Université de Franche-Comté

Projet M2 - Magistère

Théorème de Dwork sur la rationalité de la fonction zeta

Auteur :
Alix Mathieu

Encadrant :
Christine Huyghe

24 janvier 2025

Table des matières

Table des figures

Introduction

0.1 Introduction

En 1959, Bernard Dwork a surpris la communauté mathématique en prouvant la première partie de la conjecture de Weil sous une forme forte, à savoir que la fonction zêta de toute variété algébrique sur un corps fini était une fonction rationnelle. De plus, sa preuve n'était pas du tout conforme à l'idée répandue à l'époque selon laquelle les conjectures de Weil seraient et devraient être résolues par la construction d'une théorie de cohomologie appropriée pour les variétés sur les corps finis. Pour ces travaux, Bernard Dwork reçu le prix Cole en théorie des nombres.

Cette démonstration passe par l'utilisation d'analyse p-adique, c'est celle-ci que nous essayerons de retracer. Nous commencerons dans le chapitre 1 par nous intéresser à la notion de série entières p-adique, puis nous explorerons de nouveaux outils à l'image des polygones de Newton dans le chapitre 2.

Enfin, dans le chapitre 3, nous tacherons d'énoncer le théorème de Borel-Dwork, d'en présenter une preuve, pour enfin l'appliquer à la fonction zêta et montrer la dite rationalité. Pour se faire, il est nécéssaire de s'intéresser à la p-méromorphie de la fonction zêta, on en donnera une preuve complète. Pour ce faire, il est nécessaire d'utiliser une formule liant le déterminant et les traces itérées, celle-ci est présenté dans [4] dans un cadre plus général et dans [5]. On re-démontrera celle-ci dans le cas particulier étudié.

Chapitre 1

Les séries entières p-adiques

1.1 Rappels préliminaires

Proposition 1.1. *Dans un espace métrique dont la distance provient d'une norme $\|.\|$ non-archimédienne, une suite $(x_n)_{n\in\mathbb{N}}$ est de Cauchy si et seulement si $\|x_{n+1} - x_n\| \underset{n\to+\infty}{\longrightarrow} 0$.*

Démonstration.

* Si (x_n) est de Cauchy, alors en considérant $\varepsilon > 0$, il existe $N \in \mathbb{N}$ tel que $\forall n, p \geq N, \left\|x_{n+p} - x_n\right\| \leq \varepsilon$. En prenant $p = 1$, on a bien le résultat souhaité.
* Si $\|x_{n+1} - x_n\| \underset{n\to+\infty}{\longrightarrow} 0$, alors en considérant $\varepsilon > 0$, il existe $N \in \mathbb{N}$ tel que $\forall n \geq N, \|x_{n+1} - x_n\| \leq \varepsilon$ Dès lors, en considérant $n, p \geq N$, on a par non-archimédiannité de la norme que :

$$\begin{aligned}\left\|x_{n+p} - x_n\right\| &= \left\|\sum_{i=n}^{n+p-1} (x_{i+1} - x_i)\right\| \\ &\leq \max\{\|x_{i+1} - x_i\|, i \in \{n, \dots, n+p-1\}\} \\ &\leq \varepsilon\end{aligned}$$

Donc la suite $(x_n)_{n\in\mathbb{N}}$ est de Cauchy.

■

Proposition 1.2. *Dans un espace métrique complet dont la distance provient d'une norme $\|.\|$ non-archimédienne, une série converge si et seulement si son terme général tend vers 0.*

Démonstration. Une série de terme général u_n converge si et seulement si la suite des sommes partielles $(S_n)_{n\in\mathbb{N}}$ est de Cauchy car l'espace métrique est complet. Or par la proposition précédente, cela revient à $\|S_n - S_{n-1}\| = \|u_n\| \underset{n\to+\infty}{\longrightarrow} 0$ ■

Proposition 1.3. *Si on considère un espace métrique complet dont la distance provient d'une norme $\|.\|$ non-archimédienne. Si on prend $(a_n)_{n\in\mathbb{N}}$ une suite telle que $\sum\limits_{n\geq 0} a_n$ converge* (i.e. $a_n \to 0$) *et qu'on considère $(a'_n)_{n\in\mathbb{N}}$ un réarrangement de $(a_n)_{n\in\mathbb{N}}$ alors $\sum\limits_{n\geq 0} a'_n$ converge* (i.e. $a'_n \to 0$) *et $\sum\limits_{n\geq 0} a_n = \sum\limits_{n\geq 0} a'_n$.*

Démonstration.

* Soit $\varepsilon > 0$, comme $a_n \to 0$, alors il existe $N_0 \in \mathbb{N}$ tel que pour tout $n \geq N_0, \|a_n\| \leq \varepsilon$. Mais en terme d'ensemble, $\{a_n, n \in \mathbb{N}\} = \{a'_n, n \in \mathbb{N}\}$ donc la liste $\{a_0, \cdots, a_{N_0-1}\}$ est inclus dans $\{a'_0, \cdots, a'_{N_1-1}\}$ pour un certain $N_1 \in \mathbb{N}$. Alors pour tout $n \geq N_1, \|a'_n\| \leq \varepsilon$ et donc la série $\sum\limits_{n\geq 0} a'_n$ converge par la proposition précédente.

* En notant $S := \sum_{n\geq 0} a_n$, on souhaite montrer que $\sum_{n\geq 0} a'_n = S$. Pour cela, prenons $\varepsilon > 0$, comme $a_n \to 0$, alors $A = \{n, \|a_n\| > \varepsilon\}$ est fini, on peut alors noter m le plus grand entier inclus dans A et ainsi, on a $A \subseteq \{1, 2, \cdots, m\}$. On peut dès lors écrire :

$$\begin{aligned} S - \sum_{n\in A} a_n &= S - \sum_{n=0}^{m} a_n + \sum_{n=0}^{m} a_n - \sum_{n\in A} a_n \\ &= \sum_{n>m} a_n - \left(\sum_{n=0}^{m} a_n - \sum_{n\in A} a_n \right) \end{aligned}$$

On observe qu'en prenant la norme et en utilisant le caractère non-arhcimédien de la norme :

$$\begin{aligned} \left\| S - \sum_{n\in A} a_n \right\| &\leq \left\| \sum_{n>m} a_n \right\| + \left\| \left(\sum_{n=0}^{m} a_n - \sum_{n\in A} a_n \right) \right\| \\ &\leq \underbrace{\max_{n>m} \|a_n\|}_{\leq \varepsilon} + \underbrace{\left\| \left(\sum_{n=0}^{m} a_n - \sum_{n\in A} a_n \right) \right\|}_{\text{chaque terme restant de norme} \leq \varepsilon} \\ &\leq 2\varepsilon \end{aligned}$$

De même, comme $a'_n \to 0$, alors $A' = \{n, \|a'_n\| > \varepsilon\}$ est fini et égal à A car on a juste un réarrangement des a_n. On peut de même noter m' le plus grand entier inclus dans A' et ainsi on a $A' \subseteq \{1, 2, \cdots, m'\}$. On a alors :

$$\sum_{n\in A} a_n = \sum_{n\in A'} a'_n \tag{1.1}$$

et pour $N > m'$,

$$\left\| \sum_{n=0}^{N} a'_n - \sum_{n\in A'} a'_n \right\| \leq \varepsilon \text{ (car chaque terme restant de norme } \leq \varepsilon) \tag{1.2}$$

Ainsi pour $N > m'$, on a :

$$\begin{aligned} \left\| S - \sum_{n=0}^{N} a'_n \right\| &= \left\| S - \sum_{n\in A} a_n + \sum_{n\in A} a_n - \sum_{n=0}^{N} a'_n \right\| \\ &= \left\| S - \sum_{n\in A} a_n + \sum_{n\in A'} a'_n - \sum_{n=0}^{N} a'_n \right\| \\ &\leq \max\left(\left\| S - \sum_{n\in A} a_n \right\|, \left\| \sum_{n\in A'} a'_n - \sum_{n=0}^{N} a'_n \right\| \right) \\ &\leq 2\varepsilon \end{aligned}$$

Ainsi $\sum_{n\geq 0} a'_n = S$.

■

Proposition 1.4. *Soit $F(X,Y) \in \mathbb{R}[[X,Y]]$ s'il existe $(a,b) \in \mathbb{R}$, tel que pour tout $(x,y) \in]a,b[$, $F(x,y) = 0$, alors tous les coefficients de la série formelle sont nuls.*

Démonstration. Notons $F(X,Y) = \sum_{(l,k)\in\mathbb{N}^2} a_{l,k} X^k Y^l$. Dans un premier temps, on remarque :

$$\begin{aligned} F(X,Y) &= \sum_l \left(\sum_k a_{l,k} X^k \right) Y^l \\ &= \sum_l g_l(X) Y^l \text{ où } g_l(X) = \sum_k a_{l,k} X^k \in \mathbb{R}[X] \end{aligned}$$

Comme $\forall (x,y) \in]a,b[, F(x,y) = 0$, alors par le prolongement analytique, on a $\forall x \in]a,b[, \sum_l g_l(x) Y^l = 0$ donc pour tout $x \in]a,b[, l \in \mathbb{N}, g_l(x) = 0$ donc par le prolongement analytique $g_l(X) = 0$ pour tout $l \in \mathbb{N}$. Ainsi $a_{l,k} = 0$ pour tout $(l,k) \in \mathbb{N}^2$ et donc on a la série formelle nulle. ∎

1.2 Séries entières et premières définitions

Remarque 1.5.

- On se placera dans $\mathbb{C}_p$ le complété de la cloture algébrique de $\mathbb{Q}_p$.
- On munira $\mathbb{C}_p$ de la norme p-adique étendue depuis $\mathbb{Q}_p$ que l'on notera toujours $|.|_p$.

Définition 1.6. On appelle série entière tout élément $f(X) = \sum_{n=0}^{+\infty} a_n X^n$ où $a_n \in \mathbb{C}_p$.

Proposition 1.7. *Pour $x \in \mathbb{C}_p$, la série numérique $\sum_{n=0}^{+\infty} a_n x^n$ converge si et seulement si $|a_n x^n|_p \underset{n\to+\infty}{\longrightarrow} 0$*

Démonstration. Cela résultat du fait que $\mathbb{C}_p$ est un espace complet muni d'une norme non-archimédienne $|.|_p$, et on utilise la proposition 1.2. ∎

Définition 1.8. On appelle rayon de convergence d'une serie entière f, noté $R(f)$, l'élément suivant :

$$R(f) = \sup\{r \in \mathbb{R}_+, |a_n|_p \, r^n \underset{n\to+\infty}{\longrightarrow} 0\}$$

Proposition 1.9.

$$R(f) = \frac{1}{\limsup |a_n|_p^{1/n}}$$

Démonstration. Notons pour la suite ici $r = \frac{1}{\limsup |a_n|_p^{1/n}}$

- Supposons que x soit tel que $|x|_p < r$ et montrons que $|a_n x^n|_p \to 0$. Comme $|x|_p < r$, on peut écrire $|x|_p = (1-\varepsilon)r$ pour $\varepsilon > 0$. Ainsi, on a :

  $$|a_n x^n|_p = (r\,|a_n|_p^{1/n})^n (1-\varepsilon)^n$$

  mais par définition de la limite sup, on a pour n assez grand que

  $$|a_n|_p^{1/n} \leq \frac{1}{r(1-\frac{\varepsilon}{2})}$$

et donc que

$$\lim_{n\to+\infty} |a_n x^n|_p \leq \lim_{n\to+\infty} \left(\frac{(1-\varepsilon)^n}{(1-\frac{\varepsilon}{2})^n}\right) = 0$$

* Supposons maintenant que $|x|_p > r$, *i.e.* $\frac{1}{r} > \frac{1}{|x|_p}$ alors pour une infinité de n on a $|a_n|_p^{1/n} |x|_p > 1$, *i.e.* $|a_n x^n|_p > 1$ donc le terme $|a_n x^n|_p$ ne peut converger vers 0.

■

Exemple 1.10. Considérons la série $\sum_{n=1}^{+\infty} \frac{(-1)^{n+1}}{n} X^n$ et intéressons nous à la convergence de cette dite série. Notre terme général ici est $a_n = \frac{(-1)^{n+1}}{n}$, alors on a $|a_n|_p = p^{\mathrm{ord_p}(n)}$ et donc $\lim_{n\to+\infty} |a_n|_p^{1/n} = 1$. Ainsi,

* si $|x|_p < 1$, la série converge.
* si $|x|_p > 1$, la série diverge.
* si $|x|_p = 1$, alors $|a_n x^n|_p = p^{\mathrm{ord_p}\, n} \geq 1$ donc la série diverge.

Avant de continuer, introduisons quelques notations qui nous serons utiles par la suite.

Définition 1.11. Si A est un anneau, on notera

— $A[[X]]$ l'anneau des séries formelles en X à coefficients dans A.

— $1 + XA[[X]] \underset{\text{def}}{:=} \{f \in A[[X]], \text{ de terme constant } a_0 = 1\}$

Définition 1.12. Soit $a \in \mathbb{C}_p$ et $r \in \mathbb{R}$. On appelle

— Disque fermé de centre a et de rayon r l'ensemble :

$$D_a(r) \underset{\text{def}}{:=} \{x \in \mathbb{C}_p, |x-a|_p \leq r\}$$

— Disque ouvert de centre a et de rayon r l'ensemble :

$$D_a(r^-) \underset{\text{def}}{:=} \{x \in \mathbb{C}_p, |x-a|_p < r\}$$

On prendra la notation suivante : $D(r) := D_0(r)$ et $D(r^-) := D_0(r^-)$.

Lemme 1.13. *Toute série entière $f(X) \in \mathbb{Z}_p[[X]]$ converges sur $D(1^-)$.*

Démonstration. Soit $f(X) = \sum_{n=0}^{+\infty} a_n X^n$ tel que $a_n \in \mathbb{Z}_p$ et $x \in D(1^-)$, alors $|x|_p < 1$ et comme $|a_n|_p \leq 1$ pour tout $n \in \mathbb{N}$, on obtient $|a_n x^n|_p \leq |x|_p^n \underset{n\to+\infty}{\longrightarrow} 0$ ce qui assure la convergence. ■

Lemme 1.14. *Toute série entière $f(X) = \sum_{n=0}^{+\infty} a_n X^n \in \mathbb{C}_p[[X]]$ qui converge sur un disque $D = D(r)$ ou $D(r^-)$ est continue sur D.*

Démonstration. Considérons $\varepsilon > 0$, et $x \in D$. Comme la suite $(|a_n x^n|_p)_{n\in\mathbb{N}}$ converge, elle est bornée disons par un élément $M > 0$. Considérons $\delta' = \frac{|x|_p \varepsilon}{M}$ et $\delta = \min(|x|_p - \varepsilon, \delta')$,

alors en considérant $x' \in D$ tel que $|x' - x|_p < \delta$, et comme $\delta < |x|_p$, alors $|x'|_p = |x|_p$. On a dès lors :

$$\begin{aligned}
\left|f(x) - f(x')\right|_p &= \left|\sum_{n=0}^{+\infty}(a_n x^n - a_n x'^n)\right|_p \\
&\leq \max_n |a_n(x^n - x'^n)|_p \\
&= \max_n(|a_n|_p\,|x - x'|_p\left|x^{n-1} + x^{n-2}x' + \cdots + xx'^{n-2} + x'^{n-1}\right|_p) \\
&\leq \max_n(|a_n|_p\,|x - x'|_p\,|x|_p^{n-1}) \ \ (\text{car } |x|_p = |x'|_p) \\
&< \frac{\delta}{|x|_p}\max_n(|a_n x^n|_p) \\
&\leq \varepsilon
\end{aligned}$$

D'où la continuité de $f(X)$. ∎

1.3 Logarithme et exponentielle p-adique

1.3.1 Le logarithme p-adique

Revenons dans un premier temps sur l'exemple 1.10 pour lequel nous avons vu que le dique de convergence est $D(1^-)$. Cette série $\sum_{n=1}^{+\infty}\frac{(-1)^{n+1}}{n}X^n$ définit donc une fonction sur $D(1^-)$ à valeurs dans $\mathbb{C}_p$.

