, P_m), k)$ pour désigner la restriction au corps fini k de la variété algébrique définie par $(P_1, \ldots, P_m)$ sur le corps infini $\bar{k}$, la clôture algébrique de k.

1.1.2 Cas des caractéristiques finies

Dans toute la suite nous allons considérer des variétés algébriques uniquement sur des corps de caractéristique finie.

Soit p un nombre premier et notons $\mathbf{F}_{p^s}$ le corps à p^s éléments pour tout $s \in \mathbf{N}^*$. Soit q une puissance de p. Soit un polynôme $f \in \mathbf{F}_q[X_1, \ldots, X_n]$. Pour $s \in \mathbf{N}^*$, on pose

$$N_s = |\mathcal{H}_f(\mathbf{F}_{q^s})|$$

le nombre de point de $\mathcal{H}_f$ sur $\mathbf{F}_{q^s}$.

La suite $(N_s)_{s \in \mathbf{N}^*}$ est alors l'objet principal de ce rapport. C'est dans le but d'étudier cette suite que nous définissons la fonction zêta de l'hypersurface $\mathcal{H}_f$ comme suit.

Cependant, nous allons aussi nous intéresser à une version légèrement modifiée de cette suite, en particulier pour prouver la formule de la trace de Dwork. On définit ainsi, pour $s \in \mathbf{N}^*$

$$N_s^* = |\{x \in (\mathbf{F}_{q^s}^*)^n \mid f(x) = 0\}|$$

ie. le nombre d'éléments dans $\mathcal{H}_f(\mathbf{F}_{q^s})$ dont tous les coordonnées sont non nulles.

Définition 3 (Fonction Zêta)**.** La *fonction zêta* de l'hypersurface $\mathcal{H}_f$ sur le corps $\mathbf{F}_q$, est la fonction génératrice

$$Z(\mathcal{H}_f/\mathbf{F}_q, T) = \exp\left(\sum_{i=1}^{\infty} \frac{N_i}{i} T^i\right)$$

On généralise cette définition de façon intuitive aux variétés algébriques affines et projectives, définies par plusieurs polynômes.

Nous verrons dans la suite que cette fonction est bien définie et est même une fraction rationnelle à coefficients dans $\mathbf{Z}$.

Lemme 1. *La fonction $Z(\mathcal{H}_f/\mathbf{F}_q, T)$ est bien définie sur le disque de centre 0 et de rayon q^{-n}.*

Démonstration. Il suffit de démontrer ce résultat pour la série $\sum_{i=1}^{\infty} \frac{N_i}{i} T^i$. Pour $i \in \mathbf{N}^*$, $0 \leq N_i \leq |\ \mathbf{F}_{q^s}^n\ | = q^{in}$. Alors

$$0 \leq \sum_{i=1}^{\infty} \frac{N_i}{i} T^i \leq \sum_{i=1}^{\infty} \frac{(q^n T)^i}{i}$$

dont le rayon de convergence est q^{-n}. D'où le résultat. □

Exemple 2.

1. Calculons la fonction zêta d'un point $P = (a_1, \ldots, a_n)$ dans $\mathbf{A}^n_{\mathbf{F}_q}$. Alors pour tout $s \in \mathbf{N}^*$, $\{P\} = V(X_1 - a_1, \ldots, X_n - a_n)(\mathbf{F}_{q^s})$, et $N_s = 1$. Ainsi

$$Z(V/\mathbf{F}_q, T) = \exp\left(\sum_{i=1}^{\infty} \frac{T^i}{i}\right) = \exp(-\log(1-T)) = \frac{1}{1-T}$$

2. Calculons maintenant la fonction zêta de l'espace $\mathbf{A}^n_{\mathbf{F}_q}$ tout entier. Ici $f = 0$ et pour $s \in \mathbf{N}^*$, $N_s = (q^n)^s$. Donc

$$Z(\mathcal{H}_f/\mathbf{F}_q, T) = \exp\left(\sum_{i=1}^{\infty} \frac{(q^n T)^i}{i}\right) = \exp(-\log(1-q^n T)) = \frac{1}{1-q^n T}$$

3. Considérons maintenant le cas d'un espace projectif. Calculons la fonction zêta de l'espace projectif $\mathbf{P}^n_{\mathbf{F}_q}$. Pour $s \in \mathbf{N}^*$,

$$N_s = |\mathbf{P}^n_{\mathbf{F}_{q^s}}| = \frac{q^{s(n+1)} - 1}{q^s - 1} = 1 + q^s + \cdots + (q^s)^n$$

Donc

$$\begin{aligned} Z(\mathcal{H}_f/\mathbf{F}_q, T) &= \exp\left(\sum_{i=1}^{\infty} \frac{1 + q^i + \cdots + (q^i)^n}{i} T^i\right) \\ &= \prod_{l=0}^{n} \exp\left(\sum_{i=1}^{\infty} \frac{(q^l T)^i}{i}\right) \\ &= \prod_{l=0}^{n} \frac{1}{1-q^l T} \end{aligned}$$

4. Considérons $f = X_1 X_2 = \tilde{f}$ Alors pour $s \in \mathbf{N}^*$, $N_s = 2q^s - 1$. Donc

$$\begin{aligned} Z(\mathcal{H}_f/\mathbf{F}_q, T) &= \exp\left(\sum_{s\geq 1} \frac{(qT)^s}{s}\right)^2 \exp\left(-\sum_{s\geq 1} \frac{T^s}{s}\right) \\ &= \frac{1-T}{(1-qT)^2} \end{aligned}$$

Calculons maintenant $Z(\tilde{\mathcal{H}}_f/\mathbf{F}_q, T)$. Dans ce cas, pour $s \in \mathbf{N}^*$,

$$\tilde{N}_s = 2q^s + 1$$

car

$$\begin{aligned} \tilde{N}_s &= |\{[x_0, x_1, x_2] \mid \tilde{f}([x_0, x_1, x_2]) = 0\}| \\ &= N_s + |\{[0,1,0], [0,0,1]\}| \end{aligned}$$

où le second terme est l'ensemble des points à l'infini. Ainsi,

$$Z(\tilde{\mathcal{H}}_f/\mathbf{F}_q, T) = \frac{1}{(1-T)(1-qT)^2}$$

Remarque. Notons la fonction zêta de RIEMANN

$$\zeta(x) = \sum_{i=1}^{\infty} \frac{1}{i^x}$$

Soient $f_1, \ldots, f_r \in \mathbf{Z}[X_1, \ldots X_n]$. Pour tout p premier, on peut définir $V((f_1, \ldots, f_r), p)$ la variété affine associée aux polynômes obtenus en réduisant les coefficients de $f_1, \ldots, f_r$ modulo p. On définit ainsi la *fonction zêta globale* de $(f_1, \ldots, f_r)$,

$$Z((f_1, \ldots, f_r), x) = \prod_{p \text{ premier}} Z(V((f_1, \ldots, f_r), p)/\mathbf{F}_p, p^{-x})$$

Prenons $f_1, \ldots, f_n$ comme dans l'exemple ci-dessus, $f_i = (X_i - a_i)$ avec les $a_1, \ldots, a_n \in \mathbf{Z}$. Ainsi, comme dans l'exemple ci-dessous, pour tout p premier,

$$Z(V((f_1, \ldots, f_r), p)/\mathbf{F}_q, T) = \exp(-\log(1-T)) = \frac{1}{1-T}$$

Donc

$$\begin{aligned} Z((f_1, \ldots, f_r), x) &= \prod_{p \text{ premier}} \frac{1}{1-p^{-x}} \\ &= \zeta(x) \end{aligned}$$

Cela illustre pourquoi les fonctions zêta sont prises sous cette forme et pourquoi elles portent ce nom.

1.2 Conjectures de WEIL et théorème de DWORK

En 1949, André WEIL énonce quatre conjectures à propos des fonctions zêta. Ces conjectures ont motivé plusieurs années de recherche en géométrie algébrique et en théorie des nombres pour enfin devenir des théorèmes en 1974 lorsque la troisième conjecture, nommée "Hypothèse de RIEMANN", fut démontrée par Pierre DELIGNE. Les trois autres conjectures ont été démontré dès le début des année 1960 grâce aux travaux de Bernard DWORK, puis GROTHENDIECK, ARTIN et VERDIER.

Le conjectures de WEIL concernent des variétés projectives. Cependant le théorème de DWORK, cité ci-dessous, qui fut le premier pas vers la preuve de ces conjectures, s'applique aussi aux variétés affines.

Nous énonçons ci-dessous des version simplifiées des trois premières conjectures.

Conjecture 1 (Conjectures de WEIL)**.** *Soit $f \in \mathbf{F}_q[X_1, \ldots, X_n]$ tel que $\tilde{\mathcal{H}}_{\tilde{f}}$ soit une hypersurface projective lisse, ie. tel que $\tilde{f}$ et ses dérivées partielles selon chaque variable ne s'annulent pas simultanément. Alors,*

1. *(Rationnalité)* $Z(\tilde{\mathcal{H}}_{\tilde{f}}/\mathbf{F}_q, T)$ *est rationnel de la forme*

$$\frac{P(T)^{(-1)^n}}{(1-T)(1-qT)\dots(1-q^{n-1}T)}$$

où $P(T) \in 1 + T\mathbf{Z}[T]$

2. *Si* $\alpha \in \mathbf{C}$ *est une racine réciproque de* P*, ie* $1 - \alpha T | P$*, alors* $\frac{q^{n-1}}{\alpha}$ *aussi.*
3. *(Hypothèse de* Riemann*) Si* $\alpha \in \mathbf{C}$ *est une racine réciproque de* $P(T)$*, alors* α *est de module* $q^{\frac{n-1}{2}}$*.*

Remarque. L'hypothèse de Riemann pour les fonctions zêta est appelée ainsi par analogie avec la conjecture de Riemann classique. En effet, supposons que ces conjectures sont vraies. Soit $\tilde{\mathcal{H}}_{\tilde{f}}$ une hypersurface projective lisse. Prenons n pair afin que la fonction zêta puisse avoir des zéros. Posons

$$F : x \in D \mapsto Z(\tilde{\mathcal{H}}_{\tilde{f}}/\mathbf{F}_q, q^{-x})$$

où $D = \mathbf{C} \setminus [\![0, n-1]\!]$. Les zéros de F sont les zéros de P. Notons $P(T) = (1-\beta_1 T)\dots(1-\beta_k T)$. Soit $x \in \mathbf{C}\setminus[\![0, n-1]\!]$ un zéro de F. Alors $P(q^{-x}) = 0$ Donc il existe $i \in [\![1, k]\!]$ tel que $1 - \beta_i q^{-x} = 0$. Ainsi, par l'hypothèse de Riemann, $\mid q^x \mid = q^{\frac{n-1}{2}} = q^{\mathcal{R}e(x)}$. Donc $\mathcal{R}e(x) = \frac{n-1}{2}$. Donc dans le cas d'une courbe, ie $n = 2$, $\mathcal{R}e(x) = \frac{1}{2}$.

Remarque. Le cas 4 de l'exemple 2 fournit un contre-exemple à la première conjecture. En effet, pour $f = X_1 X_2$,

$$Z(\tilde{\mathcal{H}}_f/\mathbf{F}_q, T) = \frac{1}{(1-T)(1-qT)^2}$$

qui n'est pas sous la forme annoncée. Cela explique l'hypothèse que $\tilde{\mathcal{H}}_{\tilde{f}}$ soit lisse. Ici, $\frac{\partial f}{\partial X_1}$ et $\frac{\partial f}{\partial X_2}$ s'annulent simultanément en $[1, 0, 0]$. Donc la conjecture ne s'applique pas dans ce cas.

Théorème 1 (Théorème de Dwork)**.** *La fonction zêta d'une hypersurface (affine ou projective) est le quotient de deux polynômes à coefficients dans* $\mathbf{Z}$ *et de terme constant 1.*

Ce théorème sera admis. Dans la suite de ce rapport, nous nous intéresserons surtout à un autre théorème de Dwork qui porte sur les fonction zêta, et en particulier, la suite (N_s^*), le théorème de la trace de Dwork.

Exemple 3. Supposons ici que $p > 2$. Soit $f = X_1^2 + X_2^2 - 1$. Alors $\tilde{f} = X_1^2 + X_2^2 - X_0^2$. Alors $\tilde{f}$ et ses dérivées partielles ne s'annulent pas simultanément sur $\mathbf{P}^2(\mathbf{F}_q)$ et donc les conjectures de Weil s'appliquent. Nous allons vérifier la première conjecture explicitement. Calculons la fonction zêta de $V = \tilde{\mathcal{H}}_{\tilde{f}}$. On considère la fonction

$$\varphi : (x_0, x_1, x_2) \mapsto \begin{cases} (x_2 + x_0, 2x_1) \text{ si } (x_2 + x_0, 2x_1) \neq 0 \\ (0, 1) \text{ sinon} \end{cases}$$

φ induit un isomorphisme entre V et la droite projective $\tilde{L}$, de réciproque

$$\psi : (x_1, x_2) \mapsto (4x_1^2 + x_2^2, 4x_1x_2, 4x_1^2 - x_2^2)$$

On peut vérifier que, si $(x'_0, x'_1, x'_2) = \psi(x_1, x_2)$ $x_1'^2 + x_2'^2 - x_0'^2 = 0$.