Définition 1.15. On appelle logarithme p-adique la fonction $\log_p(1+X)$ définit comme suit :

$$\log_p(1+X) : \left|\begin{array}{ccc} D(1^-) & \longrightarrow & \mathbb{C}_p \\ x & \longmapsto & \log_p(1+x) = \sum_{n=1}^{+\infty}\frac{(-1)^{n+1}}{n}x^n \end{array}\right.$$

Proposition 1.16. *Pour $(x, y) \in D(1^-)^2$, on a*

$$\log_p[(1+x)(1+y)] = \log_p(1+x) + \log_p(1+y)$$

Démonstration. Comme $x, y \in D(1^-)$, on a $(1+x)(1+y) = 1+(x+y+xy) \in 1+D(1^-)$, on peut donc bien donner un sens et définir :

$$\log_p[(1+x)(1+y)] = \sum_{n=1}^{+\infty}\frac{(-1)^{n+1}}{n}(x+y+xy)^n$$

On a de plus que sur $\mathbb{R}$, $\log[(1+x)(1+y)] = \log(1+x)+\log(1+y)$, donc en notant $F(X,Y) = \log[(1+X)(1+Y)] - \log(1+X) - \log(1+Y)$. F doit donc s'annuler sur $]-1,1[^2$, et donc tous les coefficients devant X^nY^m dans $F(X,Y)$ doivent s'annuler par la propositon 1.4. Cela nous assure que dans $\mathbb{Q}[[X,Y]]$, on a l'égalité :

$$\sum_{n=1}^{+\infty}\frac{(-1)^{n+1}}{n}X^n + \sum_{n=1}^{+\infty}\frac{(-1)^{n+1}}{n}Y^n = \sum_{n=1}^{+\infty}\frac{(-1)^{n+1}}{n}(X+Y+XY)^n$$

Or par la proposition 1.3, $\log_p[(1+x)(1+y)]$ peut être écrit comme $\sum_{m,n=0}^{+\infty} c_{m,n} x^n y^m$. Ainsi l'identité formelle dans $\mathbb{Q}[[X,Y]]$ nous assure que les nombres rationnels $c_{m,n}$ doivent s'annuler sauf si $n = 0$ ou $m = 0$ et dans ce cas : $c_{0,n} = c_{n,0} = \frac{(-1)^{n+1}}{n}$. En d'autre mots, on peut conclure que

$$\begin{aligned}\log_p[(1+x)(1+y)] &= \sum_{n=1}^{+\infty} \frac{(-1)^{n+1}}{n} x^n + \sum_{n=1}^{+\infty} \frac{(-1)^{n+1}}{n} y^n \\ &= \log_p(1+x) + \log_p(1+y)\end{aligned}$$

■

Lemme 1.17. *Soit ζ une racine p^m-ème primitive de l'unité, alors $|\zeta - 1|_p = p^{\frac{-1}{\varphi(p^m)}}$ où $\varphi(.)$ est la fonction indicatrice d'Euler.*

Démonstration. ζ est donc une racine du polynôme cyclotomique $\Phi_{p^m}(X)$.Or on sait que

$$\begin{aligned}\Phi_{p^m}(X) = \Phi_p(X^{p^{m-1}}) &= \frac{X^{p^m} - 1}{X^{p^{m-1}} - 1} \\ &= 1 + X^{p^{m-1}} + \cdots + X^{(p-1)p^{m-1}} \\ &= \prod_{\substack{1 \le j \le p^m - 1 \\ p \nmid j}} (X - \zeta^j)\end{aligned}$$

Alors on obtient en substituant $X = 1$ dans la dernière égalité que

$$p \overset{(*)}{=} \prod_{\substack{1 \le j \le p^m - 1 \\ p \nmid j}} (1 - \zeta^j)$$

Mais on a d'autre part que $\zeta = 1 \mod p$ et que pour tout $j \in \mathbb{N}$,

$$\frac{1-\zeta^j}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{j-1} = j \mod p$$

Ainsi si $1 \le j \le p^m - 1$ et $p \nmid j$, alors $\frac{1-\zeta^j}{1-\zeta} = 1 \mod p$ et donc $\left|1 - \zeta^j\right|_p = |1 - \zeta|_p$.

Ainsi en prenant la norme dans $(*)$, on obtient que $\frac{1}{p} = |1-\zeta|_p^{\varphi(p^m)}$ et donc $\zeta - 1 = p^{\frac{-1}{\varphi(p^m)}}$ ■

Corollaire 1.18. *Si $1 + x$ est une racine p^m-ème de l'unité alors $\log_p(1+x) = 0$*

Démonstration. Si $1+x$ est une racine p^m-ème de l'unité, alors par le lemme précédent $|x|_p < 1$, et on peut donc bien s'intéresser à $\log_p(1+x)$. Or, par la proposition précédente, $p^m \log_p(1+x) = \log_p[(1+x)^{p^m}] = \log_p(1) = 0$. Ainsi $\log_p(1+x) = 0$ ■

Après avoir défini l'équivalent du logarithme réel, on peut se demander si l'exponentielle peut-être de la même façon définie.

1.3.2 L'exponentielle p-adique

Avant de s'intéresser à l'exponentielle comme la série $\sum_{n=0}^{+\infty} \frac{X^n}{n!}$, nous allons nous intéresser au coefficient $n!$ de cette dite série.

Lemme 1.19. *Soit n un entier et $p \geq 2$ un nombre premier, alors :*

$$\mathrm{ord_p}(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Démonstration. Les multiples de p^k dans $\{1, \ldots, n\}$ sont au nombre de $\left\lfloor \frac{n}{p^k} \right\rfloor$. Ainsi, parmi les entiers de $\{1, \ldots, n\}$, ceux de valuation p-adique exactement k sont au nombre de $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$. On remarque de plus que pour $m > \log_p(n)$, $\left\lfloor \frac{n}{p^m} \right\rfloor = 0$. Ainsi :

$$\begin{aligned}
\mathrm{ord_p}(n!) &= \mathrm{ord_p}\left(\prod_{k=1}^{n} k\right) \\
&= \sum_{k=1}^{n} \mathrm{ord_p}(k) \\
&= \sum_{k=1}^{m} k \,\mathrm{Card}(\{j \in \{1, \ldots, n\}, \mathrm{ord_p}(j) = k\}) \\
&= \sum_{k=1}^{m} k \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) \\
&= \sum_{k=1}^{m} \left\lfloor \frac{n}{p^k} \right\rfloor \quad \text{(Après simplification par télescopage)} \\
&= \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor
\end{aligned}$$

■

Lemme 1.20. *Soit n un entier et $p \geq 2$ un nombre premier, alors, en notant S_n la somme des chiffres de n en base p, on a :*

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

Démonstration. On écrit la décomposition de n en base p :

$$n = \sum_{j=0}^{+\infty} n_j p^j \text{ où } n_j = 0 \text{ pour } j > \log_p n$$

Alors,

$$\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k \geq 1} \sum_{j \geq k} n_j p^{j-k}$$

$$\begin{aligned}
\sum_{k\geq 1}\left\lfloor \frac{n}{p^k}\right\rfloor &= \sum_{j\geq 1} n_j \sum_{k=1}^{j} p^{j-k} \\
&= \sum_{j\geq 1} n_j p^j \times \sum_{k=1}^{j}\left(\frac{1}{p}\right)^k \\
&= \sum_{j\geq 1} n_j p^j \times \frac{p^j-1}{p-1} \\
&= \frac{1}{p-1}\left(\sum_{j\geq 1} n_j p^j - \sum_{j\geq 1} n_j\right) \\
&= \frac{1}{p-1}((n-n_0)-(S_n-n_0)) \\
&= \frac{n-S_n}{p-1}
\end{aligned}$$

d'où l'égalité recherchée en utilisant le lemme 1.19. ∎

Proposition 1.21. *Le rayon de convergence r de la série $\sum_{n=0}^{+\infty}\frac{X^n}{n!}$ est $p^{-1/(p-1)}$.*

Démonstration. Par le lemme 1.20, nous avons obtenu $\left|\frac{1}{n!}\right|_p = p^{\frac{n-S_n}{p-1}}$. En utilisant alors la formule du rayon de convergence $r = \frac{1}{\limsup|a_n|_p^{1/n}}$, on tire tout d'abord que $r = \frac{1}{\limsup p^{\frac{n-S_n}{n(p-1)}}}$ et donc que

$$\mathrm{ord_p}(r) = \liminf\left(-\frac{n-S_n}{n(p-1)}\right)$$

Mais, on a $\lim_{n\to+\infty} -\left(\frac{n-S_n}{n(p-1)}\right) = -\frac{1}{p-1}$, ce qui nous donne bien le résultat. ∎

Remarque 1.22. On a vu la convergence de la série $\sum_{n=0}^{+\infty}\frac{x^n}{n!}$ pout $|x|_p < p^{-1/(p-1)}$ et la divergence pour $|x|_p > p^{-1/(p-1)}$. Mais qu'en est-il pour $|x|_p = p^{-1/(p-1)}$? Dans cette situation, on a :

$$\mathrm{ord_p}(a_n x^n) = -\frac{n-S_n}{p-1} + \frac{n}{p-1} = \frac{S_n}{p-1}$$

Or en considérant $n = p^m$ pour un certain $m \in \mathbb{N}$, alors $\mathrm{ord_p}(a_{p^m}x^{p^m}) = \frac{1}{p-1}$ car $S_{p^m} = 1$. Ainsi $\left|a_{p^m}x^{p^m}\right|_p = p^{-1/(p-1)} \nrightarrow 0$. Ainsi, le disque de convergence est ouvert.

Définition 1.23. On appelle Exponentielle p-adique la fonction $\exp_p(X)$ définit comme suit :

$$\exp_p(X) : \left|\begin{array}{ccc} D(p^{-1/(p-1)^-}) & \longrightarrow & \mathbb{C}_p \\ x & \longmapsto & \exp_p(x) = \sum_{n=0}^{+\infty}\frac{x^n}{n!} \end{array}\right.$$

Remarque 1.24.

* Comme $D(p^{-1/(p-1)^-}) \subset D(1^-)$, on obtient que $\exp_p$ converge sur un disque plus petit que $\log_p$.

* On remarque que le disque de convergence de l'exponentielle p-adique est beaucoup plus petit que celui de l'exponentielle réelle/complexe.

Proposition 1.25. *Si* $(x, y) \in D(p^{-1/(p-1)^-})^2$, *on a* $\exp_p(x+y) = \exp_p(x)\exp_p(y)$.

Démonstration. Si $(x, y) \in D(p^{-1/(p-1)^-})^2$, alors on a tout d'abord par non-archimédiannité de $|.|_p$, $x + y \in D(p^{-1/(p-1)})$. On peut ainsi bien définir $\exp_p(x+y)$. Comme pour le $\log_p$, on a sur $\mathbb{Q}[[X, Y]]$ que

$$\begin{aligned}\exp(X+Y) &= \sum_{n=0}^{+\infty} \frac{(X+Y)^n}{n!} \\ &= \sum_{n=0}^{+\infty} \frac{X^n}{n!} \times \sum_{n=0}^{+\infty} \frac{Y^n}{n!}\end{aligned}$$

provenant de l'égalité sur $\mathbb{R}$ de $\exp(x+y) = \exp(x)\exp(y)$.

Or par la propostion 1.3, $\exp_p(x+y)$ peut être écrit : $\sum_{m,n=0}^{+\infty} c_{m,n} x^n y^m$. Mais l'identité formelle dans $\mathbb{Q}[[X, Y]]$, nous assure que $c_{m,n} = \frac{1}{n!m!}$. En d'autres mots, on peut conclure que

$$\begin{aligned}\exp_p(x+y) &= \sum_{n=0}^{+\infty} \frac{x^n}{n!} \times \sum_{n=0}^{+\infty} \frac{y^n}{n!} \\ &= \exp_p(x)\exp_p(y)\end{aligned}$$

■

1.3.3 Exponentielle et Logarithme p-adique comme réciproque l'un de l'autre

Proposition 1.26.

1. *Pour* $x \in D(p^{-1/(p-1)^-})$, $\log_p(\exp_p(x)) = x$
2. *Pour* $x \in D(p^{-1/(p-1)^-})$, $\exp_p(\log_p(1+x)) = 1+x$

Démonstration.

1. Si $x \in D(p^{-1/(p-1)^-})$, on peut donc considérer $\exp_p(x) = 1 + \sum_{n\geq 1} \frac{x^n}{n!}$. On a aussi

$$\mathrm{ord_p}\left(\frac{x^n}{n!}\right) > \frac{n}{p-1} - \frac{(n-S_n)}{p-1} = \frac{S_n}{p-1} > 0$$

Ainsi, on en déduit que $\exp_p(x)-1 \in D(1^-)$. On peut donc bien définir l'élément $\log_p(1+\exp_p(x)-1)$. Or, on a aussi

$$\begin{aligned}\log_p(1+\exp_p(x)-1) &= \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{(\exp_p(x)-1)^n}{n} \\ &= \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{\left(\sum_{m=1}^{+\infty} \frac{x^m}{m!}\right)^n}{n}\end{aligned}$$

Or par la proposition 1.3, la série peut être mise sous la forme $\sum_{n=1}^{+\infty} c_n x^n$. Comme précédemment pour $\log_p$ et $\exp_p$, on a l'identité formelle suivante sur $\mathbb{Q}[[X]]$:

$$\sum_{n=1}^{+\infty}(-1)^{n+1}\frac{\left(\sum_{m=1}^{+\infty}\frac{X^m}{m!}\right)^n}{n} = X$$

provenant de l'égalité $\log(\exp(x)) = x$ sur $\mathbb{R}$. Ansi, on tire que les coefficients sont : $c_1 = 1, c_n = 0$ pour $n > 1$. On peut donc bien écrire :

$$\log_p(1 + \exp_p(x) - 1) = \log_p(\exp_p(x)) = x \text{ pour } x \in D(p^{-1/(p-1)^-})$$

2. Si $x \in D(p^{-1/(p-1)^-})$, alors pour $n \geq 1$:

$$\mathrm{ord_p}\left(\frac{x^n}{n}\right) - \frac{1}{p-1} > \frac{n}{p-1} - \mathrm{ord_p}(n) - \frac{1}{p-1} = \frac{n-1}{p-1} - \mathrm{ord_p}(n)$$

L'expression $\frac{n-1}{p-1} - \mathrm{ord_p}(n)$ atteint son minimum en $n = 1$ et $n = p$ pour laquelle elle vaut 0. D'où, $\mathrm{ord_p}(\log_p(1 + x)) \geq \min_{n\geq 1} \mathrm{ord_p}\left(\frac{x^n}{n}\right) > \frac{1}{p-1}$. On a donc bien le droit de prendre l'exponentielle p-adique de $\log_p(1 + x)$. Or comme précédemment,

$$\begin{aligned}\exp_p(\log_p(1+x)) &= \sum_{n=0}^{+\infty}\frac{\log_p(1+x)^n}{n!} \\ &= \sum_{n=0}^{+\infty}\frac{\left(\sum_{n=1}^{+\infty}(-1)^{n+1}\frac{x^n}{n}\right)^n}{n!}\end{aligned}$$

Or cette serie peut être mis sous la forme $\sum_{n=1}^{+\infty} c_n x^n$ par la proposition 1.3 et on a l'identité formelle sur $\mathbb{Q}[[X]]$:

$$\sum_{n=0}^{+\infty}\frac{\left(\sum_{n=1}^{+\infty}(-1)^{n+1}\frac{X^n}{n}\right)^n}{n!} = 1 + X$$

provenant de $\exp(\log(1 + x)) = x$ sur $\mathbb{R}$. On en déduit que $c_0 = c_1 = 1$ et que $c_n = 0$ pour $n \geq 2$. Ainsi :

$$\exp_p(\log_p(1 + x)) = 1 + x \text{ pour } x \in D(p^{-1/(p-1)^-})$$

■

Des différentes propositions précédentes (morphismes et ci-dessus), on peut en déduire le théorème suivant :

Théorème 1.27. *Les fonctions* $\log_p$ *and* $\exp_p$ *sont des isomorphismes inverses entre le groupe multiplicatif* $D(1, p^{-1/(p-1)^-})$ *et le groupe additif* $D(p^{-1/(p-1)^-})$.

1.4 Lemme de Dwork

On termine ce chapitre par une section démontrant un lemme de Dwork, qui nous permettra par la suite de construire une série entière p-adique qui aura toute son importance dans le chapitre 3 lors de la discussion de la preuve du théorème de Dwork.

Remarque 1.28. On commence par rappeller qu'une série formelle est inversible si et seulement si son coefficient constant est inversible dans l'anneau considéré.

Lemme 1.29 (Dwork)**.** *Soit* $F(X) = 1 + \sum_{n=1}^{+\infty} a_n X^n \in 1 + X\mathbb{Q}_p[X]$. *Alors* $F(X) \in 1 + X\mathbb{Z}_p[[X]]$ *si et seulement si* $\frac{F(X^p)}{F(X)^p} \in 1 + pX\mathbb{Z}_p[[X]]$.

Démonstration.

* Si $F(X) \in 1 + X\mathbb{Z}_p[[X]]$, alors comme $(a+b)^p = a^p + b^p \mod [p]$ et $a^p = a \mod [p]$ pour $a \in \mathbb{Z}_p$, on obtient qu'il existe $G(X) \in X\mathbb{Z}_p[[X]]$ tel que $F(X)^p = F(X^p) + pG(X)$. Ainsi, $F(X)^p \in 1 + X\mathbb{Z}_p[[X]]$ et donc $F(X)^p$ est inversible par la remarque précédente et on a

$$\frac{F(X^p)}{F(X)^p} = 1 - \frac{pG(X)}{F(X)^p} \in 1 + pX\mathbb{Z}_p[[X]]$$

* Si $F(X^p) = F(X)^p G(X)$ avec $G(X) \in 1 + pX\mathbb{Z}_p[[X]]$, alors notons $F(X) = \sum_{i=0}^{+\infty} a_i X^i$ et $G(X) = \sum_{i=0}^{+\infty} b_i X^i$. On doit montrer que les a_i sont dans $\mathbb{Z}_p$. Faisons cela par récurrence :

$\underline{n = 0}$: Par hypothèse $a_0 = 1 \in \mathbb{Z}_p$

$\underline{i < n}$: On suppose que les coefficients a_i, pour $i < n$ sont dans $\mathbb{Z}_p$. On regarde les coefficients de chaque coté de l'égalité supposée :
Pour le terme de gauche, on voit que si $p|n$ le coefficient devant X^n est $a_{n/p}$, sinon celui-ci vaut 0. Pour le terme de droite, développons :

$$\left(\sum_{i=0}^{n} a_i X^i\right)^p \left(1 + \sum_{i=1}^{n} b_i X^i\right) = \underbrace{\left(\sum_{i=0}^{n} a_i X^i\right)^p}_{A} + \underbrace{\left(\sum_{i=0}^{n} a_i X^i\right)^p}_{B} \underbrace{\left(\sum_{i=1}^{n} b_i X^i\right)}_{C}$$

Alors en considérant modulo p, on obtient que

$$\left(\sum_{i=0}^{n} a_i X^i\right)^p = \sum_{i=0}^{n} a_i^p X^{ip} \mod [p] = \sum_{i=0}^{n} a_i X^{ip} \mod [p]$$

Son unique coefficient contribuant au terme X^n qui n'est pas égale à 0 modulo p est donc $a_{n/p}$ dans le cas où $p|n$. On peut alors soustraire de chaque côté de l'égalité les coefficients $a_{n/p}$ de l'égalité. On voit donc que tous les autres termes possibles contribuant au coefficient X^n dans A sont des éléments de $p\mathbb{Z}_p$. Maintenant, on peut donc voir que le coefficient devant X^n dans A est de la forme $pa_n + \alpha$ où $\alpha \in p\mathbb{Z}_p$ car α est une somme de produits de a_i pour $i < n$ qui sont par hypothèse des éléments de $\mathbb{Z}_p$ et pour lesquels nous avons vu qu'ils congruent à 0 modulo p.

Le coefficient de X^n dans la série entière représentée par BC est un élément de $p\mathbb{Z}_p$. En effet, chaque b_i est un élément de $p\mathbb{Z}_p$ et les seuls termes de B qui contribuent sont similaires à ce qui précède, et sont donc aussi dans $p\mathbb{Z}_p$. En réarrangeant, on obtient donc que $pa_n \in p\mathbb{Z}_p$ donc $a_n \in \mathbb{Z}_p$.

■

Remarque 1.30. Il est possible de généraliser le lemme précédent comme suit :

Soit $F(X,Y) = \sum a_{m,n} X^n Y^m \in 1 + X\mathbb{Q}_p[[X,Y]] + Y\mathbb{Q}_p[[X,Y]]$. Alors tous les $a_{m,n}$ sont dans $\mathbb{Z}_p$ si et seulement si

$$\frac{F(X^p, Y^p)}{F(X,Y)^p} \in 1 + pX\mathbb{Z}_p[[X,Y]] + pY\mathbb{Z}_p[[X,Y]]$$

On va maintenant utiliser le lemme de Dwork pour montrer qu'une certaine série entière, que l'on utilisera plus tard, est à coefficients entiers.

Proposition 1.31. *Considérons $F(X,Y) \in \mathbb{Q}_p[[X,Y]]$ définie par :*

$$\begin{aligned} F(X,Y) &= B_{X,p}(Y) B_{(X^p-X)/p}(Y^p) B_{(X^{p^2}-X^p)/p^2} \cdots B_{(X^{p^n}-X^{p^{n-1}})/p^n} \cdots \\ &:= (1+Y)^X (1+Y^p)^{(X^p-X)/p} (1+Y^{p^2})^{(X^{p^2}-X^p)/p^2} \cdots \end{aligned}$$

Alors $F(X,Y) \in \mathbb{Z}_p[[X,Y]]$

Démonstration. On commence dans un premier temps par montrer que $F(X,Y)$ définie bien un élément de $1 + X\mathbb{Q}_p[[X,Y]] + Y\mathbb{Q}_p[[X,Y]]$. On part du développement du binome :

$$\begin{aligned} F(X,Y) = &\left(\sum_{i=0}^{+\infty} \frac{X(X-1)\cdots(X-i+1)}{i!} Y^i \right) \times \\ &\prod_{n=1}^{+\infty} \left(\sum_{i=0}^{+\infty} \frac{X^{p^n} - X^{p^{n-1}}}{p^n} \left(\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - 1 \right) \cdots \left(\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - i + 1 \right) \frac{Y^{ip^n}}{i!} \right) \end{aligned}$$

Chaque coefficient devant $X^n Y^m$ provient d'un nombre fini de termes du produit infini. De plus, on obtient de l'écriture de la proposition, que $a_{0,0} = 1$ et donc que $F(X,Y) \in 1 + X\mathbb{Q}_p[[X,Y]] + Y\mathbb{Q}_p[[X,Y]]$. Or, on a

$$\begin{aligned} \frac{F(X^p, Y^p)}{F(X,Y)^p} &= \frac{(1+Y^p)^{X^p} (1+Y^{p^2})^{(X^{p^2}-X^p)/p} (1+Y^{p^3})^{(X^{p^3}-X^{p^2})/p^2} \cdots}{(1+Y)^{pX} (1+Y^p)^{X^p - X} (1+Y^{p^2})^{(X^{p^2}-X^p)/p} \cdots} \\ &= \frac{(1+Y^p)^X}{(1+Y)^{pX}} \end{aligned}$$

Or, en appliquant le lemme de Dwork 1.29 à $1 + Y \in 1 + Y\mathbb{Z}_p[[Y]]$, on en déduit qu'il existe $G(Y) \in \mathbb{Z}_p[[Y]]$ tel que

$$\frac{(1+Y^p)}{(1+Y)^p} = 1 + pYG(Y)$$

Alors

$$\frac{(1+Y^p)^X}{(1+Y)^{pX}} = (1 + pYG(Y))^X = \sum_{i=0}^{+\infty} \frac{X(X-1)\cdots(X-i+1)}{i!} p^i (YG(Y))^i$$

Cette dernière quantité est dans $1+pX\mathbb{Z}_p[[X,Y]]+pY\mathbb{Z}_p[[X,Y]]$, et donc le lemme de Dwork généralisé 1.30, nous permet donc de conclure que $F(X,Y) \in \mathbb{Z}_p[[X,Y]]$. ■

Chapitre 2

Les Polygones de Newton

2.1 Polygones de Newton pour les polynômes

Soit $f(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\mathbb{C}_p[X]$ un polynôme de degré n à coefficients dans $\mathbb{C}_p$ de terme constant 1. On considère la suite de points dans le plan réel :

$$(0,0), (1, \mathrm{ord_p}(a_1)), (2, \mathrm{ord_p}(a_2)), \ \dots\ , (i, \mathrm{ord_p}(a_i))\ \dots\ , (n, \mathrm{ord_p}(a_n))$$

(Si $a_i = 0$, on omettra le point.)

Définition 2.1. On appelle Polygone de Newton de $f(X)$ l'enveloppe convexe supérieur de cet ensemble de points. (*i.e.* la ligne polygonale connexe la plus élevée joignant $(0,0)$ à $(n, \mathrm{ord_p}(a_n))$ qui passe par ou en dessous de tout les points $(i, \mathrm{ord_p}(a_i))$).

Remarque 2.2. Comment construire le polygone de Newton d'un polynôme $f(X)$?

1. On considère la droite verticale passant par $(0,0)$.
2. On fait tourner cette droite autour de $(0,0)$ dans le sens anti-horaire jusqu'à ce que la droite rencontre un point $(i_1, \mathrm{ord_p}(a_{i_1}))$.
3. Le premier segment du Polygone de Newton de $f(X)$ est donc le segment joignant $(0,0)$ à $(i_1, \mathrm{ord_p}(a_{i_1}))$.
4. On continue à faire tourner la droite initialement verticale jusqu'à rencontrer un point $(i_2, \mathrm{ord_p}(a_{i_2}))$ $(i_2 > i_1)$.
5. Le segment joignant $(i_1, \mathrm{ord_p}(a_{i_1}))$ à $(i_2, \mathrm{ord_p}(a_{i_2}))$ est le deuxième segment du Polygone de Newton.
6. On continue jusqu'à atteindre le dernier point $(n, \mathrm{ord_p}(a_n))$.

Exemple 2.3.

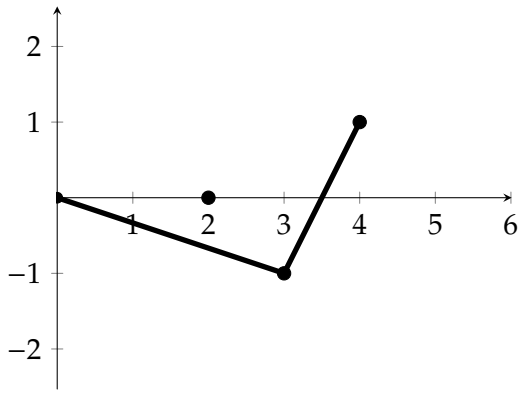


FIGURE 2.1 – Polygone de Newton de $f(X) = 1 + X^2 + \frac{1}{3}X^3 + 3X^4 \in \mathbb{Q}_3[X]$

Définition 2.4.

— Si un segment joint les points (i, m) à (i', m'), on appelle pente du segment la quantité $\frac{i'-i}{m'-m}$.

— On appelle longueur de la pente, la quantité $i'-i$ (*i.e.* la longueur de la projection du segment correspondant sur l'axe horizontal).

— On appelle sommets du Polygone de Newton les points $(i_j, \mathrm{ord}_\mathrm{p}(a_{i_j}))$ où la pente change.

Lemme 2.5. *Si on considère $f(X) = (1 - \frac{X}{\alpha_1}) \cdots (1 - \frac{X}{\alpha_n})$ la factorisation de $f(X)$ avec ses racines $\alpha_i \in \mathbb{C}_p$, et que l'on note $\lambda_i = -\mathrm{ord}_\mathrm{p}(\alpha_i)$. Alors si λ est une pente du Polygone de Newton de longueur ℓ. Alors, il existe un ensemble $S \subseteq \{1, \ldots, n\}$ de cardinal ℓ tel que $\lambda_j = \lambda$ pour tout $j \in S$.*

Démonstration. Sans perte de généralité, on peut écrire

$$f(X) = \prod_{i=1}^{n} \left(1 - \frac{X}{\alpha_i}\right)$$

avec les α_i rangées de tel sorte que $\lambda_i = -\mathrm{ord}_\mathrm{p}(\alpha_i)$ soient ordonnées. Notons r le plus petit entier tel que $\lambda_1 = \lambda_2 = \cdots = \lambda_r < \lambda_{r+1}$ et montrons que le premier segment du Polygone de Newton de $f(X)$ est le segment joignant $(0, 0)$ à $(r, r\lambda_1)$. On commence par remarquer que pour tout $i \in \{1, \ldots, n\}$, on a :

$$a_i = \sum_{\substack{J \in \mathcal{P}(\{1,\ldots,n\}) \\ |J|=i}} \prod_{j \in J} \frac{1}{\alpha_j}$$

et on a pour un tel J

$$\mathrm{ord}_\mathrm{p}\left(\prod_{j \in J} \frac{1}{\alpha_j}\right) \geq i\lambda_1$$

d'où le fait qu'on ait $\mathrm{ord}_\mathrm{p}(a_i) \geq i\lambda_1$. Or on sait aussi que :

$$\mathrm{ord}_\mathrm{p}(a_i) \geq i\lambda_1 \iff \underbrace{\frac{\mathrm{ord}_\mathrm{p}(a_i)}{i}}_{\substack{\text{pente du segment} \\ (0,0)\text{->}(i,\mathrm{ord}_\mathrm{p}(a_i))}} \geq \underbrace{\lambda_1}_{\substack{\text{pente du segment} \\ (0,0)\text{->}(r,r\lambda_1)}}$$

Donc les points $(i, \mathrm{ord}_\mathrm{p}(a_i))$ se trouve être sur ou au dessus du segment joignant $(0, 0)$ à $(r, \lambda_1 r)$. Il nous suffit donc de montrer que ce segment est atteint au point $(r, \mathrm{ord}_\mathrm{p}(a_r))$ et qu'au dessus cela n'est pas lieu pour obtenir le premier segment de notre polygone de Newton.

En considérant $a_r = \sum_{\substack{J \in \mathcal{P}(\{1,\ldots,n\}) \\ |J|=r}} \prod_{j \in J} \frac{1}{\alpha_j}$. Dans cette somme, on a le terme $\frac{1}{\alpha_1 \ldots \alpha_r}$ qui est de plus petite valuation $r\lambda_1$, on obtient ainsi que $\mathrm{ord}_\mathrm{p}(a_r) = r\lambda_1$. Si on considère maintenant $i > r$, de la même façon que précédemment que $\mathrm{ord}_\mathrm{p}(a_i) > i\lambda_1$ d'où le résultat souhaité.

De la même façon, on montre que si on a $\lambda_s < \lambda_{s+1} = \cdots = \lambda_{s+r} < \lambda_{s+r+1}$, alors le segment joignant $(s, \lambda_1 + \lambda_2 + \cdots + \lambda_s)$ à $(s + r, \lambda_1 + \lambda_2 + \cdots + \lambda_s + r\lambda_{s+1})$ est un segment du polygone de Newton de $f(X)$. Dire que ce segment est un segment

polygone de Newton de $f(X)$ est équivalent à dire que pour $i \in \{s+1, \cdots, s+r\}$, les points $(i, \mathrm{ord_p}(i))$ sont au dessus ou sur la ligne de pente λ_{s+1}. Or cela équivaut à dire que $i \in \{s+1, \cdots, s+r\}$, la pente de la ligne joignant $(s, \lambda_1 + \cdots + \lambda_s)$ à $(i, \mathrm{ord_p}(a_i))$ est supérieur à la pente de la ligne joignant $(s, \lambda_1 + \cdots + \lambda_s)$ à $(s+r, \lambda_1 + \cdots + \lambda_s + r\lambda_{s+1})$ *i.e.*

$$\frac{\mathrm{ord_p}(a_i) - \lambda_1 - \cdots - \lambda_s}{i - s} \geq \lambda_{s+1}$$

i.e.

$$\mathrm{ord_p}(a_i) \geq \lambda_1 + \cdots + \lambda_s + (i-s)\lambda_{s+1}$$

Vérifions que l'on ait bien cette condition. Si on considère $a_i = \sum_{\substack{\Theta \in \{1,\cdots,n\} \\ |\Theta| = i}} \prod_{j \in \Theta} \frac{1}{\alpha_j}$.

Comme $\mathrm{ord_p}\left(\prod_{j\in\Theta} \frac{1}{\alpha_j}\right) \geq \lambda_1 + \cdots + \lambda_s + (i-s)\lambda_{s+1}$, alors $\mathrm{ord_p}(a_i) \geq \lambda_1 + \cdots + \lambda_s + (i-s)\lambda_{s+1}$, la condition est donc bien vérifiée.

Il nous suffit donc de montrer que ce segment est atteint au point $(r+s, \mathrm{ord_p}(a_{r+s}))$ et qu'au dessus cela n'est pas lieu pour obtenir le premier segment de notre polygone de Newton. En considérant $a_{r+s} = \sum_{\substack{\kappa \in \mathcal{P}(\{1,\ldots,n\}) \\ |J| = r+s}} \prod_{j\in\kappa} \frac{1}{\alpha_j}$. Dans cette somme, on a le terme $\frac{1}{\alpha_1 \ldots \alpha_s} \times \frac{1}{\alpha_{s+1} \cdots \alpha_{s+r}}$ qui est de plus petite valuation $(i-s)\lambda_{s+1} + \lambda_1 + \cdots + \lambda_s$, on obtient ainsi que $\mathrm{ord_p}(a_{r+s}) = (i-s)\lambda_{s+1} + \lambda_1 + \cdots + \lambda_s$. Ainsi par construction, c'est bien un segment du polygone de Newton de $f(X)$. ∎

2.2 Les Polygones de Newton pour les séries entières

Considérons maintenant $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ une série entière. On définit $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\mathbb{C}_p[X]$ comme la n-ème somme partielle de $f(X)$. On supposera dans toute cette section que $f(X)$ n'est pas un polynôme.

Définition 2.6. On définit le Polygone de Newton de $f(X)$ comme la limite des polygones de Newton de $f_n(X)$.

Remarque 2.7. Il faut prendre quelques précautions supplémentaire dans la construction par rapport à celle des pôlynômes. En effet, étudions quelques cas particuliers :

1. On peut avoir un nombre infini de segments de longueurs finis.

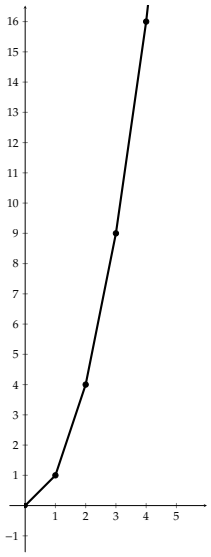


FIGURE 2.2 – Polygone de Newton de $f(X) = 1 + \sum_{i=1}^{+\infty} p^{i^2} X^i \in \mathbb{Q}_p[X]$

2. À un certain moment, la droite que l'on fait tourner peut atteindre simultanément des points $(i, \mathrm{ord_p}(a_i))$ loin. Dans ce cas, le polygone de Newton a un nombre fini de segments, le dernier étant infiniement long.