De plus, si $(8x_1^2, 8x_1x_2) \neq 0$,

$$\varphi \circ \psi(x_1, x_2) = (8x_1^2, 8x_1x_2) = 8x_1(x_1, x_2)$$

et si $(8x_1^2, 8x_1x_2) = 0$,

$$\varphi \circ \psi(x_1, x_2) = (0, 1)$$

Dans mes deux cas $[x_1, x_2] = [\varphi \circ \psi(x_1, x_2)]$

De même, si $(x_2 + x_0, 2x_1) \neq 0$,

$$\begin{aligned}\psi \circ \varphi(x_0, x_1, x_2) &= \psi(x_2 + x_0, 2x_1) \\ &= \left(4(x_2 + x_0)^2 + (2x_1)^2, 4(x_2 + x_0)(2x_1), 4(x_2 + x_0)^2 - (2x_1)^2\right) \\ &= 4(x_0^2 + x_1^2 + x_2^2 + 2x_0x_2, 2x_0x_1 + 2x_1x_2, x_0^2 - x_1^2 + x_2^2 + 2x_0x_2)\end{aligned}$$

Puisque $x_1^2 + x_2^2 - x_0^2 = 0$,

$$\psi \circ \varphi(x_0, x_1, x_2) = 8(x_0 + x_2)(x_0, x_1, x_2)$$

et $(x_0 + x_2) \neq 0$ Si $x_2 + x_0 = 2x_1 = 0$,

$$\psi \circ \varphi(x_0, x_1, x_2) = \psi(0, 1) = (1, 0, -1)$$

Dans les deux cas, $[x_0, x_1, x_2] = [\psi \circ \varphi(x_0, x_1, x_2)]$.

Donc pour tout s, $V(\mathbf{F}_{q^s})$ est isomorphe à la droite projective $\mathbf{P}^1(\mathbf{F}_{q^s})$. Donc $\tilde{N}_s = q^s + 1$. Et ainsi,

$$Z(V/\mathbf{F}_q, T) = \exp\left(\sum_{s \geq 1} \frac{q^s + 1}{s}\right) = \frac{1}{(1 - T)(1 - qT)}$$

Ce qui est bien la forme annoncée par la conjecture.

Le résultat suivant sur les N_s est étroitement lié à la première conjecture de Weil et au théorème de Dwork. En effet, il est même équivalent au théorème de Dwork.

Proposition 1. *Il existe des complexes algébriques $\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_u \in \mathbf{C}$ tels que*

$$\forall s \in \mathbf{N}^*, N_s = \sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s$$

Démonstration. Notons f le polynôme en question. Alors d'après le théorème de Dwork, $Z(\mathcal{H}_f/\mathbf{F}_q, T) = \frac{R(T)}{S(T)}$ avec $S, R \in 1 + T\mathbf{Z}[T]$, de degrés respectifs $t, u \in \mathbf{N}^*$. On peut alors factoriser ces polynômes dans $\mathbf{C}$ ainsi :

$$R(T) = \prod_{i=1}^{u} \beta_i \prod_{i=1}^{u} \left(\frac{1}{\beta_i} - T\right) = \prod_{i=1}^{u} (1 - \beta_i T)$$
$$S(T) = \prod_{i=1}^{t} \alpha_i \prod_{i=1}^{t} \left(\frac{1}{\alpha_i} - T\right) = \prod_{i=1}^{t} (1 - \alpha_i T)$$

Ainsi, les $\frac{1}{\alpha_i}$ et $\frac{1}{\beta_i}$ sont des complexes algébriques, et donc les α_i et les β_i aussi. De plus

$$Z(\mathcal{H}_f/\mathbf{F}_q, T) = \exp\left(\sum_{i=1}^{\infty} \frac{N_i}{i} T^i\right) = \frac{R(T)}{S(T)} = \frac{\prod_{i=1}^{u} (1 - \beta_i T)}{\prod_{i=1}^{t} (1 - \alpha_i T)}$$

Donc

$$\begin{aligned}
\ln(Z(\mathcal{H}_f/\mathbf{F}_q, T)) = \sum_{i=1}^{\infty} \frac{N_i}{i} T^i &= \sum_{i=1}^{u} \ln(1 - \beta_i T) - \sum_{i=1}^{t} \ln(1 - \alpha_i T) \\
&= \sum_{i=1}^{u} -\sum_{s=1}^{\infty} \frac{(\beta_i T)^s}{s} - \sum_{i=1}^{t} -\sum_{s=1}^{\infty} \frac{(\alpha_i T)^s}{s} \\
&= \sum_{s=1}^{\infty} \frac{\sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s}{s} T^s
\end{aligned}$$

Or ces séries ont des rayons strictement positifs, d'où le résultat. □

1.3 Les nombres p-adiques

Dans ce paragraphe, nous allons introduire le corps $\mathbf{Q}_p$ des nombres p-adiques pour un nombre premier p. Les corps des nombres p-adiques sont des complétions de $\mathbf{Q}$, et sont même les seules complétions de $\mathbf{Q}$ autres que $\mathbf{R}$ d'après le théorème d'Ostrowski, énoncé ci-dessous. Ces corps possèdent certaines propriétés contre-intuitives car très différentes des situations analogues dans $\mathbf{R}$. C'est grâce à ces corps que nous allons démontrer la formule de la trace de Dwork.

Fixons p un nombre premier.

1.3.1 Propriétés de la norme p-adique $\|.\|_p$

Nous allons munir $\mathbf{Q}$ d'une norme qui s'avèrera non-archimédienne.

Définition 4. Une *norme* sur un corps F est une application $N : F \to R^+$ telle que

— $\forall x \in F,\ N(x) = 0 \iff x = 0$
— $\forall x, y \in F,\ N(xy) = N(x)N(y)$
— $\forall x, y \in F,\ N(x + y) \leq N(x) + N(y)$

De plus, une norme est *non-archimédienne* si elle vérifie :

$$\forall x, y \in F, N(x + y) \leq \max(N(x), N(y))$$

Définition 5. Pour tout $n \in \mathbf{Z}^*$, posons $\mathrm{ord}_p(n) \stackrel{\text{def}}{=} m$ où $m \in \mathbf{N}$ est le plus grand entier tel que p^m divise n. Pour $n = 0$ on pose $\mathrm{ord}_p(0) = +\infty$.

On étend cette définition à $\mathbf{Q}$. Pour $x = \frac{a}{b} \in \mathbf{Q}$, où $a \in Z$ et $b \in \mathbf{Z}^*$, on pose $\mathrm{ord}_p(x) \stackrel{\text{def}}{=} \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$.

Remarque. ord_p est bien défini sur $\mathbf{Z}$ car $0 \in \{m \mid p^m \text{ divise } n\} \neq \emptyset$. De plus,

$$\forall a, b \in \mathbf{Z}, \mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b) \tag{1}$$

Ce résultat est classique car ord_p correspond à la valuation p-adique sur $\mathbf{Z}$. (Notons $n = \mathrm{ord}_p(a)$ et $m = \mathrm{ord}_p(b)$. Si a ou b est nul, l'égalité est triviale. Supposons a et b non nuls. Alors $p^n \mid a$ et $p^m \mid b$ donc $p^{n+m} \mid ab$ et $n + m \leq \mathrm{ord}_p(ab)$. De plus $p^{\mathrm{ord}_p(ab)-m} \mid a\frac{b}{p^m}$ et p ne divise pas $\frac{b}{p^m}$ donc par le lemme d'Euclide, $p^{\mathrm{ord}_p(ab)-m} \mid a$. Donc $\mathrm{ord}_p(ab) - m \leq n$ et $\mathrm{ord}_p(ab) \leq n + m$. D'où $\mathrm{ord}_p(ab) = n + m$.)

Montrons maintenant que ord_p est bien défini sur $\mathbf{Q}$. Supposons $pgcd(a, b) = 1$ avec les notations de la définition et soit $c \in \mathbf{Z}^*$. Alors $x = \frac{ac}{bc}$ et $\mathrm{ord}_p(x) = \mathrm{ord}_p(ac) - \mathrm{ord}_p(bc)$.

Ainsi, $\mathrm{ord}_p(x) = \mathrm{ord}_p(a) + \mathrm{ord}_p(c) - \mathrm{ord}_p(b) - \mathrm{ord}_p(c) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$. L'application est donc bien définie.

On peut aussi étendre la propriété (1) de ord_p à tout $\mathbf{Q}$.

Lemme 2. *Pour $x, y \in \mathbf{Q}$*

$$ord_p(xy) = ord_p(x) + ord_p(y) \tag{2}$$
$$ord_p(x + y) \geq \min(ord_p(x), ord_p(y)) \tag{3}$$

Démonstration. Démontrons l'égalité (2). Pour $x, y \in \mathbf{Q}$ on note $x = \frac{a}{b}$ et $y = \frac{c}{d}$. Ainsi

$$\begin{aligned}
\mathrm{ord}_p(xy) = \mathrm{ord}_p\left(\frac{ac}{bd}\right) &= \mathrm{ord}_p(ac) - \mathrm{ord}_p(bd) \\
&= \mathrm{ord}_p(a) + \mathrm{ord}_p(c) - \mathrm{ord}_p(b) - \mathrm{ord}_p(d) \\
&= (\mathrm{ord}_p(a) - \mathrm{ord}_p(b)) + (\mathrm{ord}_p(c) - \mathrm{ord}_p(d)) \\
&= \mathrm{ord}_p(x) + \mathrm{ord}_p(y)
\end{aligned}$$

Démontrons maintenant l'inégalité (3). Commençons par le cas où $x, y \in \mathbf{Z}$. Par définition, $p^{\mathrm{ord}_p(x)} \mid x$ et $p^{\mathrm{ord}_p(y)} \mid y$. Ainsi, si $m = min(\mathrm{ord}_p(x), \mathrm{ord}_p(y))$,

alors $p^m \mid x+y$. Donc $\mathrm{ord}_p(x+y) \geq \min(\mathrm{ord}_p(x), \mathrm{ord}_p(y))$. Supposons maintenant $x, y \in \mathbf{Q}$ et notons $x = \frac{a}{b}$ et $y = \frac{c}{d}$. Alors

$$\begin{aligned}
\mathrm{ord}_p(x+y) &= \mathrm{ord}_p\left(\frac{a}{b} + \frac{c}{d}\right) = \mathrm{ord}_p\left(\frac{ad+bc}{bd}\right) \\
&= \mathrm{ord}_p(ad+bc) - \mathrm{ord}_p(bd) \\
&\geq \min(\mathrm{ord}_p(ad) - \mathrm{ord}_p(bd), \mathrm{ord}_p(bc) - \mathrm{ord}_p(bd)) \quad \text{par le cas entier} \\
&\geq \min(\mathrm{ord}_p(a) - \mathrm{ord}_p(b), \mathrm{ord}_p(c) - \mathrm{ord}_p(d)) \\
&\geq \min(\mathrm{ord}_p(x), \mathrm{ord}_p(y))
\end{aligned}$$

□

Soit $x \in \mathbf{Q}^*$. Alors on peut noter $x = \frac{a}{b}p^m$ où p ne divise ni a, ni b et où $m \in \mathbf{Z}$. Ainsi m correspond à $\mathrm{ord}_p(x)$. L'application ord_p a donc une interprétation concrète sur $\mathbf{Q}$, et même nous verrons sur $\mathbf{Q}_p$, analogue à celle sur $\mathbf{Z}$.

Le lemme suivant donne un exemple de calcul d'ordre p-adique qui sera utile dans la suite.

Lemme 3. *Soit $n \in \mathbf{N}$, écrit en base p, $n = a_0 + a_1 p + \cdots + a_s p^s$ où les a_i sont dans $[\![0, p-1]\!]$, et notons $S_n = \sum_{i=0}^{s} a_i$. Alors*

$$ord_p(n!) = \frac{n - S_n}{p-1}$$

Démonstration. $\mathrm{ord}_p(n!) - \mathrm{ord}_p((n-1)!) = \mathrm{ord}_p(n)$ et

$$\frac{n - S_n}{p-1} - \frac{n - 1 - S_{n-1}}{p-1} = \frac{1 - (S_n - S_{n-1})}{p-1}$$

Notons $d = \mathrm{ord}_p(n)$. Alors $n = a_d p^d + \cdots + a_s p^s$. Donc

$$n - 1 = (p-1)1 + (p-1)p + \cdots + (p-1)p^{d-1} + (a_d - 1)p^d + \cdots + a_s p^s$$

car $a_d \neq 0$ par définition. Donc $S_n - S_{n-1} = 1 - (p-1)d$. D'où $d = \frac{1-(S_n - S_{n-1})}{p-1}$. Enfin, $\mathrm{ord}_p(1) = 0$ et $\frac{0 - S_0}{p-1} = 0$ donc

$$\begin{aligned}
\mathrm{ord}_p(n!) &= \mathrm{ord}_p(0!) + \sum_{i=1}^{n} (ord_p(i!) - \mathrm{ord}_p((i-1)!)) \\
&= \frac{0 - S_0}{p-1} + \sum_{i=1}^{n} \left(\frac{n - S_n}{p-1} - \frac{n-1-S_{n-1}}{p-1}\right) \\
&= \frac{n - S_n}{p-1}
\end{aligned}$$

□

Remarque. $\mathrm{ord}_p(n!) =_{n\to\infty} \mathcal{O}(n)$ et même $\mathrm{ord}_p(n!) \sim_{n\to\infty} \frac{n}{p-1}$, car

$$0 \leq S_n \leq (p-1)(\log_p(n)+1)$$

De plus 1 est un valeur d'adhérence de S_n, donc S_n ne tend pas ver l'infini.

Définissons maintenant la norme p-adique $\|.\|_p$.

Définition 6. Pour $x \in \mathbf{Q}$ on pose

$$\|x\|_p \stackrel{\text{def}}{=} p^{-\mathrm{ord}_p(x)}$$

avec la convention $p^{-\infty} = 0$. Ainsi $x = 0$, $\|0\|_p \stackrel{\text{def}}{=} 0$.

Remarque. Cela définit bien une norme sur $\mathbf{Q}$. En effet,

— $\|x\|_p = 0 \iff \mathrm{ord}_p(x) = +\infty \iff x = 0$.