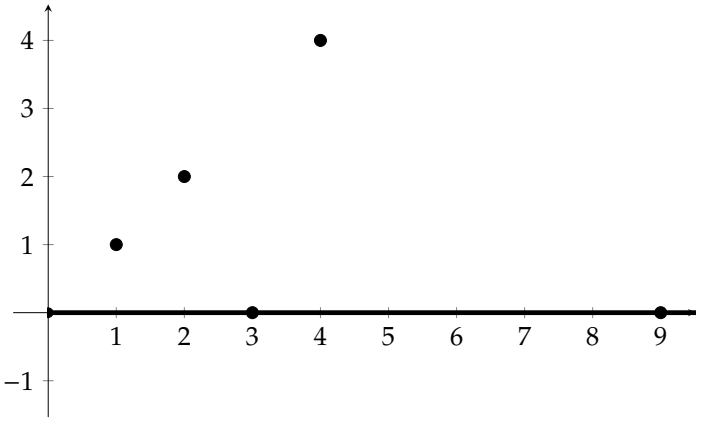


FIGURE 2.3 – Polygone de Newton de $f(X) = \sum_{i=0}^{+\infty} ((3X)^i + X^{3^i}) \in \mathbb{Q}_3[X]$

3. À un moment donné, la droite que l'on fait tourner n'a atteint aucun des points $(i, \mathrm{ord_p}(a_i))$ plus loin, mai si l'on continue plus loin elle passerait ces points. Quand cela arrive, on définit le dernier segment du polygone de newton comme étant celui de pente la borne supérieure des pentes passant en dessous des points.

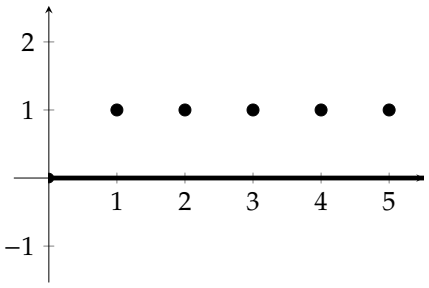


FIGURE 2.4 – Polygone de Newton de $f(X) = 1 + \sum_{i=1}^{+\infty} pX^i \in \mathbb{Q}_p[X]$

Dans cet exemple, quand la droite passe l'axe horizontal, elle ne peut pas tourner plus sans passer de points, la pente est donc de 0.

4. Un cas dégénéré du précédent est quand la droite ne peut pas être tournée de son axe vertical, ce cas correspond à avoir un rayon de convergence nul (cas qu'on exclura pour la suite).

On a vu dans le cas des polynômes que le polygone de Newton est utile car il ne permet de voir à quel rayon (pour la norme p-adique) les racines sont situées. Avant de s'intéresser au cas des séries entières, regardons un exemple.

Exemple 2.8. On s'intéresse à

$$f(X) = 1 + \frac{X}{2} + \frac{X^2}{3} + \cdots + \frac{X^i}{i+1} + \cdots = -\frac{1}{X}\log_p(1-X)$$

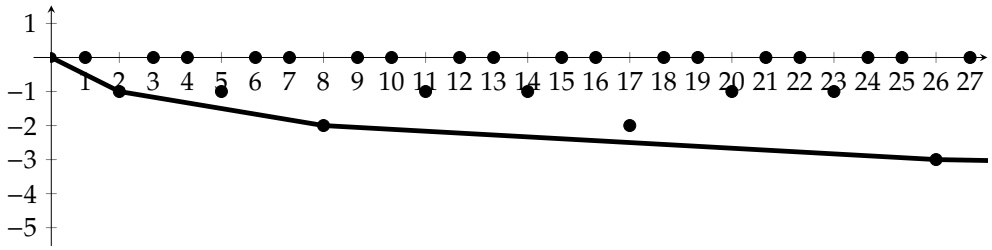


FIGURE 2.5 – Polygone de Newton de $f(X) = -\frac{1}{X}\log_3(1-X) \in \mathbb{Q}_3[X]$

Le polygone de Newton de $f(X)$ est la ligne polygonale joignant les points $(0,0), (p-1,-1), (p^2-1,-2), \ldots, (p^j-1,-j), \ldots$ On est donc dans le cas 1. de la remarque précédente. Si le lemme 2.5 reste valide pour les séries entières, on s'attend à avoir $p^{j+1} - p^j$ racines de valuation p-adique $\frac{1}{p^{j+1}-p^j}$.

Intéressons nous donc aux racines de $\frac{-1}{X}\log_p(1+X)$? On sait que si $x = 1-\zeta$ où ζ est une racine p^{j+1}-ème primitive de l'unité. Par le lemme 1.17 et le corollaire 1.18, on sait que $\mathrm{ord_p}(x) = \frac{1}{p^{j+1}-p^j}$ et que $\log_p(1-x) = \log_p(\zeta) = 0$. Or il y a $p^{j+1} - p^j$ racines p^{j+1}-ème primitive de l'unité, ce qui nous donne bien celles prédites. Y'a-t-il d'autres racines de $f(X)$ dans $D(1^-)$?

Si $x \in D(1^-)$ est une racine de $f(X)$, alors pour tout j, $x_j = 1-(1-x)^{p^j} \in D(1^-)$ est aussi une racine de $f(X)$ car $\log_p(1-x_j) = p^j \log_p(1-x) = 0$. Alors pour j suffisament grand, on a $x_j \in D(p^{-1/(p-1)\ -})$ et donc $1 - x_j = \exp_p(\log_p(1-x_j)) = \exp_p(0) = 1$, ce

qui revient à dire que $(1-x)^{p^j} = 1$ et donc x fait partie des racines prédites. Il semble que le lemme 2.5 persiste dans ce cas présent.

Nous allons le démontrer pour tout $f(X) \in 1 + X\mathbb{C}_p[[X]]$. Pour se faire, nous allons démontrer un ensemble de lemmes qui serviront à démontrer le théorème de préparation de Weierstrass p-adique. Dès lors, le résultat en sera un corollaire immédiat.

Lemme 2.9. *Soit b la borne supérieure des pentes du polygone de Newton de $f(X)$ définie par $1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + \mathbb{C}_p[[X]]$. Alors le rayon de convergence de $f(X)$ est p^b. (b peut être infini, dès lors $f(X)$ converge sur tout $\mathbb{C}_p$).*

Démonstration.

* Soit x tel que $|x|_p < p^b$, *i.e.* $\mathrm{ord_p}(x) > -b$. Dison que $\mathrm{ord_p}(x) = b'$ avec $b' < b$. Alors $\mathrm{ord_p}(a_i x^i) = \mathrm{ord_p}(a_i) - ib'$. Comme $b' < b$ et que b est la borne supérieur des pentes. Cela nous assure que pour i suffisament grand, $(i, \mathrm{ord_p}(a_i))$ se trouve aussi loin au dessus de $(i, b'i)$. Ainsi $\mathrm{ord_p}(a_i x^i) \to +\infty$ donc $\left|a_i x^i\right|_p \to 0$ et donc $f(X)$ converge pour $X = x$.
* Soit x tel que $|x|_p > p^b$, *i.e.* $\mathrm{ord_p}(x) = -b' < -b$, *i.e.* $b' > b$. Alors, comme $b' > b$ qui est la borne supérieur des pentes, il existe une infinité de i tel que $(i, \mathrm{ord_p}(a_i))$ soit sous $(i, b'i)$. Ainsi $\mathrm{ord_p}(a_i x^i) = \mathrm{ord_p}(a_i) - ib'$ est négatif pour une infinité de valeurs de i et donc $\left|a_i x^i\right|_p > 1$ pour un nombre infini de i et donc $f(x)$ ne converge pas.

Ainsi le rayon de convergence de $f(X)$ est p^b. ∎

Remarque 2.10. Si $c \in \mathbb{C}_p$ tel que $\mathrm{ord_p}(c) = \lambda$ et que l'on considère $g(X) = f\left(\frac{X}{c}\right)$. En notant $f(X) = 1 + \sum_i a_i X^i$ et $g(X) = 1 + \sum_i b_i X^i$, alors $\mathrm{ord_p}(b_i) = \mathrm{ord_p}(a_i) - \lambda i$. Cela nous assure que le polygone de Newton de g est obtenu via celui de f en soustrayant la droite $y = \lambda x$ passant par $(0,0)$ de pente λ.

Exemple 2.11. En reprenant l'exemple 2.3. On considère $c = 9 \in \mathbb{C}_p$, pour $p = 3$, on a $\mathrm{ord_p}(c) = 2$. Considérons $g(X) = f(X/9)$ où $f(X) = 1 + X^2 + \frac{1}{3}X^3 + 3X^4$, alors $g(X) = 1 + \frac{1}{3^4}X^2 + \frac{1}{3^7}X^3 + \frac{1}{3^8}X^4$.

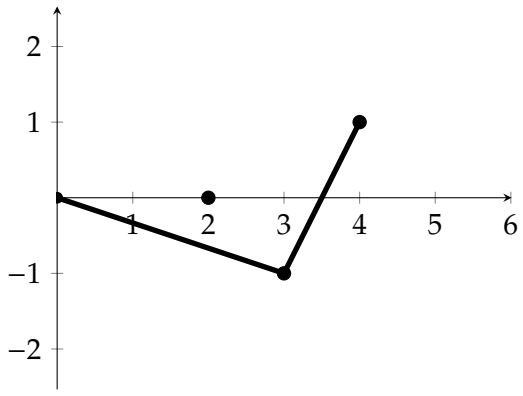


FIGURE 2.6 – Polygone de Newton de $f(X) = 1 + X^2 + \frac{1}{3}X^3 + 3X^4 \in \mathbb{Q}_3[X]$

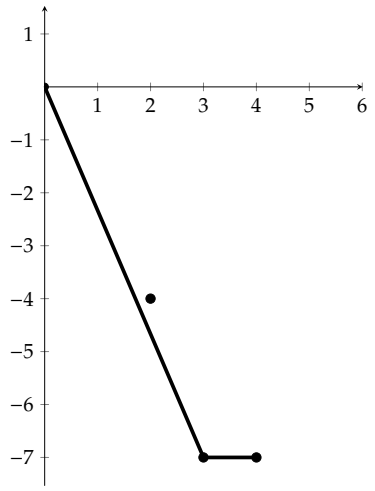


FIGURE 2.7 – Polygone de Newton de $g(X) \in \mathbb{Q}_3[X]$

Lemme 2.12. *Supposons que λ_1 soit la première pente du polygone de Newton de $f(X) = 1 + \sum_i a_i X^i \in 1 + X\mathbb{C}_p[[X]]$. Notons $c \in \mathbb{C}_p$ tel que $\mathrm{ord_p}(c) = \lambda \leq \lambda_1$ et supposons que $f(X)$ converge sur $D(p^\lambda)$. Alors en notant*

$$g(X) = (1 - cX)f(X) \in 1 + X\mathbb{C}_p[[X]]$$

Le polygone de Newton de g est obtenue en joignant le segment reliant $(0, 0)$ à $(1, \lambda)$ avec le polygone de Newton de f. De plus, si $f(X)$ a comme dernière pente λ_f et converge sur $D(p^{\lambda_f})$, alors $g(X)$ aussi, et réciproquement.

Démonstration.

* On commence par démontrer le cas où $c = 1, \lambda = 0$. Considérons donc $g = 1 + \sum_i b_i X^i$ où $b_{i+1} = a_{i+1} - a_i$ pour $(i \geq 0)$ avec $a_0 = 1$, alors on a

  $$\mathrm{ord_p}(b_{i+1}) \geq \min(\mathrm{ord_p}(a_{i+1}), \mathrm{ord_p}(a_i))$$

  avec l'égalité si $\mathrm{ord_p}(a_{i+1}) \neq \mathrm{ord_p}(a_i)$. Or comme les points $(i, \mathrm{ord_p}(a_i))$ et $(i, \mathrm{ord_p}(a_{i+1}))$ sont sur ou au dessus du polygone de Newton (car la première pente doit être supérieur ou égale à $0 = \lambda$), cela nous assure que $(i, \mathrm{ord_p}(b_{i+1}))$ aussi. Si $(i, \mathrm{ord_p}(a_i))$ est un sommet, alors $\mathrm{ord_p}(a_{i+1}) > \mathrm{ord_p}(a_i)$ et donc $\mathrm{ord_p}(b_{i+1}) = \mathrm{ord_p}(a_i)$. Cela nous assure que le polygone de Newton est bien celui décrit dans le théorème jusqu'au dernier sommet du polygone de Newton de $f(X)$ s'il existe.

* Il reste à montrer que, dans le cas où le polygone de Newton de $f(X)$ a une dernière pente λ_f infinie, alors celle de $g(X)$, notée λ_g aussi et que si $f(X)$ converge sur $D(p^{\lambda_f})$ alors $g(X)$ aussi et réciproquement. On a tout d'abord, avec les mêmes arguments que précédemment, que $\lambda_g \geq \lambda_f$ et que $g(X)$ converge là ou $f(X)$ converge. Supposons que l'on ait $\lambda_g > \lambda_f$, alors il existerait i tel que le point $(i + 1, \mathrm{ord_p}(a_i))$ se retrouve sous le polygone de Newton de $g(X)$, mais alors, on aurait pour tout $j \geq i + 1$, $\mathrm{ord_p}(b_j) > \mathrm{ord_p}(a_i)$. Or $a_{i+1} = b_{i+1} + a_i$ donc $\mathrm{ord_p}(a_{i+1}) = \mathrm{ord_p}(a_i)$ et donc par récurrence pour tout $j > i$, $\mathrm{ord_p}(a_j) = \mathrm{ord_p}(a_i)$. Ceci est impossible car on a donc $|a_i|_p = \frac{1}{p^{\mathrm{ord_p}(a_i)}}$ qui est constant à partir de $i + 1$ donc qui ne tend pas vers 0 ce qui contredit donc la convergence de $f(X)$ sur $D(1) = D(p^\lambda)$. On a donc bien $\lambda_g = \lambda_f$.

* Les deux points précédents étaient vérifiés dans le cas où $c = 1, \lambda = 0$, nous allons maintenant montrons que l'on peut s'y ramener. Si l'on est pas dans ce cas, alors en posant $f_1(X) = f\left(\frac{X}{c}\right)$ et $g_1(X) = (1 - X)f_1(X)$, on est dans le cas des deux premiers points de la démonstration du lemme en utilisant la remarque précédant le lemme et on obtient la forme du polygone de Newton de $g_1(X)$. On peut ensuite voir que $g(X) = g_1(cX)$, et dès lors en utilisant à nouveau la remarque précédant le lemme, on obtient bien le résultat souhaité sur le polygone de Newton de $g(X)$.

■

Lemme 2.13. *Soit $f(X) = 1 + \sum_i a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ ayant un polygone de Newton de première pente λ_1. Supposons que $f(X)$ converge sur $D(p^{\lambda_1})$ et que la droite passant par $(0, 0)$ de pente λ_1 passe par un point $(i, \mathrm{ord_p}(a_i))$. Alors, il existe $x \in \mathbb{C}_p$ tel que $\mathrm{ord_p}(x) = -\lambda_1$ et $f(x) = 0$.*

Démonstration.

* Commençons comme dans le lemme précédent par le cas où $\lambda_1 = 0$. Ainsi $\mathrm{ord_p}(a_i) \geq 0$ pour tout i et $f(X)$ converge sur $D(1)$ ce qui nous assure que $|a_i|_p \to 0$ et donc que $\mathrm{ord_p}(a_i) \to +\infty$. On peut alors considérer $N \geq 1$ le plus grand entier i tel que $\mathrm{ord_p}(a_i) = 0$. Notons pour la suite $f_n(X) = 1 + \sum_{i=1}^{n} a_i X^i$. Par le lemme 2.5, pour $n \geq N$, il existe un ensemble $S_{n,N} = \{x_{n,1}, \cdots, x_{n,N}\}$ de racines de $f_n(X)$ tel que $\mathrm{ord_p}(x_{n,i}) = 0$
* Construisons une suite $(x_n)_{n\geq N}$ de Cauchy et montrons que sa limite $x \in \mathbb{C}_p$ vérifie les conclusions du théorème. Pour se faire, on pose $x_N = x_{N,1}$ et pour $n \geq N$, considérons x_{n+1} comme étant l'élément $x_{n+1,i}$ tel que $|x_{n+1,i} - x_n|_p$ soit minimal. Montrons que cette suite ainsi construite est bien de Cauchy. Pour $n \geq N$, en notant R_n les racines du polynôme f_n, on a :

$$\begin{aligned}\left|f_{n+1}(x_n) - f_n(x_n)\right|_p &= \left|f_{n+1}(x_n)\right|_p \ (\text{car } f_n(x_n) = 0)\\ &= \prod_{\omega\in R_{n+1}} \left|1 - \frac{x_n}{\omega}\right|_p\end{aligned}$$

Or le polygone de Newton de f_{n+1}, nous dit que les racines de f_{n+1} qui ne sont pas dans $S_{n+1,N}$ sont de valuation p-adique > 0, et donc de norme p-adique < 1. Ainsi, pour toute racine $\omega \in R_{n+1}\backslash S_{n+1,N}$, $|\omega|_p < 1$ et donc $\left|\frac{x_n}{\omega}\right|_p = \frac{|x_n|_p}{|\omega|_p} > 1$ et donc $\left|1 - \frac{x_n}{\omega}\right|_p = 1$. Ainsi en reprenant l'égalité ci-dessus.

$$\begin{aligned}\left|f_{n+1}(x_n) - f_n(x_n)\right|_p &= \prod_{\omega\in R_{n+1}} \left|1 - \frac{x_n}{\omega}\right|_p\\ &= \prod_{i=1}^{N} \left|1 - \frac{x_n}{x_{n+1,i}}\right|_p\\ &= \prod_{i=1}^{N} |x_{n+1,i} - x_n|_p \quad \text{car } |x_{n+1,i}|_p = 1\\ &\geq |x_{n+1} - x_n|_p^N \quad \text{par choix de } x_{n+1}\end{aligned}$$

Ainsi,

$$|x_{n+1} - x_n|_p^N \leq \left|f_{n+1}(x_n) - f_n(x_n)\right|_p = \left|a_{n+1}x_n^{n+1}\right|_p = |a_{n+1}|_p \to 0$$

Donc la suite $(x_n)_{n\geq N}$ est bien de Cauchy par le rappel 1.1.

* Comme $\mathbb{C}_p$ est complet, alors il existe $x \in \mathbb{C}_p$ tel que $x_n \to x$, et comme somme partielle, on a $f(x) = \lim_{n\to+\infty} f_n(x)$. Il nous suffit donc pour conclure de montrer que $f_n(x) \to 0$. En effet,

$$\begin{aligned}\left|f_n(x)\right|_p = \left|f_n(x) - f_n(x_n)\right|_p &= \left|\sum_{i=1}^{n} a_i(x^i - x_n^i)\right|_p = |x - x_n|_p \left|\sum_{i=1}^{n} a_i \frac{x^i - x_n^i}{x - x_n}\right|_p\\ &\leq |x - x_n|_p \max_{i=1}^{n} \left|a_i \frac{x^i - x_n^i}{x - x_n}\right|_p\end{aligned}$$

$$\leq |x - x_n|_p \max_{i=1}^{n} \left| \frac{x^i - x_n^i}{x - x_n} \right|_p \text{ car } |a_i|_p \leq 1$$

$$\leq |x - x_n|_p \max_{i=1}^{n} \max_{k=1}^{i} \left| x^{i-1-k} x_n^k \right|_p \leq |x - x_n|_p$$

La dernière égalité provenant de $\left|x^{i-1-k}x_n^k\right|_p \leq \left|x^{i-1-k}\right|_p$ et que

$$|x|_p = \left|x - x_{n_0} + x_{n_0}\right|_p \leq \max(\left|x - x_{n_0}\right|_p, \left|x_{n_0}\right|_p) \leq 1$$

en ayant considéré $n_0 \in \mathbb{N}$ tel que $\left|x - x_{n_0}\right|_p \leq \varepsilon < 1$. Ainsi comme $x_n \to x$ alors $f_n(x) \to 0$. ce qui conclut pour ce cas.

* Revenons au cas général : Considérons $(i, \mathrm{ord_p}(a_i))$ qui est sur la ligne passant par $(0,0)$ de pente λ_1 et on considère π une racine i-ème de a_i. Alors $\mathrm{ord_p}(\pi) = \frac{\mathrm{ord_p}(a_i)}{i} = \lambda_1$. Posons alors $g(X) = f\left(\frac{X}{\pi}\right)$, alors $g(X)$ est telle que sa première pente est nulle par la remarque. Ainsi, il existe $x_0 \in \mathbb{C}_p$ tel que $f(x_0) = 0$ et $\mathrm{ord_p}(x_0) = 0$. En considérant donc $x = \frac{x_0}{\pi}$, on a $f(x) = f\left(\frac{x_0}{\pi}\right) = g(x_0) = 0$ et $\mathrm{ord_p}(x) = -\lambda_1$.

■

Lemme 2.14. *Soit $f(X) = 1 + \sum_i a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ et $\alpha \in \mathbb{C}_p$ tel que f converge en α et que $f(\alpha) = 0$. Considérons*

$$g(X) := \frac{f(X)}{1 - \frac{X}{\alpha}} := f(X) \times \sum_i \frac{X^i}{\alpha^i} = 1 + \sum_i b^i X^i$$

Alors $g(X)$ converge sur $D(|\alpha|_p)$.

Démonstration. Soit $f_n(X) = \sum_{i=1}^{n} a_i X^i$, la somme partielle de $f(X)$. On a alors que

$$b_i = \sum_{k=0}^{i} \frac{a_k}{\alpha^{i-k}}$$

Ainsi $\left|b_i \alpha^i\right|_p = \left|f_i(\alpha)\right|_p \underset{i \to +\infty}{\to} 0$ car $f(\alpha) = 0$. ■

Théorème 2.15 (Théorème p-adique de préparation de Weierstrass)**.** *Soit $f(X) = 1 + \sum_{i=1}^{+\infty} a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ convergeant sur $D(p^\lambda)$. Notons N la longueur totale des segments du polygone de Newton de pente $\leq \lambda$ si cette longueur est finie. Sinon, le polygone de Newton de f a un dernier segment infini de pente λ et considérons N comme étant le plus grand i tel que $(i, \mathrm{ord_p}(a_i))$ soit sur le dernier segment. (Celui-ci existe car $f(X)$ converge sur $D(p^\lambda)$). Alors, il existe un polynôme $h(X) \in 1 + X\mathbb{C}_p[X]$ de degré N et une série entière $g(X) = 1 + \sum_i b_i X^i$ non-nulle qui converge sur $D(p^\lambda)$ tel que*

$$h(X) = f(X)g(X)$$

Le polynôme $h(X)$ est uniquement déterminé par les propriétés ci-dessus et son polygone de Newton coincide avec celui de $f(X)$ jusqu'à $(N, \mathrm{ord_p}(a_N))$.

Démonstration.

* Commençons par démontrer le cas où $\lambda = 0$ puis on démontrera que l'on peut s'y ramener comme dans les lemmes préliminaires.
* Démontrons le résultat par récurrence sur N :
  - $N = 0$: Ce cas revient à montrer que $f(X)$ est inversible, d'inverse $g(X)$ qui est non-nulle et convergente sur $D(1)$. En notant ainsi, $g(X) = 1 + \sum_i b_i X^i$, on cherche les b_i de tel sorte que $f(X)g(X) = 1$. Ainsi :

$$f(X)g(X) = \left(1 + \sum_i a_i X^i\right)\left(1 + \sum_i b_i X^i\right) = 1 + \sum_{i=1}^{+\infty}\left(\sum_{k=0}^{i} a_k b_{i-k}\right) X^i$$

    On a donc en posant $a_0 = b_0 = 1$ que pour tout $i \geq 1$, $\sum_{k=0}^{i} a_k b_{i-k} = 0$, c'est à dire :

$$b_i = -(b_{i-1}a_1 + b_{i-2}a_2 + \cdots + b_1 a_{i-1} + a_i)$$

    Pour terminer ce cas, avec de tels b_i construits, il suffit de montrer que $g(X)$ converge sur $D(1)$, ce qui revient à montrer que $\mathrm{ord}_p(b_i) \underset{i\to+\infty}{\to} +\infty$. Or, on a tout d'abord comme $f(X)$ converge sur $D(1)$ et que $N = 0$, alors pour tout i, $0 < \mathrm{ord}_p(a_i) \underset{i\to+\infty}{\to} +\infty$. Par construction des b_i, on en déduit par une récurrence immédiate que $\mathrm{ord}_p(b_i) > 0$ pour tout i. De plus, en considérant $M > 0$, il existe $m > 0$ tel que pour tout $i \geq m, \mathrm{ord}_p(a_i) \geq M$. Posons dès lors

$$\varepsilon = \min(\mathrm{ord}_p(a_1), \mathrm{ord}_p(a_2), \cdots, \mathrm{ord}_p(a_m)) > 0$$

    et montrons par récurrence sur n que

$$\forall i > nm, \mathrm{ord}_p(b_i) \geq \min(M, n\varepsilon)$$

    Le cas $n = 0$ est immédiat. On s'intéresse donc à l'hérédité, et considérons $n \geq 1$ et $i > nm$, alors en s'intéressant à :

$$b_i = -(b_{i-1}a_1 + \cdots + b_{i-m}a_m + b_{i-(m+1)}a_{m+1} + \cdots + a_i)$$

    Or pour chaque terme $b_{i-j}a_j$ où $j > m$, on a $\mathrm{ord}_p(b_{i-j}a_j) \geq \mathrm{ord}_p(a_j) \geq M$. Pour les termes tels que $j \leq m$, comme $(i - j) > (n - 1)m$, alors par hypothèse de récurrence et définition de ε, on a

$$\mathrm{ord}_p(b_{i-j}a_j) \geq \mathrm{ord}_p(b_{i-j}) + \varepsilon \geq \min(M, (n-1)\varepsilon) + \varepsilon \geq \min(M, n\varepsilon)$$

    Ainsi pour tout $i > nm, \mathrm{ord}_p(b_i) \geq \min(M, n\varepsilon)$ car chaque terme de la somme est bien minoré par $\min(M, n\varepsilon)$. Ainsi $\mathrm{ord}_p(b_i) \underset{i\to+\infty}{\to} +\infty$, d'où le résultat pour le cas $N = 0$.
  - Supposons maintenant que $N \geq 1$ et que le théorème soit vrai au rang $N - 1$. Considérons $\lambda_1 \leq \lambda$ la première pente du polygone de Newton de $f(X)$. Alors par le lemme 2.13, il existe $\alpha \in \mathbb{C}_p$ tel que $f(\alpha) = 0$ et

$\mathrm{ord_p}(\alpha) = -\lambda_1$. En considérant $f_1(X) = \frac{f(X)}{1-\frac{X}{\alpha}} = 1 + \sum_i a_i' X^i \in 1 + X\mathbb{C}_p[[X]]$, alors par le lemme 2.14, $f_1(X)$ converge sur $D(p^{\lambda_1})$. En notant $c = \frac{1}{\alpha}$, on a donc $f(X) = (1 - cX)f_1(X)$, et en considérant η_1 la premère pente du polygone de Newton de $f_1(X)$, alors $\eta_1 \geq \lambda_1$. En effet, sinon $\eta_1 < \lambda_1$, il existerait $\beta \in \mathbb{C}_p$ tel que $f_1(\beta) = 0$ et $\mathrm{ord_p}(\beta) = -\eta_1$, on tirerait donc que $f(\beta) = 0$ et donc que la première pente du polygone de Newton de $f(X)$ est strictement inférieur à η_1 ce qui est impossible car celle-ci vaut λ_1. On a donc bien que $\eta_1 \geq \lambda_1$.
Alors par le lemme 2.12 appliqué à $f(X) = (1 - cX)f_1(X)$, on tire que le polygone de Newton de $f_1(X)$ est le même que celui de $f(X)$ en retirant le segment de $(0, 0)$ à $(1, \lambda_1)$. De plus, dans le cas où f a une dernière pente λ, comme f converge sur $D(p^\lambda)$ alors f_1 doit aussi converger sur $D(p^\lambda)$.
On peut dès lors appliquer l'hypothèse de récurrence à $f_1(X)$ qui satisfait bien les conditions avec $N - 1$. Il existe donc $h_1(X) \in 1 + X\mathbb{C}_p[X]$ de degré $N - 1$ et une série $g(X) \in 1 + X\mathbb{C}_p[[X]]$ qui converge et n'est pas nulle sur $D(p^\lambda)$ tel que

$$h_1(X) = f_1(X)g(X)$$

En notant $h(X) = (1 - cX)h_1(X)$, on tire que

$$h(X) = f(X)g(X)$$

avec $h(X)$ et $g(X)$ satisfaisant bien les propriétés souhaitées.

* Démontrons maintenant l'unicité de $h(X)$: Supposons qu'il existe $\tilde{h}(X) \in 1 + X\mathbb{C}_p[X]$ de degré N tel que $\tilde{h}(X) = f(X)g_1(X)$, où $g_1(X)$ converge et ne s'annule par sur $D(p^\lambda)$. Comme $\tilde{h}(X)g(X) = g_1(X)f(X)g(X) = h(X)g_1(X)$. Montrons que cette égalité nous assure que $\tilde{h}$ et h ont même racines et même multiplicité, cela nous donnera l'unicité décrit dans l'énoncé. Montrons le par réccurence sur N.
  - $N = 1$: c'est clair car $\tilde{h}(x) = 0 \iff h(x) = 0$ pour $x \in D(p^\lambda)$ car g, g_1 ne s'annule pas sur $D(p^\lambda)$.
  - Supposons maintenant que $N > 1$, sans perte de généralité, on peut supposer que $-\lambda = \mathrm{ord_p}(\alpha)$ où α est une racine de $h(X)$ tel que $\mathrm{ord_p}$ soit minimal. Comme on a l'égalité $\tilde{h}g = hg_1$ et que g, g_1 ne s'annule pas sur $D(p^\lambda)$, alors α est aussi une racine de $\tilde{h}$ tel que $\mathrm{ord_p}$ soit minimal, alors en divisant l'égalité par $(1 - \frac{X}{\alpha})$ et en utilisant le lemme 2.14 ; on s'est ramené au cas $N - 1$ et on utilise l'hypothèse de récurrence. Cela nous permet de conclure l'unicité.
* Revenons au cas général : Considérons $(i, \mathrm{ord_p}(a_i))$ qui est sur la dernière droite de pente λ et on considère π une racine i-ème de a_i. Alors $\mathrm{ord_p}(\pi) = \frac{\mathrm{ord_p}(a_i)}{i} = \lambda$. Posons alors $f_1(X) = f\left(\frac{X}{\pi}\right)$, alors $f_1(X)$ est telle que sa dernière pente est nulle. Ainsi, par le cas précédent, il existe $h_1(X)$ de degré N et $g_1(X)$ qui ne s'annule pas et converge sur $D(1)$ tel que

$$f_1(X) = h_1(X)g_1(X)$$

Alors

$$f(X) = f_1(\pi X) = h_1(\pi X)g_1(\pi X)$$

donc en posant $h(X) = h_1(\pi X)$ et $g(X) = g_1(\pi X)$, on a bien h de degré N et g qui ne s'annule pas et converge sur $D(p^\lambda)$.

■

On peut enfin ainsi énoncé l'équivalent du lemme 2.5 pour les séries qui donne tout intérêt aux polygones de Newton.

Corollaire 2.16. *Si un segment du polygone de Newton de $f(X) \in 1 + X\mathbb{C}_p[[X]]$ est finie de longueur N et de pente λ. Alors, il y a exactement N racines de f tel que* $\mathrm{ord_p} = -\lambda$.

Corollaire 2.17. *Si $f(X) \in 1 + X\mathbb{C}_p[[X]]$ converge sur $\mathbb{C}_p$ tout entier, alors $f(X)$ peut être factorisé en un produit infini de $(1 - \frac{X}{r})$ où r correspond à ses racines. De plus, si $f(X)$ n'a pas de racines et converge partout, alors $f(X)$ est constant.*

Démonstration. Si $f(X)$ converge sur $\mathbb{C}_p$, considérons λ. Par le théorème de préparation p-adique de Weierstrass, il existe $h_\lambda(X)$ de degré N_λ et $g_\lambda(X)$ qui ne s'annule pas et converge sur $D(p^\lambda)$ tel que

$$f(X) = h_\lambda(X)g_\lambda(X)$$

En notant $h_\lambda(X) = 1 + \sum_i^{N_\lambda} a_i X^i$ et $f(X) = 1 + \sum_i^{+\infty} b_i X^i$, comme les polygones de Newton coincident jusqu'à $(N_\lambda, \mathrm{ord_p}(a_{N_\lambda}))$, on a que pour $i \leq N_\lambda, \mathrm{ord_p}(a_i) \geq \mathrm{ord_p}(b_i)$, alors comme $\mathrm{ord_p}(a_i - b_i) \geq \min(\mathrm{ord_p}(a_i), \mathrm{ord_p}(b_i)) \geq \mathrm{ord_p}(b_i)$

$$|a_i - b_i|_p = \frac{1}{p^{\mathrm{ord_p}(b_i - a_i)}} \leq \frac{1}{p^{\mathrm{ord_p}(b_i)}} \to 0$$

car $f(X)$ converge sur $\mathbb{C}_p$ donc sur $\mathrm{ord_p}(b_i) \to +\infty$. Ainsi quand $\lambda \to +\infty$, on obtient que $h_\lambda \to f$. En particulier, on écrit h_λ en produit de ses racines puis comme $h_\lambda \to f$ alors $f(X) = \prod_{i=1}^{+\infty}(1 - \frac{X}{r_i})$ où r_i sont les racines de f. ■

2.3 Quelques exemples de polygones de Newton

Exemple 2.18.

1. Déterminons le polygône de Newton de $f_1(X) = \sum_{i=0}^{+\infty} \frac{X^{p^i - 1}}{p^i}$. Pour cette série entière, les coefficients sont donnés par

$$a_i = \begin{cases} \frac{1}{p^j} \text{ si } i = p^j - 1 \\ 0 \text{ sinon} \end{cases}$$

Nous avons donc $\mathrm{ord_p}(a_{p^j - 1}) = -j$. Le polygone de Newton est donc composée des segments joignant $(p^j - 1, -j)$ à $(p^{j+1} - 1, -(j+1))$. Un exemple ci-dessous pour $p = 2$

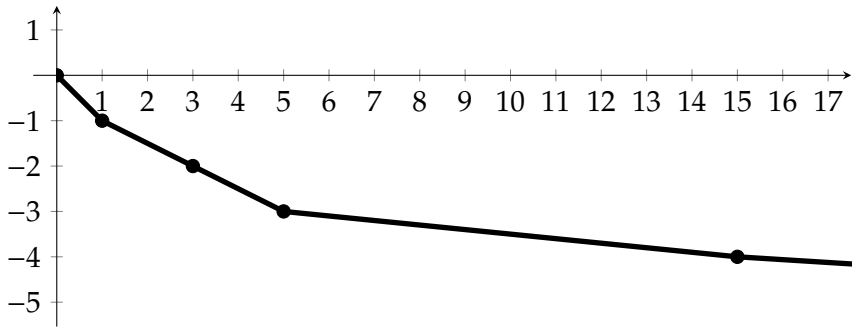


FIGURE 2.8 – Polygone de Newton de $f_1(X) \in \mathbb{Q}_2[[X]]$

2. Déterminons le polygone de Newton de $f_2(X) = \sum_{i=0}^{+\infty}((pX)^i + X^{p^i})$. Nous avons donc

$$a_i = \begin{cases} p^{p^j} + 1 \text{ si } i = p^j \text{ pour } j \in \mathbb{N} \\ p^i \text{ sinon} \end{cases}$$

Ainsi pour tout $j \in \mathbb{N}$, $\mathrm{ord_p}(a_{p^j}) = 0$, on obtient donc une ligne infinie horizontale nulle.