— $\forall x, y \in \mathbf{Q}$, grâce au (2) du lemme précédent,

$$\begin{aligned}\|xy\|_p &= p^{-\mathrm{ord}_p(xy)} = p^{-\mathrm{ord}_p(x)-\mathrm{ord}_p(y)} = p^{-\mathrm{ord}_p(x)}p^{-\mathrm{ord}_p(y)} \\ &= \|x\|_p\|y\|_p\end{aligned}$$

— De même, grâce au (3) du lemme précédent, $\forall x, y \in Q$,

$$\|x+y\|_p \leq \max(\|x\|_p, \|y\|_p) \ (\leq \|x\|_p + \|y\|_p)$$

Cette norme est donc non-archimédienne.

On munit $\mathbf{Q}$ de cette norme p-adique.

Le résultat suivant précise le cas d'égalité dans l'inégalité triangulaire dans tout corps muni d'une norme non-archimédienne.

Proposition 2. *Soit F un corps muni d'une norme non-archimédienne N. Pour $x, y \in F$,*

$$N(x \pm y) \leq \max(N(x), N(y))$$

avec égalité si $N(x) \neq N(y)$.

Démonstration. L'inégalité découle de la définition. Supposons $N(x) < N(y)$. Alors $N(y) = N((y-x)+x) \leq \max(N(y-x), N(x))$. Or $N(y) > N(x)$, donc $N(y) \leq N(x-y) \leq N(y)$. Donc $N(x-y) = N(y)$. De même pour $N(x+y)$. □

Remarque. Le fait que la norme soit non-archimédienne a plusieurs conséquences intéressantes.

— Tout triangle est isocèle ! En effet, soient $x, y, z \in F$. Si $N(x-z) \neq N(y-z)$ alors $N(x-y) = \max(N(y-z), N(x-z))$. Donc le triangle (x, y, z) est toujours isocèle.

— Notons $B(x, r) = \{y \in F \mid N(y-x) < r\}$ la boule ouverte de centre x et de rayon r dans F. Soit $y \in B(x, r)$. Soit $z \in B(x, r)$.

$$N(z-y) \leq \max(N(z-x), N(y-x)) < r$$

Donc $z \in B(y, r)$. Ainsi $B(x, r) \subset B(y, r)$ et par symétrie $B(y, r) \subset B(x, r)$. Donc

$$\forall y \in B(x, r), B(y, r) = B(x, r)$$

Un autre résultat qui découle du cas d'égalité est le lemme suivant.

Lemme 4. *Pour toute suite de* CAUCHY (a_n) *dans* $(\mathbf{Q}, \|.\|_p)$*, la suite* $(\|a_n\|_p)$ *converge.*

Démonstration. Soit (a_n) une suite de CAUCHY dans $\mathbf{Q}$ pour la norme $\|.\|_p$. Si (a_n) tend vers 0, le résultat est trivial. Supposons alors que (a_n) ne tende pas vers 0. Alors il existe $\epsilon > 0$ tel que pour tout $N \in \mathbf{N}$, il existe $n \geq N$ tel que $\|a_n\|_p > \epsilon$. Or (a_n) est une suite de CAUCHY, donc il existe $N \in \mathbf{N}$ tel que pour tous $n, m \geq N$, $\|a_n - a_m\|_p < \epsilon$. En particulier, pour tout $n \geq N$, $\|a_n - a_N\|_p < \epsilon$. Prenons alors un N tel que $\|a_N\|_p > \epsilon$. Alors pour tout $n \geq N$, $\|a_n\|_p \leq \max(\|a_n - a_N\|_p, \|a_N\|_p)$. Et puisque $\|a_n - a_N\|_p < \epsilon < \|a_N\|_p$, $\|a_n\|_p = \|a_N\|_p$. Donc la suite $(\|a_n\|_p)$ est stationnaire et donc convergeante. □

1.3.2 Construction de $\mathbf{Q}_p$

Dans ce paragraphe nous allons énoncer une construction du corps Ω donnée notamment dans le livre de KOBLITZ [3]. Cette construction consiste d'abord à compléter le corps $\mathbf{Q}$ en un corps $\mathbf{Q}_p$, complet pour la norme $\|.\|_p$. Ce corps n'étant pas algébriquement clos, on considère sa clôture algébrique $\bar{\mathbf{Q}}_p$. Malheureusement, ce nouveau corps n'est pas complet. On le complète donc en un nouveau corps Ω, qui est un corps complet et algébriquement clos.

La complétion de $\mathbf{Q}$ vers $\mathbf{Q}_p$ est analogue à sa complétion, pour la norme associé à la valeur absolue, vers $\mathbf{R}$. En effet on désigne par $\mathbf{Q}_p$ l'anneau des suites de CAUCHY de $(\mathbf{Q}, \|.\|_p)$, quotienté par l'idéal maximal des suites de $(\mathbf{Q}, \|.\|_p)$ tendant vers 0. En particulier, $\mathbf{Q}_p$ est bien un corps.

Ainsi, on peut étendre $\|.\|_p$ à $\mathbf{Q}_p$.

Définition 7. Pour tout $\alpha \in \mathbf{Q}_p$, on prend (a_n) un représentant de α dans l'ensemble des suites de CAUCHY de $(\mathbf{Q}_p, \|.\|_p)$. On pose $\|\alpha\|_p \overset{\text{def}}{=} \lim_{n\to\infty} \|a_n\|_p$.

Remarque. $\|\alpha\|_p$ est bien défini grâce au lemme 4 et au fait que si deux suites de CAUCHY, (a_n) et (b_n), sont des représentants de α, alors $\lim_{n\to\infty} \|a_n - b_n\|_p = 0$, et donc $\lim_{n\to\infty} \|a_n\|_p = \lim_{n\to\infty} \|b_n\|_p$.

Remarque. Que ce soit dans $\mathbf{Q}_p$ ou dans $\mathbf{Q}$, $\|.\|_p$ est à valeurs dans $\{p^n\}_{n\in\mathbf{Z}} \cup \{0\}$. On peut ainsi étendre ord_p à $\mathbf{Q}_p$ en posant $\text{ord}_p(\alpha) = -\log_p(\|\alpha\|_p)$ pour $\alpha \neq 0$.

Représenter les éléments de $\mathbf{Q}_p$ comme des classes d'équivalence de suites de Cauchy dans $(\mathbf{Q}, \|.\|_p)$ n'est pas la façon la plus simple de les manipuler. Ainsi, dans la suite nous allons les représenter comme dans le théorème suivant qui sera admis.

Théorème 2. *Pour tout* $\alpha \in \mathbf{Q}_p$*, il existe une unique suite d'entier* $(b_n)_{n\geq m}$ *où* $m = ord_p(\alpha) \in \mathbf{Z}$*, tels que pour* $n \geq m$*,* $b_n \in [\![0, p-1]\!]$*,* $b_m > 0$ *et*

$$\alpha = \sum_{n\geq m} b_n p^n$$

Remarque. Ce théorème a notamment pour conséquence le fait que $\mathbf{Q}_p$ soit équipotent à $\mathbf{R}$. En effet, $\mathbf{Q}_p$ est en bijection avec $\mathbf{Z} \times [\![1, p-1]\!] \times [\![0, p-1]\!]^{\mathbf{N}}$, qui est équipotent à $\mathbf{R}$. Ainsi $\mathbf{Q}_p$ est aussi un analogue de $\mathbf{R}$ en terme de cardinalité.

De plus, nous n'allons pas préciser la construction explicite de Ω car elle ne sera pas utile dans la suite. Nous allons donc désigner par Ω une extension de corps de $\mathbf{Q}_p$ qui est complète et algébriquement close. Il peut être utile de savoir par ailleurs que Ω n'est pas une extension finie et que l'on étend la norme $\|.\|_p$ et la valuation ord_p à Ω.

Nous avons évoqué en introduction de cette partie que les corps $\mathbf{Q}_p$ sont, avec $\mathbf{R}$, les seules complétions du corps $\mathbf{Q}$. Cela est dû au théorème suivant qui sera admis. Ce théorème illustre notamment l'importance des corps $\mathbf{Q}_p$.

Théorème 3 (Théorème d'Ostrowski)**.** *Toute norme non triviale sur* $\mathbf{Q}$ *est équivalente à* $\|.\|_p$ *pour un* p *ou à la norme de la valeur absolue.*

1.3.3 L'anneau $\mathbf{Z}_p$

Nous allons maintenant considérer l'anneau des entiers p-adiques.

Définition 8. L'anneau des entiers p-adiques $\mathbf{Z}_p$ est défini ainsi.

$$\mathbf{Z}_p \overset{\text{def}}{=} \{\alpha \in \mathbf{Q}_p \mid \mathrm{ord}_p(\alpha) \geq 0\} = \{\alpha \in \mathbf{Q}_p \mid \|\alpha\|_p \leq 1\}$$

Autrement dit, les éléments de $\mathbf{Z}_p$ sont les nombres p-adiques qui peuvent s'écrire $\alpha = \sum_{n \geq 0} b_n p^n$ avec $\forall n, b_n \in [\![0, p-1]\!]$.

Remarque. $\mathbf{Z} \subsetneq \mathbf{Z}_p$ car, par exemple, $\sum_{n \geq 0} 1p^n \in \mathbf{Z}_p \setminus \mathbf{Z}$. De plus, $\mathbf{Z}$ et $\mathbf{Z}_p$ n'ont pas la même cardinalité. En effet, $\mathbf{Z}_p$ est en bijection avec $[\![0, p-1]\!]^{\mathbf{N}}$ et donc avec $\mathbf{R}$. Ainsi $\mathbf{Z}_p$ et $\mathbf{Q}_p$ ont la même cardinalité.

Remarque. On peut étendre la notion de congruence modulo p^s à $\mathbf{Z}_p$:

$$\sum_{n \geq 0} b_n p^n \equiv \sum_{n \geq 0} b'_n p^n \mod p^s \iff \forall n \in [\![0, s-1]\!], b_n = b'_n$$

Remarque. $\mathbf{Z}_p$ est l'anneau des entiers de $\mathbf{Q}_p$.

Proposition 3. $(\mathbf{Z}_p, \|.\|_p)$ *est un compact, et est donc complet.*

Démonstration. Nous déduisons de la définition que $\mathbf{Z}_p$ est en bijection naturelle avec $[\![0, p-1]\!]^{\mathbf{N}}$. La distance d induite sur $[\![0, p-1]\!]^{\mathbf{N}}$ par $\|.\|_p$ est $d((x_n), (y_n)) = p^{-\min\{n \in \mathbf{N} | x_n \neq y_n\}}$. Montrons que cette distance engendre la topologie produit. Pour cela il suffit de montrer qu'une suite (α_n) de $[\![0, p-1]\!]^{\mathbf{N}}$ converge dans $([\![0, p-1]\!]^{\mathbf{N}}, d)$ si et seulement si elle converge simplement.

Soit une suite (α_n) de $[\![0, p-1]\!]^{\mathbf{N}}$ qui converge pour la distance d vers $\alpha^* \in [\![0, p-1]\!]^{\mathbf{N}}$. Alors soient $i \in \mathbf{N}$ et $\epsilon = p^{-i}$. À partir d'un certain rang $N \geq 0$, $d(\alpha_n, \alpha^*) < \epsilon$, donc pour $n \geq N$, $\alpha_{n,i} = \alpha^*_i$. Donc (α_n) converge simplement.

Supposons réciproquement que (α_n) converge simplement vers une suite α^* de $[\![0, p-1]\!]^{\mathbf{N}}$. Soient $\epsilon > 0$ et $i_\epsilon = -\log_p(\epsilon)$. Il existe $N \in \mathbf{N}$ tel que pour $n \geq N$, pour $i \in [\![0, i_\epsilon]\!]$, $|\alpha_{n,i} - \alpha_i^*| = 0$ et donc $d(\alpha_n, \alpha^*) < \epsilon$. Donc la suite converge pour d. La topologie est donc bien celle de la convergence simple, qui est la topologie produit.

On peut donc conclure avec le théorème de Tykhonov. □

Proposition 4. $\mathbf{Z}$ *est dense dans* $\mathbf{Z}_p$.

Démonstration. Il suffit de considérer $\alpha_n = \sum_{i=0}^{n} b_i p^i \in \mathbf{Z}$, et ainsi

$$\alpha_n \xrightarrow[n\to\infty]{\|.\|_p} \alpha$$

□

Avec les deux propositions précédentes, nous pouvons démontrer le prochain lemme qui sera utile dans la définition de la fonction θ.

Lemme 5. *Pour tous* $x = \frac{a}{b} \in Q_p$ *tel que* $b \wedge p = 1$, *et* $k \in \mathbf{N}$, $\binom{x}{k} \in \mathbf{Z}_p$.

Démonstration. Nous pouvons déjà remarquer qu'un tel x est un entier p-adique. En effet, $\mathrm{ord}_p(b) = 0$ donc $\mathrm{ord}_p(x) \geq 0$. Ainsi, puisque $\mathbf{Z}$ est dense dans $\mathbf{Z}_p$, il existe une suite (x_n) dans $\mathbf{Z}$ tel que $x_n \to x$. Or, pour tout $n \in \mathbf{N}$, $\binom{x_n}{k} \in \mathbf{Z}$. Par continuité de la multiplication et de l'inversion dans $\mathbf{Q}_p$, $\binom{x_n}{k} \to \binom{x}{k}$. Ainsi, par compacité de $\mathbf{Z}_p$, $\binom{x}{k} \in \mathbf{Z}_p$. □

Nous allons maintenant énoncer un lemme important pour la suite qui permet de relever une racine d'un polynôme dans $\mathbf{F}_p$ en une racine dans $\mathbf{Z}_p$.

Lemme 6 (Lemme de Hensel)**.** *Soit un polynôme* $f \in \mathbf{Z}_p[X]$. *Supposons qu'il existe un entier p-adique* $a \in \mathbf{Z}_p$ *tel que* $f(a) \equiv 0 \mod p$ *et* $f'(a) \not\equiv 0 \mod p$.