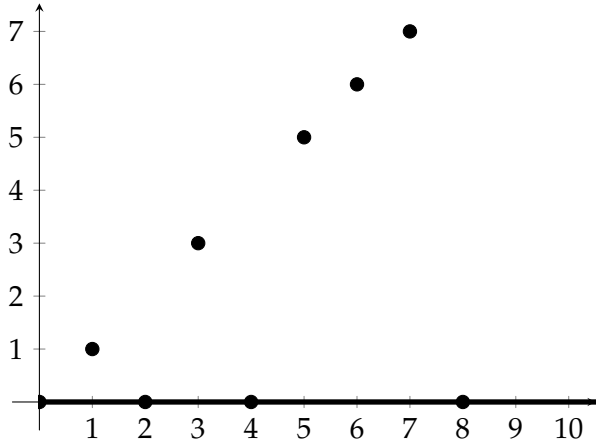


FIGURE 2.9 – Polygone de Newton de $f_2(X) \in \mathbb{Q}_2[[X]]$

3. Déterminons le polygône de Newton de $f_3(X) = \sum_{i=0}^{+\infty} i!X^i$. Nous avons vu précédemment que $\mathrm{ord_p}(i!) = \frac{i-S_i}{p-1}$. Les sommets du polygone de Newton de $f_3(X)$ correspondent aux indices i tel que S_i soit maximal. Cela revient à dire, les indices i tels que tous les coefficients du développement p-adique sont égaux à $p-1$. Ces indices sont donc tels que pour tout $r > 0$:

$$\begin{aligned} i &= \sum_{l=0}^{r}(p-1)p^l \\ &= (p-1)\sum_{l=0}^{r} p^l \\ &= (p-1) \times \frac{1-p^{r+1}}{1-p} \\ &= p^{r+1} - 1 \end{aligned}$$

Calculons dès lors $\mathrm{ord_p}(a_{p^i-1})$. On a tout d'abord que $S_{p^i-1} = i(p-1)$ et donc $\mathrm{ord_p}((p^i-1)!) = \frac{(p^i-1)-S_{p^i-1}}{p-1} = \frac{p^i-1}{p-1} - i = \sum_{l=0}^{i-1} p^l - i$. Ainsi le polygone de Newton est composée des segments joignants $(p^i - 1, \sum_{l=0}^{i-1} p^l - i)$ à $(p^{i+1} - 1, \sum_{l=0}^{i} p^l - (i+1))$.

4. Déterminons le polygône de Newton de $f_4(X) = \frac{(1-pX^2)}{(1-p^2X^2)}$. On observe tout d'abord que

$$f_4(X) = (1 - pX^2) \sum_{i=0}^{+\infty} (p^2X^2)^i = \sum_{j=0}^{+\infty} b_j X^j$$

où $b_j = \begin{cases} p^{2i} - p^{2(i-1)+1} = p^{2i-1}(p-1) \text{ si } j = 2i \\ 0 \text{ sinon} \end{cases}$

On obtient ainsi que le polynôme de Newton est composée du segment joignant $(0,0)$ à $(p,1)$ puis d'une droite de pente 1.

Chapitre 3

Rationalité de la fonction zêta

3.1 Critères algébriques de rationalité

Définition 3.1. Soit $a = (a_n)_{n\geq 0}$ une suite d'éléments d'un corps K. On appelle déterminant de Hankel de rang n et d'ordre k de la suite a, et on note $D_n^k(a)$ le déterminant de la matrice $[\alpha_{ij}]$ pour $0 \leq (i,j) \leq k$ où $\alpha_{ij} = a_{n+i+j}$.

Lemme 3.2. *Soit a une suite non stationnaire, s'il existe existe k et n_0 tels que, pour $n \geq n_0$, $D_n^k(a) = 0$, il existe h et n_1 tels que $D_n^h(a) = 0$ pour $n \geq n_1$, et $D_n^{h-1}(a) \neq 0$ pour $n \geq n_1 + 1$.*

Proposition 3.3. *Soit $f(X) = \sum_{n\geq 0} a_n X^n$ série formelle. $f(X)$ est une fraction rationelle si et seulement s'il existe k tel que, pour n assez grand, $D_n^k(a) = 0$.*

3.2 Le théorème de Borel-Dwork

Remarque 3.4. Effectuons de brefs rappels :

- Soit K un corps de nombres, $K = \mathbb{Q}[X]/(f)$ avec f un polynôme irréductible de degré n. On indexe pour la suite les racines α_i de f comme suit :
  1. Pour $i \in \{1, \dots, r\}$, $\alpha_i \in \mathbb{R}$
  2. Pour $i \in \{r+1, \dots, r+s\}$, $\alpha_i \neq \bar{\alpha_i} =: \alpha_{i+s}$

  On dénotera pour $x \in K$, $i \in \{1, \dots, r+s\}$, $|x|_i = |p_i(x)|$ où $p_i \in \mathrm{Hom}(K, \mathbb{C})$ avec $|.|$ le module usuel dans $\mathbb{C}$.
- les places de K sont les classes d'équivalences de valeurs absolues sur K.
- Les places finies de K sont en bijection avec les idéaux premiers de $\mathcal{O}_K$, l'anneau des entiers de K.
- Si on note $\mathrm{Spec}(\mathcal{O}_K)$ l'ensemble de ces idéaux premiers et si $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_K)$, on notera $|x|_{\mathfrak{P}}$ la valeur absolue $\mathfrak{P}$-adique normalisée associée à $\mathfrak{P}$.
- Soit p un nombre premier divisant $\mathfrak{P}$ et $\mathbb{C}_p$ le complété de la cloture algébrique de $\mathbb{Q}_p$. On notera $\mathbb{C}_{\mathfrak{P}}$ l'extension de K isomorphe à $\mathbb{C}_p$, munie de l'unique valeur absolue $|x|_{\mathfrak{P}}$ prolongeant la valeur absolue $\mathfrak{P}$-adique normalisée de K.
- De même, à toute place infinie de K est associée une valeur absolue $|x|_i$, pour $1 \leq i \leq r+s$ qui est la valeur absolue induite par le plongement correspondant de K dans $\mathbb{C}$ muni de la valeur absolue usuelle $|z|^2 = z\bar{z}$.
- Les valeurs absolues ainsi normalisées de K satisfont la formule du produit : Pour tout $x \in K$, $|x|_{\mathfrak{P}} = 1$ pour presque tout $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_K)$, et on a :

$$\prod_{i=1}^{r+s} |x|_i^{N(i)} \times \prod_{\mathfrak{P}\in \mathrm{Spec}(\mathcal{O}_K)} |x|_{\mathfrak{P}} = 1$$

où $N(i) = 1$ si $\alpha_i \in \mathbb{R}$ et $N(i) = 2$ si $\alpha_i \notin \mathbb{R}$. (où α_i sont les racines du polynôme définissant le corps de nombre).

Nous noterons désormais C un corps valué complet algébriquement clos, extension de K, et dont la valeur absolue induit sur K l'une des valeurs absolues normalisées ci-dessus : C est donc ou bien $\mathbb{C}$ ou bien $\mathbb{C}_\mathfrak{P}$.

Définition 3.5. Soient $f(X) = \sum_{n\geq 0} a_n X^n$ une série formelle à coefficients dans C et $R > 0$; nous dirons que f définit une fonction méromorphe dans le disque de centre 0 et de rayon R, si, quel que soit $r < R$, il existe un polynôme Q_r tel que la série $Q_r f$ converge pour $|X| \leq r$.

Remarque 3.6. On dira que f est p-adiquement méromorphe si f définit une fonction méromorphe dans tout disque de $\mathbb{C}_p$.

Lemme 3.7. *Soient K un corps de nombres et $f(X) = \sum_{n\geq 0} a_n X^n$ une série formelle à coefficients dans K. S'il existe une partie finie $P_1(K)$ de $\mathrm{Spec}(\mathcal{O}_K)$ telle que pour tout $\mathfrak{P} \notin P_1(K)$ et tout $n \geq 0$, $|a_n|_\mathfrak{P} \leq 1$, alors pour tout n et k, on a $|D_n^k(a)|_\mathfrak{P} \leq 1$.*

Démonstration. Le sous-anneau de K constitué des éléments x tels que que $|x|_\mathfrak{P} \leq 1$ contient l'ensemble des a_n par hypothèse. Il contient donc aussi la valeur au point $(a_n, a_{n+1}, \ldots, a_{n+2k})$ de tout polynôme à coefficients entiers, et donc en particulier $D_n^k(a)$. Ainsi $|D_n^k(a)|_\mathfrak{P} \leq 1$. ∎

Lemme 3.8. *Soit $f(X) = \sum_{n\geq 0} a_n X^n$ une série entière à coefficients dans C définissant une fonction méromorphe dans le disque ouvert de centre O et de rayon R. Soient $r < R$ et Q_r un polynôme de degré s tel que $Q_r f$ converge pour $|X| \leq r$, et soit $k \geq s$, alors il existe c, M tel que, pour $n \geq 0$:*

$$|D_n^k(a)| \leq M c^{-ns} r^{-n(k-s)}$$

avec $c < b$ où b désigne la borne inférieure des $|z|$ lorsque z parcourt les zéros de Q_r.

Démonstration. Soit $D = [a_{ij}]$ un déterminant d'ordre $m+1$, et soit $A_j = \begin{pmatrix} a_{0j} \\ \vdots \\ a_{mj} \end{pmatrix} \in C^{m+1}$.

On munit C^{m+1} de la norme $||X||$ qui au vecteur $X = (X_i)$ associe

$$\begin{aligned} ||X|| &= \max |X_i| \text{ si } C = \mathbb{C}_\mathfrak{P} \\ &= (|X_0^2| + \cdots + |X_m^2|)^{1/2} \text{ si } C = \mathbb{C} \end{aligned}$$

Alors

$$|D| \leq ||A_0||\ ||A_1|| \cdots ||A_m|| \quad (H)$$

En effet, si l'un des A_j est nul, cette inégalité est immédiate, il suffit donc de la prouver dans le cas où $\|A_j\| = 1$, pour tout $j \in \{0, \ldots, m\}$. Dans ce cas :

- Si $C = \mathbb{C}_\mathfrak{P}$, les a_{ij} sont tous dans dans l'anneau de valuarion de $\mathbb{C}_\mathfrak{P}$, donc D aussi, et $|D| \leq 1$.
- Si $C = \mathbb{C}$ et $D \neq 0$, si $(U_0, \ldots, U_m)$ est une suite orthonormale construite à partire des A_j par le procédé d'orthonormalisation de Schmidt :

$$D(U_0, \cdots, U_m) = 1 \geq D(A_0, \cdots, A_m) = D$$

En notant $a_n(f)$ les coefficients de f, $A_n^k(f) = (a_n(f), \dots, a_{n+k}(f)) \in C^{k+1}$ et $g = Q_r f$ où

$$Q_r(X) = q_0 + \cdots + q_s X^s$$

Comme $f(0) = a_0$, 0 n'est pas un pôle de f, on peut donc supposer $q_0 \neq 0$, et quitte à normaliser ce terme, on peut supposer que $q_0 = 1$. Avec ces notations, on peut écrire :

$$D_n^k(a(f)) = D_n^k = \det(A_n^k(f), A_{n+1}^k(f), \dots, A_{n+k}^k(f))$$

Pour $k \geq s$ et $m \geq s$:

$$\begin{aligned} A_m^k(g) &= A_m^k(Q_r f) \\ &= \big(a_m(g),\ \dots,\ a_{m+k}(g)\big) \\ &= \left(\sum_{i=0}^{s} a_{m-i}(f)q_i,\ \dots,\ \sum_{i=0}^{s} a_{m+k-i}(f)q_i\right) \\ &= \sum_{i=0}^{s} q_i(a_{m-i}(f), \dots, a_{m+k-i}(f)) \\ &= \sum_{i=0}^{s} q_i A_{m-i}(f) \end{aligned}$$

On a donc pour $k \geq s$ que

$$D_n^k = \det(A_n^k(f), \dots, A_{n+s-1}^k(f), A_{n+s}^k(g), \dots, A_{n+k}^k(g))$$

Or f (resp. g) définit une fonction analytique bornée dans le disque $|X| \leq c$ où $c < b$ (resp. $|X| \leq r$), de C, et C est algébriquement clos, donc d'après les inégalités de Cauchy, il existe deux constantes L_c et L'_r telles que, pour $n \geq 0$,

$$|a_n(f)| \leq L_c c^{-n} \text{ (resp. } |a_n(g)| \leq L'_r r^{-n})$$

On en déduit, que pour tout n, k :

$$||A_n^k(f)|| \leq \begin{cases} L_c c^{-n} \max(1, c^{-k}) \text{ si } C = \mathbb{C}_{\mathfrak{P}} \\ L_c c^{-n}(1 + c^{-2} + \cdots + c^{-2k})^{1/2} \text{ si } C = \mathbb{C} \end{cases}$$

et

$$||A_n^k(g)|| \leq \begin{cases} L'_r r^{-n} \max(1, r^{-k}) \text{ si } C = \mathbb{C}_{\mathfrak{P}} \\ L'_r r^{-n}(1 + r^{-2} + \cdots + r^{-2k})^{1/2} \text{ si } C = \mathbb{C} \end{cases}$$

À k fixé, il existe donc $L_1 = L_c \max(\max(1, c^{-k}), (1 + c^{-2} + \cdots + c^{-2k})^{1/2})$ et $L'_1 = L'_r \max(\max(1, r^{-k}), (1 + r^{-2} + \cdots + r^{-2k})^{1/2})$ deux constantes, telles que, pour tout $n \geq 0$:

$$||A_n^k(f)|| \leq L_1 c^{-n} \text{ et } ||A_n^k(g)|| \leq L'_1 r^{-n}$$

En appliquant l'inégalité (H) de Hadamard, on en déduit que pour $k \geq s$ et $n \geq 0$:

$$|D_n^k| \leq \prod_{i=0}^{s-1} ||A_{n+i}^k(f)|| \cdot \prod_{i=s}^{k} ||A_{n+i}(g)||$$

$$|D_n^k| \leq L_1^s \prod_{i=0}^{s-1} c^{-(n+i)} L_1'^{k-s+1} \prod_{i=s}^{k} r^{-(n+i)}$$
$$= L_1^s c^{-ns} c^{-s(s-1)/2} L_1'^{k-s+1} r^{-n(k-s+1)} r^{-s(k-s+1)} r^{-(k-s)(k-s+1)/2} = Mc^{-ns} r^{-n(k-s)}$$

où $M = L_1^s L_1'^{k-s+1} c^{-s(s-1)/2} r^{-n} r^{-(k-s+1)(k+s)/2}$. ■

Théorème 3.9 (Borel-Dwork). *Soient K un corps de nombres et $f(X) = \sum_{n\geq 0} a_n X^n$ une série formelle à coefficients dans K. S'il existe une partie finie $P_1(K)$ de $\mathrm{Spec}(\mathcal{O}_K)$ telle que :*

i) Pour tout $\mathfrak{P} \notin P_1(K)$ et tout $n \geq 0$, $|a_n|_{\mathfrak{P}} \leq 1$.

ii) pour chacune des $r+s$ places infinies de K, f définit dans C une fonction méromorphe dans un disque ouvert de centre 0 et de rayon et de rayon R_i pour $i \in \{1, \ldots, r+s\}$.

iii) Pour $\mathfrak{P} \in P_1(K)$, f définit dans $\mathbb{C}_{\mathfrak{P}}$ une fonction méromorphe dans un disque ouvert de centre 0 et de rayon $R_{\mathfrak{P}}$.

iv) Le produit $R = \prod_{i=1}^{r+s} R_i^{N(i)} \times \prod_{\mathfrak{P}\in P_1(K)} R_{\mathfrak{P}}$ satisfait R>1.

Alors f est une fraction rationnelle.

Démonstration. Choisissons pour $i \in \{1, \ldots, r+s\}$ des réels r_i tels que $r_i < R_i$ et pour $\mathfrak{P} \in P_1(K)$ un réel $r_{\mathfrak{P}}$ tel que $r_{\mathfrak{P}} < R_{\mathfrak{P}}$ de telle sorte que le produit

$$r = \prod_{i=1}^{r+s} r_i^{N(i)} \prod_{\mathfrak{P}\in P_1(K)} r_{\mathfrak{P}} > 1$$

Notons v un indice parcourant $V = \{1, \ldots, r+s\} \cup P_1(K)$. Pour $v \in V$, considérons Q_v un polynôme de degré s_v satisfaisant les deux conditions

a) $Q_v(0) \neq 0$

b) fQ_v converge dans C_v pour $|X| \leq r_v$

Considérons b_v la borne inférieure des z_v où z_v parcourt les zéros de Q_v. Notons de plus s la borne supérieure des s_v, alors, pour $k \geq s$: par le lemme 3.8, il existe des constantes $c_v, M_{v,k}$ telles que :

$$\prod_{v\in V} |D_n^k(a)|_v^{N(v)} \leq \prod_{v\in V} \left(M_{v,k} c_v^{-ns_v} r_v^{-n(k-s_v)} \right)^{N(v)}$$

où $N(v) = 1$ si $v = \mathfrak{P}$, et $c_v < b_v$.

Posons alors $\Delta_v(k) = \left(c_v^{-s_v} r_v^{-(k-s_v)} \right)^{N(v)}$ et $\Delta(k) = \prod_{v\in V} \Delta_v(k)$, alors $\lim_{k\to+\infty} (\Delta(k))^{1/k} = \frac{1}{r} < 1$. On peut donc choisir k_0 de telle sorte que $\Delta(k_0) < 1$. Fixons un tel k_0, et soit $\Delta = \Delta(k_0)$, alors en posant $M = \prod_{v\in V} M_{v,k_0}^{N(v)}$, on a :

$$\prod_{v\in V} |D_n^{k_0}(a)|_v^{N(v)} \leq \Delta^n M \quad \text{avec} \quad \Delta < 1$$

Ainsi, étant donné le lemme 3.7 et la formule du produit, cela nous assure si $D_n^{k_0}(a) \neq 0$ que $\Delta^n M \geq \prod_{\mathfrak{P}\notin P_1(K)} \frac{1}{|D_n^{k_0}(a)|_{\mathfrak{P}}} \geq 1$ ce qui est absurde car $\Delta < 1$. Donc, pour n assez grand, $D_n^{k_0}(a) = 0$ et donc par le critère 3.3 que f est rationnelle. ■

3.3 Hypersurfaces et fonctions zêta

3.3.1 Hypersurfaces affines et projectives

Définition 3.10. Si K est un corps, on définit l'espace affine de dimension n sur K et on note :

$$\mathbb{A}_K^n = \{(x_1, \dots, x_n), x_i \in K\}$$

Définition 3.11. Soit $f(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ un polynôme en n variables $X_1, \dots, X_n$.

* On appelle hypersurface affine définie par f dans $\mathbb{A}_K^n$ et on note :

$$H_f = \left\{(x_1, \dots, x_n) \in \mathbb{A}_K^n, f(x_1, \dots, x_n) = 0\right\}$$

* On appelle dimension de H_f l'entier $n - 1$.

Remarque 3.12. Si $n = 2$, on dit que H_f est une courbe affine (*i.e.* si H_f est de dimension 1).

Définition 3.13. On appelle espace projectif de dimension n sur K :

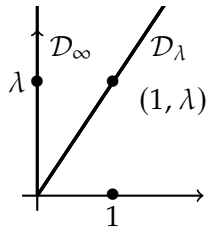
$$\mathbb{P}_K^n = \left\{[x_0, x_1, \dots, x_n] \text{ où } (x_0, \dots, x_n) \in \mathbb{A}_K^{n+1} \backslash \{(0, 0, \dots, 0)\}\right\}$$

tel que $[x_0, x_1, \dots, x_n] = [y_0, y_1, \dots, y_n]$ si et seulement si il existe $\lambda \in K^\times$ pour tout $i \in \{0, \dots, n\}, x_i = \lambda y_i$.

Exemple 3.14. Intéressons nous à $\mathbb{P}_K^1$: cela correspond aux droites vectorielles du plan affine de K^2.

* si $u_0 \neq 0$, $[u_0, u_1] = [1, \frac{u_1}{u_0}]$
* sinon $[0, u_1] = [0, 1]$

On fait donc une correspondance $[1, \lambda] \leftrightarrow \mathcal{D}_\lambda$ et $[0, 1] \leftrightarrow \mathcal{D}_\infty$



Remarque 3.15. Plus généralement, $\mathbb{P}_K^n$ correspond à l'ensemble des droites vectorielles de K^{n+1}. En effet

— À une droite vectorielle, on associe la classe d'un vecteur directeur.

— Réciproquement, si $[u_0, \dots, u_n] \in \mathbb{P}_K^n$ avec $u_i \neq 0$, on associe Vect $\left(\frac{u_0}{u_i}, \frac{u_1}{u_i}, \dots, \frac{u_i}{u_i}, \frac{u_{i+1}}{u_i}, \dots, \frac{u_n}{u_i}\right)$.

Proposition 3.16. *On a la bijection suivante :*

$$\begin{array}{rcl} \mathbb{A}_K^n & \leftrightarrow & U_i := \{[u_0, \dots, u_n], u_i \neq 0\} \\ (a_1, \dots, a_n) & \mapsto & [a_1, a_2, \dots, a_{i-1}, 1, a_i, a_{i+1}, \dots, a_n] \end{array}$$

Définition 3.17. On appelle hyperplan à l'infini et on note

$$\mathcal{Z}(u_0) = \{[u_0, \dots, u_n], u_0 = 0\}$$

(Celui-ci dépend du choix des coordonnées).

Proposition 3.18. *On peut décrire l'espace projectif affine à partir des espaces affines :*

$$\mathbb{P}_K^n = \text{pt} \cup \mathbb{A}_K^1 \cup \mathbb{A}_K^2 \cup \cdots \cup \mathbb{A}_K^n$$

Démonstration. Commençons par une première remarque liée à l'hyperplan à l'infini :

$$\mathcal{Z}(u_0) = \left\{[u_1, \dots, u_n],\ \text{où } (u_1, \dots, u_n) \in \mathbb{A}_K^n \backslash \{(0, \dots, 0)\}\right\} = \mathbb{P}_K^{n-1}$$

On a de plus via la proposition 3.16 que $\mathbb{P}_K^n \backslash \mathcal{Z}(u_0) = U_0 \simeq \mathbb{A}_K^n$. Ainsi, on obtient de proche en proche :

$$\begin{aligned}
\mathbb{P}_K^n &= \mathcal{Z}(u_0) \cup \mathbb{P}_K^n \backslash \mathcal{Z}(u_0) \\
&= \mathbb{P}_K^{n-1} \cup \mathbb{A}_K^n \\
&= \mathcal{Z}(u_1) \cup \mathbb{P}_K^{n-1} \backslash \mathcal{Z}(u_1) \cup \mathbb{A}_K^n \\
&= \mathbb{P}_K^{n-2} \cup \mathbb{A}_K^{n-1} \cup \mathbb{A}_K^n \\
&= \cdots \\
&= \mathbb{P}_K^0 \cup \mathbb{A}_K^1 \cup \cdots \cup \mathbb{A}_K^n \\
&= \mathrm{pt} \cup \mathbb{A}_K^1 \cup \cdots \cup \mathbb{A}_K^n
\end{aligned}$$

■

Définition 3.19. Considérant $f(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ de degré d, on appelle polynôme homogénéisé de f, noté $\tilde{f}$:

$$\tilde{f}(X_0, X_1, \dots, X_n) = X_0^d f\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right)$$

Remarque 3.20. L'homogénéisé de f est un polynôme homogène de degré d.

Exemple 3.21. En notant $f(X_1, X_2, X_3) = X_3^3 - 3X_1X_2X_3 + X_1 + 1 \in K[X_1, X_2, X3]$, celui-ci est de degré 3, son homogénéisé est

$$\tilde{f}(X_0, X_1, X_2, X_3) = X_0^3 + X_0^2X_1 - 3X_1X_2X_3 + X_3^3$$

Remarque 3.22. Si $\tilde{f}(X_0, \dots, X_n)$ est homogène, et si $\tilde{f}(x_0, \dots, x_n) = 0$, alors pour tout $\lambda \in K^\times$, $\tilde{f}(\lambda x_0, \dots, \lambda x_n) = 0$. Cela donc à un sens de parler de l'ensemble des points de $\mathbb{P}_K^n$ où $\tilde{f}$ s'annule.

Définition 3.23. Étant donné $f(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ un polynôme de degré d et $\tilde{f}(X_0, \dots, X_n) \in K[X_0, X_1, \dots, X_n]$ un polynôme homogène de degré d.

* On appelle hypersurface projective définie par $\tilde{f}$ dans $\mathbb{P}_K^n$ l'ensemble

$$\tilde{H}_{\tilde{f}} = \left\{[x_0, x_1, \dots, x_n] \in \mathbb{P}_K^n, \tilde{f}(x_0, \dots, x_n) = 0\right\}$$

* Si f est l'homogénéisé de f, on dit que $\tilde{H}_{\tilde{f}}$ est le complété projectif de l'hypersurface affine H_f.

Exemple 3.24.

1. Soit $f(X, Y) = \sum_{i,j} a_{i,j} X^i Y^j \in K[X, Y]$ de degré M. Notons $g = \tilde{f}(X_0, X_1, X_2) = f\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right) X_0^M$ son homogénéisé de degré M. On obtient donc

$$\begin{aligned}
H_g = \tilde{H}_{\tilde{f}} &= \{[u_0, u_1, u_2] \in \mathbb{P}_K^2, g(u_0, u_1, u_2) = 0\} \\
&= \{[u_0, u_1, u_2] \in \mathbb{P}_K^2, \left[\sum_{i,j} a_{i,j} \left(\frac{u_1}{u_0}\right)^i \left(\frac{u_2}{u_0}\right)^j\right] u_0^M = 0\}
\end{aligned}$$

$$H_g = \{[0, u_1, u_2] \in \mathbb{P}^2_K, g(0, u_1, u_2) = 0\} \cup \left\{\left[1, \frac{u_1}{u_0}, \frac{u_2}{u_0}\right] \in \mathbb{P}^2_K, g\left(1, \frac{u_1}{u_0}, \frac{u_2}{u_0}\right) = 0\right\}$$
$$= (H_g \cap u_0 = 0) \cup H_f$$

2. Considérons $K = \mathbb{R}$, $f(X, Y) = \frac{X^2}{a^2} - \frac{Y^2}{b^2} - 1$, H_f l'hyperbole :

$$H_f = \left\{(x_1, x_2) \in \mathbb{A}^2_{\mathbb{R}}, \frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} = 1\right\}$$

Alors $\tilde{f}(X_0, X_1, X_2) = \frac{X_1^2}{a^2} - \frac{X_2^2}{b^2} - X_0^2$, alors on a par ce qui précède que

$$\tilde{H}_{\tilde{f}} = \left\{[1, x_1, x_2], \frac{x_1^2}{a^2} - \frac{x_2^2}{b^2} = 1\right\} \cup \left\{[0, 1, x_2], x_2 = \pm\frac{b}{a}\right\}$$

Remarque 3.25. Si L est une extension de corps de K, on notera

$$H_f(L) = \left\{(x_1, \ldots, x_n) \in \mathbb{A}^n_L | f(x_1, \ldots, x_n) = 0\right\}$$

De façon similaire à ce qui précède, si $\tilde{f}$ est homogène, on définit $\tilde{H}_{\tilde{f}}(L)$.

3.3.2 La fonction zêta

Remarque 3.26. On travaillera dans la suite avec $K = \mathbb{F}_q$ et des extensions de corps finis $L = \mathbb{F}_{q^s}$. Dans ce cas, $H_f(L)$ et $\tilde{H}_{\tilde{f}}(K)$ consiste en un nombre fini de points car il y a un nombre fini de n-uplets (exactement q^{ns}) dans $\mathbb{A}^n_L$ tout comme dans $\mathbb{P}^n_L$.

Définition 3.27. À f ou $\tilde{f}$ fixé, on définit

* $N_s := \mathrm{Card}(H_f(\mathbb{F}_{q^s}))$ le nombre de points de $\mathbb{F}_{q^s}$ de H_f.
* $\tilde{N}_s := \mathrm{Card}(\tilde{H}_{\tilde{f}}(\mathbb{F}_{q^s}))$ le nombre de points de $\mathbb{F}_{q^s}$ de $\tilde{H}_{\tilde{f}}$.

Définition 3.28. Étant donné un polynôme $f(X_1, \ldots, X_n)$ de $\mathbb{F}_q[X_1, \ldots, X_n]$ et H_f son hypersurface affine associée, on appelle fonction zêta de H_f la série entière formelle de $\mathbb{C}_p[[T]]$

$$Z(H_f/\mathbb{F}_q; T) := \exp\left(\sum_{s=1}^{+\infty} \frac{N_s}{s} T^s\right)$$

Remarque 3.29. On observe que $Z(H_f/\mathbb{F}_q; T)$ a comme terme constant 1.

Exemple 3.30. Donnons quelques exemples de calculs de N_s et Z pour une hypersurface donnée.

1. En considérant $H_f = \mathrm{pt}$, alors $N_s = 1$. On obtient donc

$$\begin{aligned} Z(\mathrm{pt}/\mathbb{F}_q; T) &= \exp\left(\sum_{s=1}^{+\infty} \frac{1}{s} T^s\right) \\ &= \exp\left(-\log(1 - T)\right) \\ &= \frac{1}{1 - T} \end{aligned}$$

2. En considérant $H_f = \mathbb{A}^n_{\mathbb{F}_q}$, cela correspond au n-uplets de $\mathbb{F}_q$. Pour tout $s \in \mathbb{N}^*$, $N_s = q^{ns}$ et donc

$$\begin{aligned} Z(\mathbb{A}^n_{\mathbb{F}_q}/\mathbb{F}_q; T) &= \exp\left(\sum_{s=1}^{+\infty} \frac{q^n s}{s} T^s\right) \\ &= \exp\left(\sum_{s=1}^{+\infty} \frac{1}{s}(q^n T)^s\right) \\ &= \exp\left(-\log(1 - q^n T)\right) \\ &= \frac{1}{1 - q^n T} \end{aligned}$$

3. En considérant $H_f = \mathbb{P}^n_{\mathbb{F}_q} = \bigcup_{k=1}^{n} \mathbb{A}^k_{\mathbb{F}_q} \cup \text{pt}$. Alors pour tout $s \in \mathbb{N}^*$, $N_s = \sum_{k=0}^{n} q^{ks}$ et donc

$$\begin{aligned} Z(\mathbb{P}^n_{\mathbb{F}_q}/\mathbb{F}_q; T) &= \exp\left(\sum_{s=1}^{+\infty} \frac{\sum_{k=0}^{n} q^{ks}}{s} T^s\right) \\ &= \exp\left(\sum_{k=0}^{n} \sum_{s=1}^{+\infty} \frac{q^{ks}}{s} T^s\right) \\ &= \prod_{k=0}^{n} \exp\left(\sum_{s=1}^{+\infty} \frac{q^{ks}}{s} T^s\right) \\ &= \prod_{k=0}^{n} \frac{1}{1 - q^k T} \end{aligned}$$

4. Considérons une droite affine $L = H_{X_1} \subseteq \mathbb{A}^2_{\mathbb{F}_q}$. On a $N_s = q^s$ et donc

$$\begin{aligned} Z(L/\mathbb{F}_q; T) &= \exp\left(\sum_{s=1}^{+\infty} \frac{1}{s}(qT)^s\right) \\ &= \exp\left(-\log(1 - qT)\right) \\ &= \frac{1}{1 - qT} \end{aligned}$$

5. En considérant maintenant un droite projective $\tilde{L}$, on a $\tilde{N}_s = q^s + 1$ et donc

$$\begin{aligned} Z(\tilde{L}/\mathbb{F}_q; T) &= \exp\left(\sum_{s=1}^{+\infty} \frac{q^s + 1}{s} T^s\right) \\ &= \exp\left(-\log(1 - qT)\right) \exp\left(-\log(1 - T)\right) \\ &= \frac{1}{(1 - T)(1 - qT)} \end{aligned}$$

Proposition 3.31. *Soit H_f une hypersurface affine sur un corps fini $\mathbb{F}_q$. Alors $Z(H_f/\mathbb{F}_q; T)$ est à coefficients dans $\mathbb{N}$.*

Démonstration. Soit $X = (x_1, \ldots, x_n)$ un $\mathbb{F}_{q^{s_0}}$-point de H_f (où s_0 est le plus petit entier

s tel que tout les x_i soient dans $\mathbb{F}_{q^{s_0}}$). Notons x_{ij} les conjugués de x_i sur $\mathbb{F}_q$ pour tout $1 \leq j \leq s_0$. On peut alors considérer $P_j = (x_{1j}, \dots, x_{nj})$ les conjugués de X. Ceux-ci doivent être distincts, en effet, sinon, tous les x_i seraient laissé fixe par un $\mathbb{F}_q$-automorphisme σ de $\mathbb{F}_{q^{s_0}}$, ils seraient donc tous dans le sous-corps de $\mathbb{F}_{q^{s_0}}$ laissé fixe par σ (ce qui contredirait la minimalité de s_0).

Ainsi, tous les P_j sont des $\mathbb{F}_{q^s}$-points dès que $s_0|s$ et chaque P_j contribue à raison de s_0 pour $N_{s_0}, N_{2s_0}, \dots$. On obtient ainsi leurs contributions à $Z(H_f/\mathbb{F}_q; T)$:

$$\exp\left(\sum_{j=1}^{+\infty} \frac{s_0}{js_0} T^{js_0}\right) = \exp(-\log(1 - T^{s_0})) = \frac{1}{1 - T^{s_0}} = \sum_{j=0}^{+\infty} T^{js_0}$$

Or la fonction zêta est un produit de séries ci-dessus, ce qui nous assure que la fonction zêta est à coefficients entiers. ■

Lemme 3.32. *Le coefficient devant T^j dans $Z(H_f/\mathbb{F}_q; T)$ est majorée par q^{nj}.*

Démonstration. La plus grande valeur possible pour N_s est la cardinal de $\mathbb{A}^n_{\mathbb{F}_{q^s}}$ qui est q^{ns}. Ainsi, les coefficients de $Z(H_f/\mathbb{F}_q; T)$ sont donc plus petit ou égaux à ceux de la série avec $N_s = q^{ns}$. Or,

$$\exp\left(\sum_{s=1}^{+\infty} \frac{q^{ns}}{s} T^s\right) = \exp(-\log(1 - q^n T)) = \frac{1}{1 - q^n T} = \sum_{j=0}^{+\infty} q^{nj} T^j$$

■

Remarque 3.33. En particulier, cela nous assure que $Z(H_f/\mathbb{F}_q; T)$ définie une fonction holomorphe sur le disque de rayon $\frac{1}{q^n}$ dans $\mathbb{C}$.