Alors il existe un unique entier p-adique $a' \in \mathbf{Z}_p$ *tel que* $f(a') = 0$ *et* $a' \equiv a \mod p$.

Démonstration. Nous allons construire une suite (a_n) d'entier dans $\mathbf{Z}$ tels que pour tout $n \in \mathbf{N}$

$$f(a_n) \equiv 0 \mod p^{n+1} \tag{4}$$
$$a_n \equiv a_{n-1} \mod p^n \tag{5}$$
$$0 \leq a_n < p^{n+1} \tag{6}$$

Posons a_0 l'unique entier tel que $a_0 \in [\![0, p-1]\!]$ et $a_0 \equiv a \mod p$. Alors $f(a_0) \equiv 0 \mod p$. Si a_1 est un entier vérifiant les conditions voulues, alors $a_1 \equiv a_0 \mod p$ donc il existe $b_1 \in \mathbf{Z}$ tel que $a_1 = a_0 + b_1 p$. Donc

$$f(a_1) = f(a_0 + b_1 p) \equiv f(a_0) + b_1 p f'(a_0) \mod p^2$$

Or $f(a_0) \equiv 0 \mod p$ donc il existe $\alpha \in [\![0, p-1]\!]$ tel que $f(a_0) \equiv \alpha p \mod p^2$. Ainsi, la condition (4) devient $\alpha p + b_1 p f'(a_0) \equiv 0 \mod p^2$ et donc $\alpha \equiv -b_1 f'(a_0) \mod p$. Or $f'(a_0) \equiv f'(a) \mod p$ donc $f'(a_0) \not\equiv 0 \mod p$ et est donc inversible dans $\mathbf{F}_p$. Ainsi, il existe un unique $b_1 \in [\![0, p-1]\!]$ tel que $b_1 \equiv -\alpha f'(a_0)^{-1} \mod p$. On pose alors $a_1 = a_0 + b_1 p$. Ce choix est unique à cause de la condition (6).

Supposons $a_0, \ldots, a_{n-1}$ définis de façon unique. Alors de même, $a_n = a_{n-1} + b_n p^n$. De plus a_n doit vérifier $f(a_n) \equiv 0 \mod p^{n+1}$. Or

$$\begin{aligned} f(a_{n-1} + b_n p^n) &\equiv f(a_{n-1}) + b p^n f'(a_{n-1}) \mod p^{n+1} \\ &\equiv \alpha' p^n + b_n p^n f'(a_{n-1}) \mod p^{n+1} \end{aligned}$$

où α' est un entier tel que $f(a_{n-1}) \equiv \alpha' p^n \mod p^{n+1}$, car $f(a_{n-1}) \equiv 0 \mod p^n$ par hypothèse. Ainsi, la condition devient $\alpha' + b_n f'(a_{n-1}) \equiv 0 \mod p$. Or $a_{n-1} \equiv \alpha_0 \mod p$ donc $f'(a_{n-1}) \equiv f'(a_0) \not\equiv 0 \mod p$. Donc de même que dans le premier cas, on définit b_n l'unique entier dans $[\![0, p-1]\!]$ tel que $b_n = \alpha' f'(a_{n-1})^{-1}$. Ainsi, on pose $a_n = a_{n-1} + b_n p^n$ et a_n est définit de façon unique à cause de la condition (6).

Ainsi, la suite (a_n) est définie de façon unique et vérifie les conditions voulues par construction.

On pose alors $a' = a_0 + \sum_{i=1}^{\infty} b_i p^i \in \mathbf{Z}_p$. Ainsi, $a' \equiv a \mod p$. Il reste donc à montrer que $f(a') = 0$ et que a' est unique. Que $f(a')$ soit nul découle du fait que pour $n \in \mathbf{N}$, $f(a') \equiv f(a_n) \equiv 0 \mod p^{n+1}$. Maintenant si $a'' \in \mathbf{Z}_p$ convient, alors $a'' = \sum_{i=0}^{\infty} b'_i p^i$ où les b'_i vérifient les conditions ci-dessus. Ainsi $a'' = a'$, d'où l'unicité. □

Exemple 4. Considérons $f = X^2 + 1 \in \mathbf{Z}_{13}[X]$. alors $f(5) \equiv 0 \mod 13$ et $f'(5) = 11 \not\equiv 0 \mod 13$. Donc il existe $\alpha \in \mathbf{Z}_{13}$ tel que $\alpha \equiv 5 \mod 13$ et tel que $f(\alpha) = 0$. Autrement dit, -1 est un carré dans $\mathbf{Z}_{13}$.

1.3.4 Convergence des suites et séries dans Ω

Nous allons terminer ce paragraphe sur des propriétés intéressantes de convergence dans le corps $(\Omega, \|.\|_p)$.

Proposition 5. *Soit $\sum a_n$ un série à coefficients dans Ω. Alors $\sum a_n$ converge dans $(\Omega, \|.\|_p)$ si et seulement si $\|a_n\|_p \xrightarrow[n\to\infty]{} 0$.*

Démonstration. Le sens direct est immédiat. Supposons que $\|a_n\|_p \xrightarrow[n\to\infty]{} 0$. Puisque Ω est complet, il suffit de montrer que la suite $(S_n) = (\sum_{i=0}^{n} a_i)_n$ est de Cauchy. Soit $\epsilon > 0$ et soient $n \geq m \geq 0$.

$$\|S_n - S_m\|_p = \| \sum_{i=m+1}^{n} a_i \|_p \leq \max_{m+1 \leq i \leq n} \|a_i\|_p$$

Or il existe $N \geq 0$ tel que pour $n \geq N$, $\|a_n\|_p \leq \epsilon$. Donc en prenant $n, m \geq N$, on trouve $\|S_n - S_m\|_p \leq \epsilon$. Donc $\sum a_n$ converge. □

Exemple 5 (La fonction exponentielle)**.** Considérons la fonction exponentielle classique $\exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}$. Alors $\exp(x)$ converge si et seulement si $\frac{x^k}{k!} \xrightarrow[k\to\infty]{} 0$, ie. $k\mathrm{ord}_p(x) - \mathrm{ord}_p(k!) \xrightarrow[k\to\infty]{} \infty$. Or, nous avons vu que $\mathrm{ord}_p(k!) = \frac{k-S_k}{p-1}$. Donc $\exp(x)$ converge si et seulement si $k(\mathrm{ord}_p(x) + \frac{1}{p-1}) + \frac{S_k}{p-1} \xrightarrow[k\to\infty]{} \infty$. Cela équivaut à $\mathrm{ord}_p(x) > -\frac{1}{p-1}$. Donc le rayon de convergence de exp dans $\mathbf{Q}_p$, et plus généralement dans le corps Ω, est $p^{\frac{1}{p-1}}$.

Proposition 6. *Soit (a_n) une suite de* Cauchy *de Ω. Alors (a_n) converge si et seulement si $a_{n+1} - a_n \xrightarrow[n\to\infty]{} 0$.*

Démonstration. Cela découle de l'inégalité ultramétrique

$$\forall m \geq n \geq 0, \|a_m - a_n\|_p \leq \max_{n \leq i \leq m-1} \|a_{i+1} - a_i\|_p$$

□

2 Expression et calcul des N_i

Pour toute la suite nous considérons une puissance q de p, $q = p^a$.

2.1 R_0, R_1, et R

Nous avons pour l'instant défini les anneaux $\mathbf{Z}_p \subset \mathbf{Q}_p \subset \Omega$. Nous allons maintenant définir trois nouveaux anneaux qui seront des anneaux intermédiaires entre $\mathbf{Z}_p$ et Ω. Pour cela, nous considérons la suite $(\gamma_n)_{n\in\mathbf{N}\cup\{\infty\}}$ de Ω telle que,

$$\forall n \in \mathbf{N} \cup \{\infty\}, \begin{cases} \sum_{i=0}^{n} \frac{\gamma_n^{p^i}}{p^i} = 0 \\ \mathrm{ord}_p \gamma_n = \frac{1}{p-1} \end{cases}$$

Dans le cas $n = 1$, γ_1 est une racine dans Ω du polynôme $pX + X^p$. Puisque Ω est algébriquement clos, le polynôme admet p racines. Soit α une de ses $p-1$ racines non nulles. Alors $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\frac{\alpha^p}{p}) = p\mathrm{ord}_p(\alpha) - 1$. Donc $\mathrm{ord}_p(\alpha) = \frac{1}{p-1}$. On choisit alors une de ces $p-1$ racines non nulles.

Nous allons admettre l'existence de γ_n dans les autres cas car nous utiliserons dans la suite principalement γ_1 et brièvement γ_∞.

Posons pour alléger les notations $\pi \overset{\mathrm{def}}{=} \gamma_1$. On définit alors l'anneau

$$R_1 \overset{\mathrm{def}}{=} \mathbf{Z}_p[\pi] = \mathbf{Z}_p[X] \,/ X^{p-1} + p$$

Remarque. $\pi^p = -p\pi$

La propriété qui suit est une conséquence d'une version du lemme de HENSEL.

Proposition 7. *Il existe p racines p-èmes de l'unité distinctes dans R_1, de la forme $1 + \pi t_k$, où $t_1, \ldots, t_p \in R_1$.*

Démonstration. Il s'agit de trouver p racines distinctes de $(1 + \pi X)^p - 1$ dans R_1. Nous allons appliquer une version du lemme de HENSEL analogue à celle énoncée ci-dessus.

Lemme 7. *Soit $f \in \mathbf{Z}[\pi][X]$. Si x est une racine simple de f dans $\mathbf{Z}[\pi] \Big/ (\pi)$, alors il existe un unique $\tilde{x} \in R_1 = \mathbf{Z}_p[\pi]$ tel que $\tilde{x} = x \mod \pi$.*

$0, \ldots, p-1$ sont p racines distinctes de $(1 + \pi X)^p - 1$ dans $\mathbf{Z}[\pi] \Big/ (\pi)$ et donc des racines simples. On peut alors appliquer le lemme à chacune, ce qui démontre le résultat. □

Remarque. Cela montre que non seulement toutes les p racines p-èmes de l'unité dans Ω sont dans R_1, mais aussi que ces racines sont distinctes modulo π^2.

Pour la suite, nous devons définir l'indice de ramification d'une extension de $\mathbf{Q}_p$, qui nécessitera un lemme préliminaire.

Lemme 8. *Soit K une extension finie de $\mathbf{Q}_p$, de degré f. Alors $ord_p(K) \subset \frac{1}{f}\mathbf{Z}$.*

Définition 9. Soit K une extension de $\mathbf{Q}_p$ de degré fini f. Alors $\mathrm{ord}_p(K)$ est de la forme $\frac{1}{e}\mathbf{Z}$, où $e|f$. Alors *l'indice de ramification* de K est l'entier e.
L'extension est *totalement ramifiée* si $e = f$, et elle est *non-ramifiée* si $e = 1$.

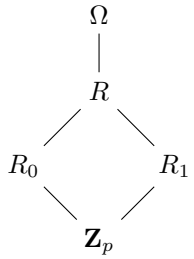
Nous définissons maintenant l'anneau R_0. Pour cela, nous avons besoin de la prochaine proposition, que nous allons admettre.

Proposition 8. *Pour tout $f \in \mathbf{N}^*$, il existe une unique extension de corps non-ramifiée de $\mathbf{Q}_p$ de degré f.*

On prend donc K l'unique extension non-ramifiée de $\mathbf{Q}_p$ de degré a (où $q = p^a$). Puis on pose R_0 son anneau des entiers, ie

$$R_0 = \{x \in K \mid \|x\|_p \leq 1\}$$

Enfin, on pose R le sous-anneau de Ω engendré par R_0 et R_1. On obtient ainsi le schéma ci-dessous.



Explicitons R_0. $\mathbf{F}_q$ est une extension de $\mathbf{F}_p$ de degré a. Ainsi il s'écrit $F_q = F_p[X] \Big/ h(X)$, avec $h \in \mathbf{F}_p[X]$ irréductible de degré a. On relève donc les coefficients de h vers $\mathbf{Z}_p$ en prenant pour tout coefficient $\bar{a} \in \mathbf{F}_p$, $a \in [\![-\frac{p}{2}+1, \frac{p}{2}]\!]$. Notons $\hat{h} \in \mathbf{Z}_p[X]$ ce nouveau polynôme. Considérons alors $\mathbf{Z}_p[\mu] = \mathbf{Z}_p[X] \Big/ \hat{h}(X)$, où $\mu \in \Omega$ est une racine de $\hat{h}$. On admet que $R_0 = \mathbf{Z}_p[\mu]$.

Les morphismes ω et τ Maintenant que nous avons défini ces trois anneaux, nous allons définir un relèvement ω depuis $\bar{\mathbf{F}}_q$ vers Ω, un corps de caractéristique nulle. Cela nous servira notamment à relever un polynôme de $\mathbf{F}_q$ en un polynôme de R. On pose donc $\omega(0) = 0$, et pour $x \in \bar{\mathbf{F}}_q$, $\omega(x)$ est l'unique racine de l'unité dans Ω, dont l'ordre divise l'ordre de x, et tel que $\omega(x) \equiv x \mod p$. Un tel relèvement s'appelle un *relèvement de Teichmüller*. Par unicité de l'extension non-ramifiée de $\mathbf{Q}_p$ d'ordre a, pour $x \in F_q$, $\omega(x) \in R_0$.

Enfin, nous allons introduire un relèvement du morphisme de Frobenius en un automorphisme τ de R. Pour cela on pose $\tau : R \to R$ un morphisme $\mathbf{Z}_p$-linéaire tel que $\tau(\pi) = \pi$ et tel que $\tau(\mu)$ est l'unique racine de $\hat{h}$ congru à μ^p modulo p. Ainsi $\tau_{|R_1} = id_{R_1}$ et τ permute les racines de $\hat{h}$. τ est bien défini car, d'après ce qui précède, on peut écrire $R = \mathbf{Z}_p[\mu, \pi]$, et puisque τ est $\mathbf{Z}_p$-linéaire, il suffit de fixer $\tau(\pi)$ et $\tau(\mu)$. La bonne définitions de $\tau(\mu)$ repose sur le lemme de Hensel. Enfin, on étend τ à $R[[X]]$ en posant $\tau(X) = X$.

Lemme 9. *Pour $x \in \mathbf{F}_q$, $\tau(\omega(x)) = \omega(x)^p$.*

Démonstration. Soit $x \in \mathbf{F}_q \backslash \{0\}$. Alors $x^{q-1} = 1$. Alors par définition, $\omega(x)^{q-1} = 1$. Et puisque τ est un automorphisme, $\tau(\omega(x))^{q-1} = 1$. Donc $\tau(\omega(x))$ est une racine $q-1$-ème de l'unité. Or $\omega(x)^p$ est aussi une racine $q-1$-ème de l'unité, et $\tau(\omega(x)) \equiv \omega(x)^p \mod p$. D'où le résultat. □

Cela justifie le fait qu'on appelle τ un relèvement du morphisme de Frobenius.

2.2 Formule de la trace de Dwork

L'objectif de ce paragraphe est de prouver l'expression suivante des N_s^*. On rappelle que $q = p^a$ et $n \in \mathbf{N}^*$ sont fixés et que pour tout $s \in \mathbf{N}^*$,

$$N_s^* = |\{x \in (\mathbf{F}_{q^s}^*)^n \mid f(x) = 0\}|$$

Fixons aussi $f \in \mathbf{F}_q[X_1, \ldots, X_n]$.

Théorème 4 (Formule de la trace de Dwork)**.** *Pour $s \in \mathbf{N}^*$,*

$$(q^s - 1)^{n+1} Tr(M_a^s) = q^s N_s^* - (q^s - 1)^n$$

où M_a^s est une matrice infinie qui sera définie dans ce paragraphe.

Cette formule repose sur un lemme essentiel, mais simple, sur les caractères de $\mathbf{F}_{q^s}$, à valeurs dans le groupe des unité d'un anneau commutatif.

Définition 10 (Caractère)**.** Un *caractère* de $\mathbf{F}_{q^s}$ à valeurs dans un anneau A est un morphisme de groupe $\varphi : (\mathbf{F}_{q^s}, +) \to (A^\times, \times)$.

Lemme 10. *Soit un caractère non trivial $\varphi : \mathbf{F}_{q^s} \to A$, où A est un anneau contenant $\mathbf{Z}$, tel que $\sum_{x \in \mathbf{F}_{q^s}} \varphi(x) = 0$. Alors*

$$\sum_{x \in (\mathbf{F}_{q^s}^*)^{n+1}} \varphi(x_0 f(x_1, \ldots, x_n)) = q^s N_s^* - (q^s - 1)^n$$

Démonstration. Soit $u \in \mathbf{F}_{q^s}$. Alors $\sum_{x_0 \in \mathbf{F}_{q^s}} \varphi(x_0 u) = \begin{cases} 0 \text{ si } u \neq 0 \\ q^s \text{ si } u = 0 \end{cases}$ Ce résultat classique découle du fait que, si $u \neq 0$, puisque φ est non trivial, il existe $x \in \mathbf{F}_{q^s}$ tel que $\varphi(x) \neq 0$. Or

$$\begin{aligned} \sum_{x_0 \in \mathbf{F}_{q^s}} \varphi(x_0 u) &= \sum_{x_0 \in \mathbf{F}_{q^s}} \varphi(x)\varphi(x^{-1} x_0 u) \\ &= \varphi(x) \sum_{x^{-1} x_0 \in \mathbf{F}_{q^s}} \varphi(x^{-1} x_0 u) \\ &= \varphi(x) \sum_{x_0 \in \mathbf{F}_{q^s}} \varphi(x_0 u) \end{aligned}$$

Ainsi, puisque $\varphi(x) \neq 1$, $\sum_{x_0 \in \mathbf{F}_{q^s}} \varphi(x_0 u) = 0$.

Donc $\sum_{x \in \mathbf{F}_{q^s} \times (\mathbf{F}_{q^s}^*)^n} \varphi(x_0 f(x_1, \ldots, x_n)) = q^s N_s^*$. Et en retirant le cas $x_0 = 0$, on trouve le résultat voulu. □

Il s'agira donc dans la suite de trouver une suite de caractères convenables pour démontrer le théorème 4. La suite en question fera apparaître la fonction *trace* de $\mathbf{F}_{q^s}$ vers $\mathbf{F}_q$.

Définition 11 (Trace)**.** On définit la *trace* d'une élément $x \in \mathbf{F}_{q^s}$ ainsi

$$Tr_{\mathbf{F}_{q^s}/\mathbf{F}_q}(x) = x + x^q + \cdots + x^{q^{s-1}} \in \mathbf{F}_q$$

Remarque. Cette application est bien définie. En effet, si $x \in F_{q^s}$,

$$\begin{aligned} \left(Tr_{\mathbf{F}_{q^s}/\mathbf{F}_q}(x)\right)^q &= (x + x^q + \cdots + x^{q^{s-1}})^q \\ &= x^q + x^{q^2} + \cdots + x^{q^s} \\ &= Tr_{\mathbf{F}_{q^s}/\mathbf{F}_q}(x) \end{aligned}$$

Donc $Tr_{\mathbf{F}_{q^s}/\mathbf{F}_q}(x)$ est racine de $X^q - X$ dans $\mathbf{F}_{q^s}$. Donc $Tr_{\mathbf{F}_{q^s}/\mathbf{F}_q}(x) \in \mathbf{F}_q$.

2.2.1 La fonction θ

Le suite de caractères qui va nous intéresser est une suite de la forme $\varphi_s = \varphi_1 \circ Tr_{\mathbf{F}_{q^s}/\mathbf{F}_q} : \mathbf{F}_{q^s} \to R_1$ pour tout $s \geq 1$, où $\varphi_1 : \mathbf{F}_q \to R_1$ devra être un caractère non trivial. Pour cela, nous allons introduire des fonction exponentielles. En particulier, nous allons poser

$$\theta(z) = \exp\left(\pi z + \frac{(\pi z)^p}{p}\right) = \exp(\pi z - \pi z^p)$$

Puis nous considérerons les caractères $\Psi_s = \theta(1)^{Tr_{\mathbf{F}_{q^s}/\mathbf{F}_q}}$.

Remarque. À première vue, ce caractère serait trivial. Or la convergence de θ sur le disque unité fermé est plus compliquée que cela. Nous ne pouvons donc pas directement substituer 1 à z dans l'expression $\exp(\pi z - \pi z^p)$, en particulier parce que cette série ne converge pas sur tout le cercle unité dans $(\Omega, \|.\|_p)$. La série $\exp(\pi z - \pi z^p) = \sum_{i=0}^{\infty} \frac{(\pi z - \pi z^p)^i}{i!}$ converge si et seulement si $\frac{(\pi z - \pi z^p)^i}{i!} \xrightarrow[i\to\infty]{} 0$, ie. $\mathrm{ord}_p(\frac{(\pi z - \pi z^p)^i}{i!}) \xrightarrow[i\to\infty]{} \infty$. Or

$$\mathrm{ord}_p(\frac{(\pi z - \pi z^p)^i}{i!}) = i\mathrm{ord}_p(\pi) + i\mathrm{ord}_p(z - z^p) - \mathrm{ord}_p(i!) = \frac{S_i}{p-1} + i\mathrm{ord}_p(z - z^p)$$

d'après le lemme 3. Donc il faut et il suffit que $\mathrm{ord}_p(z - z^p) > 0$. Ainsi, si on prend z de norme 1 tel que $\|z - z^p\|_p = 1$, alors $\mathrm{ord}_p(z - z^p) = 0$ et le terme général ne tend pas vers 0. Donc la série ne converge pas en z. On pourrait, par exemple, prendre $z = -1$ si $p \neq 2$. On verra en effet que $\theta(1) \neq 1$.

Notons $\theta(z) = \sum_{r=0}^{\infty} \lambda_r z^r$.

Proposition 9. *Il existe $\epsilon > 0$ tel que θ converge sur le disque $\{x \in \Omega \mid \|x\|_p < 1 + \epsilon\}$. En particulier, θ converge sur le disque unité fermé.*

Lemme 11. *Pour $r \in \mathbf{N}$, $\lambda_r \in R_1$ et $ord_p(\lambda_r) > \frac{(p-1)r}{p^2}$.*

Pour montrer ce lemme, on écrit la série θ sous forme de produit.

Lemme 12.

$$\exp(z) = \prod_{k=1}^{\infty} (1 - z^k)^{-\frac{\mu(k)}{k}} \tag{7}$$

$$= \prod_{\substack{k=1 \\ k \wedge p = 1}}^{\infty} (1 - z^k)^{-\frac{\mu(k)}{k}} (1 - z^{pk})^{\frac{\mu(k)}{kp}} \tag{8}$$

où μ est ici la fonction de Möbius.

Remarque. Pour rappelle, si $n = p_1 \dots p_s$ avec les p_i distincts, $\mu(n) = (-1)^s$. Si n est divisible par le carré d'un nombre premier, alors $\mu(n) = 0$.

Démonstration. Commençons par démontrer l'égalité 7.

$$\ln\left(\prod_{k=1}^{\infty}(1-z^k)^{-\frac{\mu(k)}{k}}\right) = \sum_{k=1}^{\infty} -\frac{\mu(k)}{k}\ln(1-z^k) = \sum_{k=1}^{\infty} -\frac{\mu(k)}{k}\sum_{l=1}^{\infty}\frac{z^{kl}}{l}$$
$$= \sum_{j=1}^{\infty}\left(\frac{z^j}{j}\sum_{k|j}\mu(k)\right) = z$$

car $\sum_{k|j}\mu(k) = 0$ pour $k \geq 2$. D'où l'égalité 7. L'égalité 8 en découle en ne faisant apparaître que les cas où p^2 ne divise pas k, car dans les autres cas $\mu(k) = 0$ et si $k \wedge p = 1$, $\mu(pk) = -\mu(k)$. □

De ce lemme, on tire les expressions suivantes :

$$\begin{aligned}\exp(z+\frac{z^p}{p}) &= \exp(z)\exp(\frac{z^p}{p}) \\ &= \prod_{\substack{k=1\\ k\wedge p=1}}^{\infty}(1-z^k)^{-\frac{\mu(k)}{k}}(1-z^{pk})^{\frac{\mu(k)}{kp}}\left((1-z^{pk})^{-\frac{\mu(k)}{k}}(1-z^{p^2k})^{\frac{\mu(k)}{kp}}\right)^{\frac{1}{p}} \\ &= \prod_{\substack{k=1\\ k\wedge p=1}}^{\infty}(1-z^k)^{-\frac{\mu(k)}{k}}(1-z^{kp^2})^{\frac{\mu(k)}{kp^2}}\end{aligned}$$

Et enfin,

$$\theta(z) = \exp\left(\pi z + \frac{(\pi z)^p}{p}\right) = \prod_{k\wedge p=1}(1-\pi^k z^k)^{-\frac{\mu(k)}{k}}(1-\pi^{kp^2}z^{kp^2})^{\frac{\mu(k)}{kp^2}}$$

Nous allons partir de cette expression pour montrer les résultats voulus sur le λ_r. Montrons d'abord que pour $k\wedge p = 1$ et $j \in \mathbf{N}$, $\frac{\mu(k)}{k} \in \mathbf{Z}_p$ et $\binom{-\frac{\mu(k)}{k}}{j} \in \mathbf{Z}_p$. Premièrement, $\frac{\mu(k)}{k} \in \mathbf{Q}_p$ et si $\frac{\mu(k)}{k} \neq 0$, $\mathrm{ord}_p(\frac{\mu(k)}{k}) = -\mathrm{ord}_p(k) = 0$ car $k \wedge p = 1$. Donc $\|\frac{\mu(k)}{k}\|_p \leq 1$, ie. $\frac{\mu(k)}{k} \in \mathbf{Z}_p$. Ensuite, nous pouvons appliquer le lemme 5 et conclure.

Le terme $(1-\pi^k z^k)^{-\frac{\mu(k)}{k}}$ Ce terme s'écrit $(1-\pi^k z^k)^{-\frac{\mu(k)}{k}} = \sum_{j=0}^{\infty} b_j(k) z^{kj}$ avec $b_j(k) = \binom{-\frac{\mu(k)}{k}}{j}(-\pi^k)^j$. Alors $\mathrm{ord}_p(b_j(k) = \mathrm{ord}_p(\binom{-\frac{\mu(k)}{k}}{j}) + jk\mathrm{ord}_p(\pi)$. Or $\binom{-\frac{\mu(k)}{k}}{j} \in \mathbf{Z}_p$ et donc $\mathrm{ord}_p(\binom{-\frac{\mu(k)}{k}}{j}) \geq 0$. Donc $\mathrm{ord}_p(b_j(k) \geq \frac{jk}{p-1} \geq \frac{p-1}{p^2}jk$.

Le terme $(1-\pi^{kp^2}z^{kp^2})^{\frac{\mu(k)}{kp^2}}$ De même, ce terme s'écrit $(1-\pi^{kp^2}z^{kp^2})^{\frac{\mu(k)}{kp^2}} = \sum_{j=0}^{\infty} c_j(kp^2) z^{kjp^2}$ avec $c_j(kp^2) = \binom{-\frac{\mu(k)}{kp^2}}{j}(-\pi^{kp^2})^j$. Nous avons vu précédemment que pour tout

$n = a_0 + a_1 p + \cdots + a_s p^s \in \mathbf{N}$, $\mathrm{ord}_p(n!) = \frac{n - S_n}{p-1}$, où $S_n = \sum_{i=0}^{s} a_i$. Ainsi $S_n \leq n$, donc $\mathrm{ord}_p(n!) < \frac{n}{p-1}$ pour $n > 0$. Donc

$$\begin{aligned}
\mathrm{ord}_p\left(\binom{\frac{\mu(k)}{kp^2}}{j}\right) &= \sum_{i=0}^{j-1} \mathrm{ord}_p\left(\frac{\mu(k)}{kp^2} - i\right) - \mathrm{ord}_p(j!) \\
&= \sum_{i=0}^{j-1} \mathrm{ord}_p\left(\frac{\mu(k) - kp^2 i}{kp^2}\right) - \mathrm{ord}_p(j!) \\
&= \sum_{i=0}^{j-1} \big(\mathrm{ord}_p(\mu(k) - kp^2 i) - \mathrm{ord}_p(kp^2)\big) - \mathrm{ord}_p(j!) \\
&> \sum_{i=0}^{j-1} -\mathrm{ord}_p(kp^2) - \mathrm{ord}_p(j!) \text{ car } \mu(k) - kp^2 i \in \mathbf{Z}_p \\
&> -2j - \frac{j}{p-1}
\end{aligned}$$

Alors

$$\begin{aligned}
\mathrm{ord}_p(c_j(kp^2)) &= \mathrm{ord}_p\left(\binom{\frac{\mu(k)}{kp^2}}{j}\right) + \mathrm{ord}_p((-\pi^{kp^2})^j) \\
&> -2j - \frac{j}{p-1} + \frac{jkp^2}{p-1} \geq \frac{p-1}{p^2} jkp^2
\end{aligned}$$

Conclusions sur la convergence de θ Revenons à l'expression

$$\theta(z) = \prod_{k \wedge p = 1} (1 - \pi^k z^k)^{-\frac{\mu(k)}{k}} (1 - \pi^{kp^2} z^{kp^2})^{\frac{\mu(k)}{kp^2}}$$

Ainsi

$$\begin{aligned}
\theta(z) &= \prod_{k \wedge p = 1} \sum_{j=0}^{\infty} b_j(k) z^{kj} \sum_{j=0}^{\infty} c_j(kp^2) z^{kjp^2} \\
&= \prod_{k \wedge p = 1} \sum_{N \geq 0} \left(\sum_{\substack{j,i \geq 0 \\ kj + kip^2 = N}} b_j(k) c_i(kp^2) \right) z^N \\
&= \prod_{k \wedge p = 1} \sum_{N \geq 0} d_N(k) z^N
\end{aligned}$$

Avec ce qui précède,

$$\mathrm{ord}_p(d_N(k)) \geq \min_{\substack{j,i \geq 0 \\ kj + kip^2 = N}} \big(\mathrm{ord}_p(b_j(k) c_i(kp^2))\big) > \frac{p-1}{p^2}(kj + kip^2) = \frac{p-1}{p^2} N$$

Or $\theta(z) = \sum_{r=0}^{\infty} \lambda_r z^r$ où λ_r est alors une somme de produits de $d_N(k)$ avec, pour chaque terme de la somme, les N dans le produit somment à r. Donc $\mathrm{ord}_p(\lambda_r) > \frac{p-1}{p^2} r$. Cela montre aussi que $\lambda_r \in R_1 = \mathbf{Z}_p[\pi]$ puisque les b_j et c_i sont dans R_1 et donc les d_N aussi. Ce qui démontre le lemme 11.

Nous pouvons enfin conclure la démonstration de la proposition 9. $\theta(z)$ converge si et seulement si $\mathrm{ord}_p(\lambda_r z^r) \xrightarrow[r\to\infty]{} \infty$. Or

$$\mathrm{ord}_p(\lambda_r z^r) = \mathrm{ord}_p(\lambda_r) + r\mathrm{ord}_p(z) > \left(\frac{p-1}{p^2} + \mathrm{ord}_p(z)\right) r$$

Donc il suffit que $\mathrm{ord}_p(z) > -\frac{p-1}{p^2}$, ie $\|z\|_p < p^{\frac{p-1}{p^2}}$. En posant $\epsilon = p^{\frac{p-1}{p^2}} - 1 > 0$, on obtient le résultat voulu.

Proposition 10. $\theta(z) \equiv 1 + \pi z \mod \pi^2 z^2$

Démonstration. On considère la fonction exponentielle d'Artin-Hasse :

$$E(z) = \prod_{k\wedge p=1} (1 - z^k)^{-\frac{\mu(k)}{k}} = \exp\left(\sum_{i\geq 0} \frac{z^{p^i}}{p^i}\right)$$

de sorte que $E(\pi z) \equiv \theta(z) \mod z^{p^2}$. Ainsi, $E(\pi z) = \prod_{k\wedge p=1} \sum_{j=0}^{\infty} b_j(k) z^{kj}$, et par le même raisonnement que ci-dessus, on déduit que pour $r \in [\![0, p^2 - 1]\!]$,

$$\mathrm{ord}_p(\lambda_r) \geq \frac{r}{p-1}$$

Alors, avec ce qui précède, pour $r \geq 2$, $\mathrm{ord}_p(\lambda_r) \geq \frac{2}{p-1}$, et $r \geq 2$,

$$\lambda_r \equiv 0 \mod \pi^2$$

De plus $\lambda_0 = \theta(0) = 1$, et $\lambda_1 = b_1(1) = \pi$. D'où le résultat. □

Remarque. On en déduit que $\theta(1) \neq 1$.

2.2.2 La suite de caractères Ψ_k

Ce qui précède nous permet de définir la suite de caractères suivante.

Définition 12. Notons pour$k \geq 1$, $\Phi_k(z) = \prod_{i=0}^{ak-1} \theta(z^{p^i})$ des séries à coefficients dans $\mathbf{R}_1$. Alors on pose

$$\Psi_k(z) = \Phi_k \circ \omega : \mathbf{F}_{q^k} \to R_1$$

Remarque. On rappelle que $q = p^a$ et que ω est le relèvement de Teichmüller.

Nous allons maintenant montrer que cette suite de caractères est de la forme voulue, c'est-à-dire $\Psi_k = \Psi_1 \circ Tr_{\mathbf{F}_{q^k}/\mathbf{F}_q}$ et que Ψ_k est bien à valeurs dans R_1. Pour cela, nous allons montrer que θ est une *splitting function*.

Définition 13 (Splitting function)**.** Une fonction θ est une *splitting function* si θ est une série entière à coefficients dans Ω, notons $\theta(z) = \sum_{i=0}^{\infty} \lambda_i z^i$ et si elle vérifie les propriétés suivantes.

1. Il existe $b > 0$ tel que pour tout $i \in \mathbf{N}$, $\mathrm{ord}_p(\lambda_i) \geq bi$
2. $\theta(1)$ est une racine p-ème primitive de l'unité
3. Pour tous $\gamma \in \Omega$ tel qu'il existe $s \in \mathbf{N}^*$ avec $\gamma^{p^s} = \gamma$,
$$\prod_{i=0}^{s-1} \theta(\gamma^{p^i}) = \theta(1)^{\sum_{j=0}^{s-1} \gamma^{p^i}}$$
4. Il existe une extension finie K de $\mathbf{Q}_p$ telle que pour $i \in \mathbf{N}$, $\lambda_i \in K$.

Les propriétés 1 et 4 sont des conséquences du lemme 11.
On montre alors que $\theta(1)$ est une racine p-ème de l'unité.

$$\theta(z)^p = \exp(p(\pi z - \pi z^p)) = \exp(p\pi z)\exp(-p\pi z^p)$$

On peut ici appliquer ces fonctions en $z = 1$ directement car les séries $\exp(p\pi z)$ et $\exp(-p\pi z^p)$ convergent bien sur le disque unité fermé. En effet le terme général de $\exp(p\pi z)$ est $\frac{(p\pi z)^n}{n!}$ et

$$\mathrm{ord}_p\left(\frac{(p\pi z)^n}{n!}\right) = n\left(1 + \frac{1}{p-1} + \mathrm{ord}_p(z)\right) - \frac{n - S_n}{p-1} = n(1+\mathrm{ord}_p(z)) + \frac{S_n}{p-1} \to \infty$$

si $\mathrm{ord}_p(z) > -1$, ie si $\|z\|_p < p$. De même pour $\exp(-p\pi z^p)$. Ainsi, $\theta(1)^p = 1$. $\theta(1)$ est donc même une racine p-ème primitive de l'unité. En particulier, la proposition 7 confirme que $\theta(1) \in R_1 = \mathbf{Z}_p[\pi]$. cela démontre la propriété 2.

Nous allons maintenant montrer la propriété 3, dans le cas qui nous intéresse. Soit $\gamma \in \Omega$, tel qu'il existe $k \in \mathbf{N}^*$ avec $\gamma^{p^{ak}} = \gamma$. Alors comme précédemment

$$\left(\prod_{i=0}^{s-1} \theta(\gamma^{p^i})\right)^p = \exp\left(p\pi \sum_{i=0}^{s-1} (\gamma^{p^i} - \gamma^{p^{i+1}})\right) = \exp(p\pi\gamma)\exp(-p\pi\gamma^{p^{ak}}) = 1$$

De plus $\left(\theta(1)^{\sum_{j=0}^{s-1} \gamma^{p^i}}\right)^p = 1$ car $\theta(1)$ est une racine p-ème. Et nous avons vu précédemment que $\theta(z) \equiv 1 + \pi z \mod \pi^2 z^2$. Donc $\theta(1)^{\sum_{j=0}^{s-1} \gamma^{p^i}} \equiv 1 + \pi\left(\sum_{j=0}^{s-1} \gamma^{p^i}\right)$ mod π^2 et $\prod_{i=0}^{s-1} \theta(\gamma^{p^i}) \equiv 1 + \pi\left(\sum_{j=0}^{s-1} \gamma^{p^i}\right) \mod \pi^2$. Donc $\prod_{i=0}^{s-1} \theta(\gamma^{p^i})$ et $\theta(1)^{\sum_{j=0}^{s-1} \gamma^{p^i}}$

sont des racine p-ème de l'unité dans Ω Or nous avons vu que les racines p-ème dans Ω sont distinctes modulo π^2. Donc $\prod_{i=0}^{s-1} \theta(\gamma^{p^i}) = \theta(1)^{\sum_{j=0}^{s-1} \gamma^{p^i}}$.

On en conclut que $\Psi_1(.) = \theta(1)^{\omega(.)} : \mathbf{F}_q \to R_1$ est un caractère non trivial et pour $k \geq 1$, $\Psi_k = \Psi_1 \circ Tr_{\mathbf{F}_{q^k}/\mathbf{F}_q}$. Pour pouvoir appliquer le lemme 10 dans la suite, il reste à vérifier que pour $k \in \mathbf{N}^*$, $\sum_{x \in \mathbf{F}_{q^k}} \Psi_k(x) = 0$. Or

$$\sum_{x \in \mathbf{F}_{q^k}} \Psi_k(x) = \sum_{x \in \mathbf{F}_{q^k}} \theta(1)^{Tr_{\mathbf{F}_{q^k}/\mathbf{F}_q}(x)} = k \sum_{x \in \mathbf{F}_p} \theta(1)^x = 0$$

car $\theta(1) \neq 1$.

Remarque. Dans ses travaux, Dwork définit toute une suite de telles *splitting functions*, chacune définie de façon analogue à θ : $\theta_k(z) = \exp\left(\sum_{i=0}^{k} \frac{(z\gamma_k)^{p^i}}{p^i}\right)$, où γ_k est définit au début de la partie 2.1.

Nous trouvons enfin l'expression pour N_s

$$\forall s \in \mathbf{N}^*, \sum_{x \in (\mathbf{F}_{q^s}^*)^{n+1}} \Psi_s(x_0 f(x_1, \ldots, x_n)) = q^s N_s^* - (q^s - 1)^n$$

Nous allons alors trouver une nouvelle expression du membre de gauche. Rappelons que $f \in \mathbf{F}_q[X_1, \ldots, X_n]$. Nous définissons alors trois nouvelles fonctions :

$$X_0 f = \sum_{j \in J} \bar{a}_j X^j$$

où $J \subset \mathbf{N}^{n+1}$ est fini. Notons $a_j = \omega(\bar{a}_j)$

$$F(X) = \prod_{j \in J} \theta(a_j X^j) \text{ et } F^{(a)}(X) = \prod_{j \in J} \prod_{s=0}^{a-1} \theta((a_j X^j)^{p^s}))$$

Nous verrons dans la démonstration de la proposition suivante que $F^{(a)}$ apparaît naturellement, ce qui justifie que l'on prenne $F^{(a)}$ sous cette forme.

On trouve alors l'expression suivante :

Proposition 11.

$$\forall s \in \mathbf{N}^*, q^s N_s^* - (q^s - 1)^n = \sum_{x^{q^s - 1} = 1} F^{(a)}(x) F^{(a)}(x^q) \ldots F^{(a)}(x^{q^{s-1}})$$

où la somme se fait sur les $(n+1)$-uplets de racines $(q^s - 1)$-èmes de l'unité dans Ω.

Démonstration. Soient $s \in \mathbf{N}^*$ et $\bar{x} \in (\mathbf{F}_{q^k})^{n+1}$.

$$\begin{aligned}
\Psi_s(\bar{x_0} f(\bar{x}_1, \ldots, \bar{x}_n)) &= \Psi_s(\sum_{j \in J} \bar{a}_j \bar{x}^j) \\
&= \prod_{j \in J} \Psi_s(\bar{a}_j \bar{x}^j) \text{ car } \Psi_s \text{ est un caractère} \\
&= \prod_{j \in J} \Phi_s(a_j x^j) \text{ par définition} \\
&= \prod_{j \in J} \left(\prod_{i=0}^{as-1} \theta((a_j x^j)^{p^i}) \right) \text{ par définition} \\
&= \prod_{j \in J} \left(\prod_{i'=0}^{s-1} \prod_{k=0}^{a-1} \theta((a_j x^j)^{p^{ai'} p^k}) \right) \text{ en posant } i = ai' + k \\
&= \prod_{i'=0}^{s-1} \left(\prod_{j \in J} \prod_{k=0}^{a-1} \theta((a_j^{q^{i'}} x^{q^{i'} j})^{p^k}) \right)
\end{aligned}$$

Or pour $\bar{a}_j \in \mathbf{F}_q$, $a_j^q = \omega(\bar{a}_j)^q = \omega(\bar{a}_j^q) = \omega(\bar{a}_j) = a_j$. Donc

$$\begin{aligned}
\Psi_s(\bar{x_0} f(\bar{x}_1, \ldots, \bar{x}_n)) &= \prod_{i'=0}^{s-1} \left(\prod_{j \in J} \prod_{k=0}^{a-1} \theta((a_j x^{q^{i'} j})^{p^k}) \right) \\
&= F^{(a)}(x) F^{(a)}(x^q) \ldots F^{(a)}(x^{q^{s-1}})
\end{aligned}$$

On trouve alors le résultat en sommant sur $(\mathbf{F}_{q^s}^*)^{n+1}$. □

Nous terminons ce paragraphe sur un résultat exprimant le lien entre F et $F^{(a)}$.

Lemme 13. $F^{(a)}(X) = \prod_{i=0}^{a-1} \tau^i(F(X^{p^i}))$

Démonstration. Il suffit de montrer que

$$\forall i \in [\![0, a-1]\!], \tau^i(F(X^{p^i})) = \prod_{j \in J} \theta((a_j X^j)^{p^i})$$

Or $\tau(X) = X$, $\tau_{|R_1} = id_{R_1}$ et pour $j \in J$, $\tau(a_j) = \tau(\omega(\bar{a}_j)) = \omega(\bar{a}_j)^p = a_j^p$

d'après le lemme 9. Donc

$$\begin{aligned}\tau^i(F^{(a)}(X)) &= \tau^i(\prod_{j\in J}\theta((a_jX^j)^{p^i}))\\ &= \prod_{j\in J}\theta(\tau^i(a_jX^{jp^i}))\text{ car }\forall r,\lambda_r\in R_1\text{ et }a_j^p=a_j\\ &= \prod_{j\in J}\theta(\tau^i(a_j)X^{jp^i})\text{ car }\tau(X)=X\\ &= \prod_{j\in J}\theta((a_jX^j)^{p^i})\end{aligned}$$

D'où le résultat. □

2.2.3 Fin de la démonstration de la formule de la trace de Dwork

On considère le support de $f\in\mathbf{F}_q[X_1,\ldots,X_n]$, noté $Supp(f)\subset\mathbf{N}^n$, l'ensemble des n-uplets des puissances des termes de f. Autrement dit $f=\sum_{i\in I}\bar{a}_iX^i$, où $I\subset\mathbf{N}^n$, et pour tout $i\in I$, $\bar{a}_i\neq 0$.

Définition 14. On note $\delta_1=Conv(Supp(f))\subset\mathbf{R}^n$, l'enveloppe convexe du support de f. On appelle δ_1 le *polytope de* Newton de f.

De plus, si on note $d=\deg(f)$, on pose $\delta_2\subset\mathbf{R}^n$ l'enveloppe convexe de $(0,\ldots,0)$ et des sommets $(d,0,\ldots,0),(0,d,0,\ldots,0),\ldots,(0,\ldots,0,d))$.

Alors pour tout polytope convexe δ tel que $\delta_1,\subset\delta\subset\delta_2$, on pose $\Delta\subset\mathbf{R}^{n+1}$ l'enveloppe convexe de l'origine avec l'image de δ par $x\in\mathbf{R}^n\mapsto(1,x)\in\mathbf{R}^{n+1}$.

Ensuite, $C(\Delta)$ désignera l'*enveloppe positive* de Δ, c'est à dire

$$C(\Delta)=\{tx\in\mathbf{R}^{n+1}\mid t\in\mathbf{R}^+,x\in\Delta\}$$

Enfin, on définit l'anneau $\mathfrak{L}_\Delta=\{\sum_{r\in C(\Delta)\cap\mathbf{Z}^{n+1}}A_rX^r\mid A_r\in R\}$.

Remarque. Δ_1 est le polytope de Newton de X_0f.

Exemple 6. Considérons $f=X_1+X_1^2X_2+X_1X_2^2$. Alors les ensembles δ_1, Δ_1 et $C(\Delta_1)$ sont illustrés dans la figure 1.

Exemple 7. $F\in\mathfrak{L}_\Delta$, et grâce au lemme 13, $F^{(a)}\in\mathfrak{L}_\Delta$.

Nous allons maintenant définir trois fonctions principales qui apparaissent dans la formule de Dwork et dans sa preuve. Tout d'abord, nous définissons une sorte de morphisme de Frobenius inverse.

Définition 15. On définit ψ_p sur $R[[X]]$ ainsi :

$$\psi_p(X^r)=\begin{cases}X^{\frac{r}{p}}\text{ si }p|r\\ 0\text{ sinon}\end{cases}$$

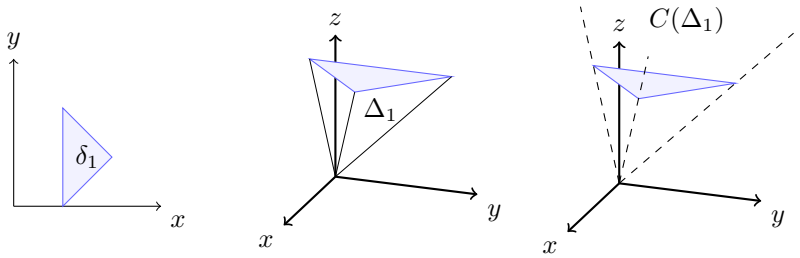


FIGURE 1 – δ_1, Δ_1 et $C(\Delta_1)$

Puis on l'étend à tout $R[[X]]$ par τ^{-1}-linéarité, ie

$$\psi_p(\sum_r A_r X^r) = \sum_r \tau^{-1}(A_r)\psi_p(X^r) = \sum_r \tau^{-1}(A_{pr})X^r$$

Remarque. ψ_p n'est pas l'inverse de τ car $\tau(\sum_r A_r X^r) = \sum_r \tau(A_r)X^r$ et non $\sum_r \tau(A_r)X^{pr}$, et tout simplement car ψ_p n'est pas un automorphisme.

Définition 16. On pose

$$\alpha = \psi_p \circ F$$
$$\alpha_a = \psi_p^a \circ F^{(a)}$$

où F et $F^{(a)}$ agissent par multiplication.

Remarque. ψ_p^a a la même action que ψ_q.

Lemme 14.

$$\alpha_a = \alpha^a$$

Démonstration. Pour commencer, nous remarquons que pour $H \in R[[X]]$,

$$\psi_p \circ H(X^p) = \tau^{-1}(H(X)) \circ \psi_p$$

En effet, en notant $H = \sum_r H_r X^r$,

$$\begin{aligned}\psi_p \circ H(X^p)) &= \sum_r \tau^{-1}(H_r)(\psi \circ X^{pr}) = \sum_r \tau^{-1}(H_r)X^r \circ \psi_p \\ &= \tau^{-1}(H(X)) \circ \psi_p\end{aligned}$$

car $\psi_p \circ X^{pr}$ et $X^r \circ \psi_p$ coïncident sur les monômes et donc sur tout $R[[X]]$ par τ^{-1}-linéarité.

Montrons alors par récurrence sur b la proposition suivante :

$$\forall b \in \mathbf{N}^*, \forall H \in R[[X]], \psi_p^b \circ \prod_{i=0}^{b-1} \tau^i(H(X^{p^i})) = (\psi_p \circ H)^b$$

Le cas $b = 1$ est trivial. Soit $b \geq 2$ et supposons le résultat vrai pour $i \in [\![1, b-1]\!]$. Soit $H \in R[[X]]$.

$$\begin{aligned}\psi_p^b \circ \prod_{i=0}^{b-1} \tau^i(H(X^{p^i})) &= \psi_p^b \circ \left(\tau^{b-1}(H(X^{p^{b-1}})) \prod_{i=0}^{b-2} \tau^i(H(X^{p^i})) \right) \\ &= \psi_p \circ \left(\psi_b^{b-1} \circ \tau^{b-1}(H(X^{p^{b-1}})) \right) \left(\prod_{i=0}^{b-2} \tau^i(H(X^{p^i})) \right) \\ &= (\psi_p \circ H(X)) \circ \left(\psi_p^{b-1} \circ \prod_{i=0}^{b-2} \tau^i(H(X^{p^i})) \right)\end{aligned}$$

grâce à la remarque ci-dessus. Ainsi, la propriété de récurrence est vraie et en prenant $H = F$, le lemme est démontré. □

Remarque. α est τ^{-1}-linéaire comme ψ_p. Donc α_a est τ^{-a}-linéaire. Or $\tau^a = id$, donc α_a est tout simplement linéaire.

Lemme 15. *$\mathfrak{L}_\Delta$ est stable par α et α_a.*

Démonstration. Cela découle tout d'abord du fait que F et $F^{(a)}$ sont dans $\mathfrak{L}_\Delta$. Il suffit maintenant de montrer que $\mathfrak{L}_\Delta$ est stable par ψ_p. Soit $r \in C(\Delta) \cap \mathbf{Z}^{n+1}$. Si $p \not| r$, $\psi_p(X^r) = 0 \in \mathfrak{L}_\Delta$. Si $p|r$, $\frac{r}{p} \in C(\Delta)$ car $C(\Delta)$ est stable par multiplication par un réel *positif*, et $\frac{r}{p} \in \mathbf{Z}^{n+1}$. Donc $\psi_p(X^r) \in \mathfrak{L}_\Delta$ et donc par τ^{-1}-linéarité, $\mathfrak{L}_\Delta$ est stable par ψ_p. □

On considère alors les matrices qui décrivent l'action de α et α_a sur $\mathfrak{L}_\Delta$ par multiplication à gauche.

Définition 17. Notons $F(X) = \sum_r F_r X^r$ et $F^{(a)}(X) = \sum_r F_r^{(a)} X^r$ (F et $F^{(a)}$ sont dan $\mathfrak{L}_\Delta$). On pose alors $M = (m_{u,v})_{u,v \in C(\Delta)}$ et $M_a = (m_{u,v}^{(a)})_{u,v \in C(\Delta)}$ les matrices infinies avec, pour $u, v \in C(\Delta)$,

$$\begin{aligned} m_{u,v} &= \tau^{-1}(F_{pu-v}) \\ m_{u,v}^{(a)} &= F_{qu-v}^{(a)} \end{aligned}$$

où $F_r = F_r^{(a)} = 0$ si $r \notin C(\Delta) \cap \mathbf{N}^{n+1}$.

Remarque. Ce choix de M et M_a se justifie ainsi :

$$\begin{aligned}\alpha(X^v) = \psi_p(\sum_r F_r X^{r+v}) &= \sum_r \tau^{-1}(F_r)\psi_p(X^{r+v}) \\ &= \sum_{\substack{r \\ p|r+v}} \tau^{-1}(F_r)\psi_p(X^{r+v})\end{aligned}$$

car $\psi_p(X^{r+v}) = 0$ si $P \not| r+v$. On pose alors $r+v = pu$ et on trouve

$$\begin{aligned}\alpha(X^v) &= \sum_u \tau^{-1}(F_{pu-v})\psi_p(X^{pu}) \\ &= \sum_u \tau^{-1}(F_{pu-v})X^u \\ &= \sum_u m_{u,v}X^u\end{aligned}$$

Et de même pour M_a.

De plus, pour tout $k \in \mathbf{N}$, M^k et M_a^k sont bien définis car leurs coefficient ne sont que des sommes finies de produits finis des coefficients de M et M_a.

Remarque. Nous pouvons aussi étendre ces définitions à M_{ak}, pour tout $k \in \mathbf{N}^*$, où M_{ak} est alors la matrice infinie représentant l'action de $\psi_p^{ak} \circ \prod_{i=0}^{k-1} F^{(a)}(X^{q^i})$ sur $\mathfrak{L}_\Delta$.

Cette dernière remarque se justifie d'autant plus avec le lemme suivant.

Lemme 16. *Pour $k \in \mathbf{N}^*$, $M_{ak} = M_a^k$.*

Démonstration. Pour cela, il suffit de montrer que $\alpha_a^k = \psi_p^{ak} \circ \prod_{i=0}^{k-1} F^{(a)}(X^{q^i})$. Or $\alpha_a^k = \left(\psi_p^a \circ F^{(a)}\right)^k$, et nous avons montré dans la démonstration du lemme 14 que pour $H \in R[[X]]$,

$$\psi_p \circ H(X^p) = \tau^{-1}(H(X)) \circ \psi_p$$

Ainsi,

$$\psi_p^a \circ H(X^{p^a}) = H(X) \circ \psi_p^a$$

Et on trouve le résultat en prenant $H = F^{(a)}$ et en remontant progressivement les $F^{(a)}(X^{q^i})$. □

Il manque alors un dernier élément pour énoncer et démontrer la formule de la trace de Dwork.

Définition 18. On définit la trace d'une matrice infinie M,

$$Tr(M) = \begin{cases} \sum_u m(u,u) \text{ si cette somme converge} \\ \infty \text{ sinon} \end{cases}$$

On rappelle alors le théorème 4.

Théorème (Formule de la trace de Dwork)**.** *Pour $s \in \mathbf{N}^*$,*

$$(q^s-1)^{n+1}Tr(M_a^s) = q^s N_s^* - (q^s-1)^n$$

Démonstration. On a montré jusque là dans la poposition 11 l'égalité suivante

$$\forall s \in \mathbf{N}^*, q^s N_s^* - (q^s-1)^n = \sum_{x^{q^s-1}=1} F^{(a)}(x)F^{(a)}(x^q)\dots F^{(a)}(x^{q^{s-1}})$$

où la somme se fait sur les $(n+1)$-uplets de racines (q^s-1)-èmes de l'unité dans Ω.

Nous allons montrer l'égalité, pour tout s,

$$\sum_{x^{q^s-1}=1} F^{(a)}(x)F^{(a)}(x^q)\dots F^{(a)}(x^{q^{s-1}}) = (q^s-1)^{n+1}Tr(M_{as})$$

On trouvera alors le résultat grâce au lemme 16.

Soit $s \in \mathbf{N}^*$. On note $\prod_{i=0}^{s-1} F^{(a)}(X^{q^i}) = \sum_{r \in C(\Delta)\cap \mathbf{Z}^{n+1}} F_r^{(as)} X^r$. Alors

$$\begin{aligned}\sum_{x^{q^s-1}=1} \prod_{i=0}^{s-1} F^{(a)}(x^{q^i}) &= \sum_{x^{q^s-1}=1} \sum_r F_r^{(as)} x^r \\ &= \sum_r F_r^{(as)} \left(\sum_{x^{q^s-1}=1} x^r \right)\end{aligned}$$

Or par un résultat classique, identique au résultat de la démonstration du lemme 10,

$$\sum_{x_i^{q^s-1}=1} x_i^{r_i} = \begin{cases} q^s-1 \text{ si } q^s-1 | r_i \\ 0 \text{ sinon} \end{cases}$$

Donc

$$\begin{aligned}\sum_{x^{q^s-1}=1} \prod_{i=0}^{s-1} F^{(a)}(x^{q^i}) &= \sum_{\substack{r \\ q^s-1|r}} F_r^{(as)} (q^s-1)^{n+1} \\ &= (q^s-1)^{n+1} \sum_r F_{(q^s-1)r}^{(as)}\end{aligned}$$

Or M_{as} est la matrice de $\psi_p^{as} \circ \prod_{i=0}^{s-1} F^{(a)}(X^{q^i})$. Donc

$$\begin{aligned}\left(\psi_p^{as} \circ \prod_{i=0}^{s-1} F^{(a)}(X^{q^i}) \right)(X^v) &= \psi_p^{as} \left(\sum_r F_r^{as} X^{r+v} \right) \\ &= \sum_u F_{q^s u - v}^{as} X^v\end{aligned}$$

comme précédemment. Donc $m_{u,v}^{(as)} = F_{q^s u - v}^{(as)}$. Et donc

$$\sum_r F_{(q^s-1)r}^{(as)} = Tr(M_{as}) = Tr(M_a^k)$$

Ainsi le théorème est démontré. □

3 Quelques résultats sur le degré des fonctions L

Dans cette partie, nous allons brièvement présenter quelques résultats que nous admettrons sur le degré d'un type de fonction proche des fonctions zêta : les fonction L. Ces résultats sont dues notamment aux travaux de Dwork, puis Adolphson et Sperber dans [1].

Nous maintenons la notation $q = p^a$ où p est premier. Nous fixons quatre entiers $n, m \in \mathbf{N}^*$, $r, s \in \mathbf{N}$, tels que $n = r + s$. Nous notons aussi $S = [\![1, n]\!]$, $S_1 = [\![1, r]\!]$ et $S_2 = [\![r+1, n]\!]$. Nous allons considérer des sommes exponentielles dans un cas plus général que précédemment, sur la variété suivante $V = (\mathbf{F}_{q^m})^r \times \mathbf{A}^s$. Nous imposons aussi des conditions différentes aux polynômes que nous étudions. En particulier, nous fixons $f = \sum_{j \in J} a_j X^j$ dans $\mathbf{F}_q[X_1, \ldots, X_n, (X_1 \ldots X_r)^{-1}]$, et nous exigeons qu'il soit *non-dégénéré* et *commode* par rapport à S_2, que nous expliquerons ci-dessous.

Définition 19. Les fonctions L de variétés algébriques sont des objets semblables aux fonctions zêta, mais définies à partir des suites que nous noterons $(S_i)_{i \in \mathbf{N}^*}$ et $(S_i^*)_{i \in \mathbf{N}^*}$. Soit $\psi : \mathbf{F}_q \to \mathbf{C}$ un caractère non trivial. Posons pour $i \in \mathbf{N}^*$,

$$S_i = \sum_{x \in V(\mathbf{F}_{q^i})} \psi \circ Tr_{\mathbf{F}_{q^i}/\mathbf{F}_q}(f(x))$$

$$S_i^* = \sum_{x \in (\mathbf{F}_{q^m}^\times)^n (\mathbf{F}_{q^i})} \psi \circ Tr_{\mathbf{F}_{q^i}/\mathbf{F}_q}(f(x))$$

où $X(\mathbf{F}_{q^i}) = \{x \in X \mid x^{q^i - 1} = 1\}$.

Nous posons donc

$$L(f, t) = \exp\left(\sum_{i=1}^{\infty} \frac{S_i(f)}{i} t^i\right)$$

$$L^*(f, t) = \exp\left(\sum_{i=1}^{\infty} \frac{S_i^*(f)}{i} t^i\right)$$

les fonctions L associées à f.

Remarque. La définition est indépendante du choix de ψ. Dans la suite nous utiliserons le même choix que précédemment, $\psi = \Psi_0$.

Remarque. Nous pouvons lier S_i^* à N_i^* de la façon suivante. Si (N_i^*) est la suite associée à un polynôme $f \in \mathbf{F}_q[X_1, \ldots, X_{n-1}]$ et (S_i^*) est associée à $X_n f$ alors d'après ce qui précède, $S_i^* = q^i N_i^* - (q^i - 1)^{n-1}$ Ainsi, d'après ce qui précède,

$$S_i^* = (q^i - 1)^n Tr(M_a^i)$$

On supposera ce résultat dans le cas général.

Notons δ l'opérateur agissant sur une série entière g de terme constant 1, de la façon suivante : $g(t)^\delta = \frac{g(t)}{g(qt)}$. On peut alors exprimer un premier résultat sur L^*.

Lemme 17.

$$L^*(f,t)^{(-1)^{n-1}} = \det(I - t\alpha_a)^{\delta^n}$$

Le résultat principal qui nous intéressera dans cette partie est une majoration des degrés de $L(f,t)$ et $L^*(f,t)$ qui se déduit d'arguments d'homologie.

On note Δ le polytope de Newton de $1+f$ (ie $Conv(\{0\} \cup J)$). On note ici $\mathbb{L}(f)$ le plus petit sous-espace vectoriel de $\mathbf{R}^n$ qui contient Δ, ie. $\mathbb{L}(f) = Vect_{\mathbf{R}^n}(\Delta) = C(\Delta) \cup -C(\Delta)$, dont on note $\tilde{n}$ la dimension. Posons $V(f)$ le volume de Δ dans $\mathbf{R}^n$, et $\tilde{V}(f)$ son volume dans $\mathbb{L}(f)$, pour la mesure de Lebesgue. Alors $V(f) = 0$ si $\mathbb{L}(f) \neq \mathbf{R}^n$.

On note, pour $A \subset S$, $\mathbf{R}^n_A = \{x \in \mathbf{R}^n \mid \forall i \in A, x_i = 0\}$. On pose de façon analogue $V_A(f)$ le volume de $\Delta \cap \mathbf{R}^n_A$ dans $\mathbf{R}^n_A$, et $\tilde{V}_A(f)$ son volume dans $\mathbb{L}(f) \cap \mathbf{R}^n_A$. De plus, on pose

$$\nu_A(f) = \sum B \subset A (-1)^{|B|}(n - |B|)! V_B(f)$$
$$\tilde{\nu}_A(f) = \sum B \subset A (-1)^{|B|}(\dim(\mathbb{L}(f) \cap \mathbf{R}^n_B)! \tilde{V}_B(f)$$

Notons $M(f) = \mathbf{Z}^n \cap C(f)$, et $R(f) = \mathbf{F}_q[x^u \mid u \in M(f)]$. On note w la jauge de l'ensemble Δ dans $\mathbf{R}^n$. On va considérer cette jauge sur $M(f)$. Notons $\bar{R}$ l'espace $R(f)$ mais muni de la multiplication

$$X^u X^{u'} = \begin{cases} X^{u+u'} \text{ si } u \text{ et } u' \text{ sont sur la même face} \\ 0 \text{ sinon} \end{cases}$$

Pour simplifier, nous allons définir B et B_0 de la façon suivante.

$$B_0 = \{ \sum_{r \in C(\Delta) \cap \mathbf{Z}^n} A_r X^r \mid A_r \in R, A_r \xrightarrow[r\to\infty]{} 0\}$$
$$B = \{ \sum_{r \in C(\Delta) \cap \mathbf{Z}^n} A_r X^r \mid A_r \in K, A_r \xrightarrow[r\to\infty]{} 0\}$$

où R est l'anneau de la partie précédente, et K son corps des fractions.

Définition 20 (Complexe de Koszul)**.** Soient A un anneau commutatif, et $(D_i)_{1\leq i\leq n}) : A \to A$ une suite de morphismes d'anneaux. Le *complexe de* Koszul associé est le complexe de chaînes de A-modules suivant

$$K_\bullet(A, (D_i)_{1\leq i\leq n}) : 0 \to \bigwedge^n A^n \xrightarrow{d_n} \bigwedge^{n-1} A^n \xrightarrow{d_{n-1}} \cdots \bigwedge^1 A^n \xrightarrow{d_1} A \to 0$$

où pour $i \in [\![1, r]\!]$, d_i est défini pour $e_1 \wedge \cdots \wedge e_i \in \bigwedge^i A^n$ ainsi

$$d_i(e_1 \wedge \cdots \wedge e_i) = \sum_{k=1}^{i} (-1)^{k+1} \left(\sum_{j=1}^{n} D_j(e_{k,j}) \right) e_1 \wedge \cdots \wedge \hat{e_k} \wedge \cdots \wedge e_i$$

où $e_k = (e_{k,1}, \ldots, e_{k,n}) \in A^n$.

On considère le *sous-complexe* $SK_\bullet(B, (\hat{D}_i)_{1\leq i\leq n})$. Posons θ_i l'endomorphisme de B qui substitue 0 à X_i, et pour $C \subset S$, $B_C = \cap_{i\in C\cap S_2} \ker(\theta_i)$. De plus, notons pour $C = \{i_1 < \cdots < i_l\} \subset S$, $e_C = e_{i_1} \wedge \cdots \wedge e_{i_l}$, tel que $(e_C)_{|C|=l}$ forme une base de $\bigwedge^l B^n$. Alors on pose pour $l \in [\![0, n]\!]$,

$$SK_l = \oplus_{|C|=l} B_{C^c} e_C$$

On relève f en $\hat{f} = \sum_{j\in J} \hat{a}_j X^j \in \Omega[X_1, \ldots, X_n, (X_1 \ldots X_n)^{-1}]$. Pour $i \in [\![1, n]\!]$, on pose

$$E_i = X_i \frac{\partial}{\partial X_i}$$

$$\hat{H}_i(X) = \sum_{l=0}^{\infty} \gamma_l p^l \hat{f}_i^{\tau^l}(X^{p^l}) \in$$

$$\hat{D}_i = E_i + \hat{H}_i$$

On suppose enfin que f est non-dégénéré. Cela signifie que pour toute face σ de Δ qui ne contient pas l'origine, si on note $f_\sigma = \sum_{j\in J\cap\sigma} a_j X^j$, alors $\frac{\partial f_\sigma}{\partial X_1}, \ldots, \frac{\partial f_\sigma}{\partial X_n}$ n'ont pas de zéros en commun dans $(\bar{\mathbf{F}}_q^\times)^n$. On suppose aussi que f est commode, c'est-à-dire que pour tout $A \subset S_2$, $\dim \Delta(f_A) = \dim \Delta(f_{S_2}) + |S_2 \setminus A|$, où f_A est le polynôme f avec tous les X_i pour $i \in A$ valués à 0. On peut alors enfin énoncer les théorèmes suivants.

Théorème 5. *Il existe $\tilde{S}_1 \subset S_1$ tel que $SK_\bullet(B, (\hat{D}_i)_{i\in\tilde{S}_1\cup S_2})$ soit exacte. De plus*

$$\dim H_0(SK_\bullet(B, (\hat{D}_i)_{i\in S})) = \tilde{\nu}_{S_2}(f)$$

Remarque. Nous obtenons ici un résultat très important. En effet, l'étude des groupes d'homologie de ces complexe permet de passer en dimension finie, et ainsi déduire une borne sur les degré de $L(f, t)$ et $L^*(f, t)$ dans le théorème suivant.

Théorème 6. *Si $\tilde{n} = n$, $L^*(f, t)^{(-1)^{n-1}}$ (resp. $L(f, t)^{(-1)^{n-1}}$) est un polynôme de degré $\leq n!V(f)$ (resp. $\leq \nu_{S_2}(f)$). Et si $\tilde{n} < n$, ce sont des fractions rationnelles de degré nul.*

Références

[1] Alan Adolphson and Steven Sperber. Exponential sums and newton polyhedra : Cohomology and estimates. *Annales of Mathematics*, 1989.

[2] Bernard Dwork. On the zeta function of a hypersurface. *Publications mathématiques de l'I.H.É.S.*, tome 12, 1962.

[3] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions.* Graduate Texts in Mathematics. Springer-Verlag, 1948.

[4] Alan G. Lauder and Daqin Wan. Counting points on varieties over finite fields of small characteristic. *Algorithmic Number Theory*, 2002.