Dans le but d'appliquer le théorème de Borel-Dwork à la fonction zêta, il suffit de démontrer que la fonction zêta définie une fonction méromorphe sur $\mathbb{C}_p$, c'est l'objectif des deux prochaines sections. Toute cette partie est par exemple omise dans le livre de Y. Amice.

3.3.3 Endomorphismes de $\mathbb{C}_p[[X_1, \dots, X_n]]$

Le but de cette sous-section est de prouver la formule de la trace de Dwork ce qui correspond au premier des deux résultats nécéssaire à la démonstration de la p-adique méromophie de la fonction zêta.

Dans toute cette sous-section, on notera $R = \mathbb{C}_p[[X_1, \dots, X_n]]$. Si $X_1^{u_1} \dots X_n^{u_n} \in R$ est un monôme, on notera X^u où $u = (u_1, \dots, u_n) \in \mathbb{N}^n$. Un élément de R peut être écrit $\sum a_u X^u$ où u parcourt l'ensemble $\mathbb{N}^n$ et $a_u \in \mathbb{C}_p$.

Notons $G \in R$. On définit un endomorphisme de R définit par la multiplication par G :

$$\begin{array}{rccc} \mu_G : & R & \to & R \\ & r & \mapsto & Gr \end{array}$$

Considérons $q \in \mathbb{N}$, on définit un autre endomorphisme de R :

$$\begin{array}{rccc} \phi_q : & R & \to & R \\ & \sum\limits_{u \in \mathbb{N}^n} a_u X^u & \mapsto & \sum\limits_{u \in \mathbb{N}^n} a_{qu} X^u \end{array}$$

En d'autres termes, si $u \in \mathbb{N}^n$ n'est pas divisible par q, alors le terme correspondant $a_u X^u$ s'annule sous l'action de ϕ_q. Si u est divisible par q, alors ϕ_q remplace X^u par $X^{u/q}$.

Enfin, on notera pour la suite $\Psi_{q,G} = \phi_q \circ \mu_G$ la composition des deux endomorphismes précédents. Si $G = \sum_{w \in \mathbb{N}^n} g_w X^w$. Alors $\Psi_{q,G}$ agit sur les monômes X^u comme suit :

$$\Psi_{q,G}(X^u) = \phi_q \left(\sum_{w \in \mathbb{N}^n} g_w X^{w+u} \right) = \sum_{w \in \mathbb{N}^n} g_{qw-u} X^w$$

Lemme 3.34. *Soit $G = \sum_{w \in \mathbb{N}^n} g_w X^w \in R$. Si l'on note $G_q(X) = G(X^q)$, alors*

$$\mu_G \circ \phi_q = \phi_q \circ \mu_{G_q} = \Psi_{q,G_q}$$

Démonstration. Il suffit de vérifier cette égalité sur les monomes X^u. On observe tout d'abord d'une part que :

$$\begin{aligned} \mu_G \circ \phi_q(X^u) &= \begin{cases} 0 & \text{si } q \nmid u \\ G X^{u/q} & \text{si } q \mid u \end{cases} \\ &= \begin{cases} 0 & \text{si } q \nmid u \\ \displaystyle\sum_{w \in \mathbb{N}^n} g_w X^{w+u/q} = \sum_{w \in \mathbb{N}^n} g_{w-u/q} X^w & \text{si } q \mid u \end{cases} \end{aligned}$$

D'autre part, on a :

* Dans le cas où $q \mid u$, on a :

$$\phi_q \circ \mu_{G_q}(X^u) = \phi_q \left(\sum_{w \in \mathbb{N}^n} g_w X^{qw+u} \right) = \sum_{w \in \mathbb{N}^n} g_{qw} X^{qw+u} = \sum_{w \in \mathbb{N}^n} g_{w-u/q} X^w$$

* Dans le cas où $q \nmid u$, on a :

$$\phi_q \circ \mu_{G_q}(X^u) = \phi_q \left(\sum_{w \in \mathbb{N}^n} g_w X^{qw+u} \right) = 0$$

On obtient bien ainsi l'égalité souhaitée. ∎

Définition 3.35. On définit l'ensemble suivant

$$R_0 = \left\{ G = \sum_{w \in \mathbb{N}^n} g_w X^w \in R \mid \exists M > 0, \forall w \in \mathbb{N}^n, \mathrm{ord}_{\mathrm{p}}(g_w) \geq M|w| \right\}$$

où $|w|$ correspond à la somme des composantes de w.

Remarque 3.36. La définition pour une série d'être dans R_0 implique sa convergence dans un disque $D(r)$ contenant au moins strictement $D(1)$.

Lemme 3.37. *R_0 est stable par multiplication et sous l'application $G \mapsto G_q$.*

Démonstration.

* Considérons $f(X) = \sum_{v \in \mathbb{N}^n} a_v X^v$, $g(X) = \sum_{w \in \mathbb{N}^n} b_w X^w$ deux séries de R_0 et enfin leur produit $f(X)g(X) = \sum_{z \in \mathbb{N}^n} c_z X^z$ où $c_z = \sum_{m+n=z} a_m b_n$.

Or par hypothèse, f et g étant dans R_0, il existe deux constantes $M_1, M_2 > 0$ telles que pour tout $w \in \mathbb{N}^n$, on ait :

$$\mathrm{ord_p}(a_w) \geq M_1|w| \text{ et } \mathrm{ord_p}(b_w) \geq M_2|w|$$

On obtient donc que :

$$\begin{aligned}
\mathrm{ord_p}(c_z) &\geq \min_{m+n=z} \mathrm{ord_p}(a_m b_n) \\
&= \min_{m+n=z} \mathrm{ord_p}(a_m) + \mathrm{ord_p}(b_n) \\
&\geq \min_{m+n=z} M_1|m| + M_2|n| \\
&\geq \min(M_1, M_2) \min_{m+n=z} |m| + |n| \\
&= \min(M_1, M_2)|z| \quad \text{car } |m| + |n| = |z|
\end{aligned}$$

Ainsi leur produit $f(X)g(X) \in R_0$, donc R_0 est stable par multiplication.

* Considérons $G(X) = \sum_{w \in \mathbb{N}^n} g_w X^w \in R_0$, Il existe une constante $M > 0$ telle que pour tout $w \in \mathbb{N}^n$, $\mathrm{ord_p}(g_w) \geq M|w|$. En considérant alors $G_q(X) = \sum_{w \in \mathbb{N}^n} g_w X^{qw}$, on peut réécrire $G_q(X) = \sum_{z \in \mathbb{N}^n} \tilde{g}_z X^z$, où $\tilde{g}_z = 0$ sauf si $q|z$. Dans le cas $q|z$, on a $z = qu$ où u est la puissance d'un monôme de $G(X)$. On obtient donc :

$$\mathrm{ord_p}(\tilde{g}_z) = \mathrm{ord_p}(g_u) \geq M|u| = \frac{M}{q} |qu| = \frac{M}{q}|z|$$

Ainsi $G_q \in R_0$.

■

Lemme 3.38. *En notant $\mathbb{U}_n(\mathbb{C})$ l'ensemble des racines n-ème de l'unité, alors*

$$\sum_{\zeta \in \mathbb{U}_n(\mathbb{C})} \zeta^a = \begin{cases} n & si\ n \mid a \\ 0 & si\ n \nmid a \end{cases}$$

Démonstration. Distinguons les cas :

* Si $n \mid a$, alors $\zeta^a = 1$ et comme il y a exactement n racines n-ème de l'unité, alors $\sum_{\zeta \in \mathbb{U}_n(\mathbb{C})} \zeta^a = n$.
* Si $n \nmid a$, comme $\mathbb{U}_n(\mathbb{C})$ forme un groupe cyclique, donc fixant $\tilde{\zeta} \in \mathbb{U}_n(\mathbb{C}) \backslash \{1\}$, alors $\mathbb{U}_n(\mathbb{C}) = \{\tilde{\zeta}^k, k \in \{0, 1, \ldots, n-1\}\}$, on en conclut que

$$\sum_{\zeta \in \mathbb{U}_n(\mathbb{C})} \zeta^a = \sum_{k=0}^{n-1} \tilde{\zeta}^{ak} = \frac{1 - \tilde{\zeta}^{an}}{1 - \tilde{\zeta}} = 0$$

■

Remarque 3.39.

* On rappelle que si V est un espace vectoriel de dimension n sur un corps K et $A : V \to V$ une application linéaire de matrice $(a_{i,j})_{1 \leq i,j \leq n}$, la trace de A est l'élément suivant :

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{i,i}$$

* Maintenant si on considère V un espace vectoriel de dimension infinie sur un corps K munie d'une norme $|.|$ et A une application linéaire de V dans V. On peut aussi définir la trace de A à condition que la somme suivante converge

$$\mathrm{Tr}(A) = \sum_{i=1}^{+\infty} a_{i,i}$$

Proposition 3.40 (Formule de la trace de Dwork)**.** *Considérons $G \in R_0$, $q \in \mathbb{N}$ et $\Psi = \Psi_{q,G}$. En notant $\mathbb{U}^n_{q^s-1}(\mathbb{C}_p)$ l'ensemble des n-uplets constitués de racines (q^s-1)-ème de l'unité (où n correspond aux nombres de variables $X_1, \dots, X_n$). Alors pour tout $s \geq 1$, $\mathrm{Tr}(\Psi^s)$ converge et*

$$(q^s-1)^n \mathrm{Tr}(\Psi^s) = \sum_{x \in \mathbb{U}^n_{q^s-1}(\mathbb{C}_p)} G(x)G(x^q)G(x^{q^2}) \cdots G(x^{q^{s}-1})$$

Démonstration. Nous allons dans un premier temps démontrer la proposition pour le cas $s = 1$, puis nous verrons que nous pouvons toujours nous y ramener.

cas $s = 1$: En notant $G = \sum_{w \in \mathbb{N}^n} g_w X^w$. Par définition, on a $\Psi(X^u) = \sum_{w \in \mathbb{N}^n} g_{qw-u} X^w$. Les éléments contribuant à la trace sont ceux dont $w = u$ et donc

$$\mathrm{Tr}(\Psi) = \sum_{u \in \mathbb{N}^n} g_{(q-1)u}$$

De plus, comme $G \in R_0$, la somme ci-dessus est convergente et la trace est bien définie.

On considère maintenant le terme de droite de l'égalité. On commence par remarquer que si $(x, w) \in (\mathbb{N}^n)^2$, alors en notant (x_i, w_i) les i-ème coordonnées respectives, alors par le lemme 3.38, on a :

$$\sum_{x_i \in \mathbb{U}_{q-1}(\mathbb{C}_p)} x_i^{w_i} = \begin{cases} q-1 & \text{si } q-1 \mid w_i \\ 0 & \text{sinon} \end{cases}$$

On en déduit alors que :

$$\sum_{x \in \mathbb{U}^n_{q^s-1}(\mathbb{C}_p)} x^w = \prod_{i=1}^{n} \left(\sum_{x_i \in \mathbb{U}_{q-1}(\mathbb{C}_p)} x_i^{w_i} \right) = \begin{cases} (q-1)^n & \text{si } q-1 \mid w \\ 0 & \text{sinon} \end{cases}$$

On peut donc maintenant voir que :

$$\sum_{x \in \mathbb{U}^n_{q^s-1}(\mathbb{C}_p)} G(x) = \sum_{w \in \mathbb{N}^n} g_w \sum_{x \in \mathbb{U}^n_{q^s-1}(\mathbb{C}_p)} x^w = (q-1)^n \sum_{u \in \mathbb{N}^n} g_{(q-1)u} = (q-1)^n \,\mathrm{Tr}(\Psi)$$

cas $s > 1$: En utilisant la définition de Ψ et le lemme 3.34, on a :

$$\begin{aligned} \Psi^s &= \phi_q \circ \mu_G \circ \phi_q \circ \mu_G \circ \Psi^{s-2} \\ &= \phi_q \circ \phi_q \circ \mu_{G_q} \circ \mu_G \circ \Psi^{s-2} \\ &= \phi_{q^2} \circ \mu_{GG_q} \circ \Psi^{s-2} \\ &\vdots \end{aligned}$$

$$= \phi_{q^s} \circ \mu_{GG_q \cdots G_{q^s-1}} = \Psi_{q^s, GG_q \cdots G_{q^s-1}}$$

Or par le lemme 3.37, la série $GG_q \cdots G_{q^s-1}$ est dans R_0. Ainsi le cas $s > 1$ se réduit au cas $s = 1$, ce qui permet de conclure.

■

Le résultat suivant est vrai dans un cadre plus général, voir par exemple ce que Serre propose dans [4]. On re-démontrera celui-ci dans notre cas particulier de Dwork.

Proposition 3.41. *Soit $G \in R_0$ et $q \in \mathbb{N}$ et $\Psi = \Psi_{q,G}$. Alors la série* $\det(1 - \Psi T) \in \mathbb{C}_p[[T]]$ *est bien définie, entière et*

$$\det(1 - \Psi T) = \exp\left(- \sum_{s=1}^{+\infty} \frac{\mathrm{Tr}(\Psi^s)}{s} T^s \right)$$

Démonstration. Soit $G(X) = \sum_{w \in \mathbb{N}^n} g_w X^w \in R_0$.

* On commence par rappeler la définition du déterminant en termes de permutations, $\det(1 - \Psi T) = \sum_{j=0}^{+\infty} b_j T^j$ où $b_j = (-1)^j \sum_{\substack{u_1, \ldots, u_j \in \mathbb{N}^n \\ \sigma \in S_n}} \mathrm{sgn}(\sigma) \prod_{i=1}^{j} \Psi_{u_i, u_{\sigma(i)}}$. On a considéré ici que $\Psi_{u,w}$ correspond à l'entrée (u, w) de la matrice (infinie) de l'endomorphisme Ψ. Or comme $\Psi(X^u) = \sum_{w \in \mathbb{N}^n} g_{qw-u} X^w$, on en déduit que $\Psi_{u,w} = g_{qu-w}$.
* Comme $G \in R_0$, il existe $M > 0$ tel que pour tout $w \in \mathbb{N}$, $\mathrm{ord_p}(g_w) \geq M|w|$. On peut obtenir une estimation de la valuation p-adique de b_j. En effet :

$$\begin{aligned} \mathrm{ord_p}(g_{qu_1 - u_{\sigma(1)}} \cdots g_{qu_j - u_{\sigma(j)}}) &\geq M(|qu_{\sigma(1)} - u_1| + \cdots + |qu_{\sigma(n)} - u_j|) \\ &\geq M\left(\sum_{i=1}^{j} q|u_i| - \sum_{i=1}^{j} |u_{\sigma(i)}| \right) \\ &= M(q-1) \sum_{i=1}^{j} |u_i| \end{aligned}$$

Comme $\sum_{i=1}^{j} |u_i| \underset{n \to +\infty}{\longrightarrow} +\infty$. On en déduit donc que $\mathrm{ord_p}(b_j) \underset{n \to +\infty}{\longrightarrow} +\infty$, ce qui nous assure que le déterminant est bien défini. On a même de plus par le théorème de Césaro que $\frac{\mathrm{ord_p}(b_j)}{j} \underset{j \to +\infty}{\longrightarrow} +\infty$. On en déduit donc que $\lim_{j \to +\infty} |b_j|_p^{1/j} = 0$, et donc que $\det(1 - \Psi T)$ est entière (a un rayon de convergence infini).

* Pour prouver l'équation donnée dans la proposition, nous considérons d'abord le cas où Ψ est un endomorphisme d'un espace vectoriel de dimension d sur $\mathbb{C}_p$. On sait que le déterminant et la trace d'un endomorphisme sont invariants par changement de base, et puisque $\mathbb{C}_p$ est algébriquement clos, on peut considérer un changement de base de sorte que la matrice Ψ, par rapport à la nouvelle base, soit triangulaire supérieure. On peut donc sans perte de généralité, supposer

que Ψ est triangulaire supérieure. On peut donc écrire d'une part

$$\det(1-\Psi T)=\prod_{i=1}^{d}(1-\Psi_{i,i}T)$$

D'autre part, on a :

$$\mathrm{Tr}(\Psi^s)=\sum_{i=1}^{d}(\Psi_{i,i})^s$$

On obtient donc finalement que :

$$\begin{aligned}\exp\left(-\sum_{s=1}^{+\infty}\sum_{i=1}^{d}\frac{(\Psi_{i,i})^s}{s}T^s\right)&=\prod_{i=1}^{d}\exp\left(-\sum_{s=1}^{+\infty}\frac{(\Psi_{i,i}T)^s}{s}\right)\\&=\prod_{i=1}^{d}\exp(\log_p(1-\Psi_{i,i}T))\\&=\prod_{i=1}^{d}(1-\Psi_{i,i}T)=\det(1-\Psi T)\end{aligned}$$

* À partir de la dimension finie, on peut étendre et démontrer la proposition, c'est ce que nous allons faire dans la suite.

■

Définition 3.42. On pose pour $M>0$ fixé l'ensemble

$$R_M=\{G=\sum_{w\in\mathbb{N}^n}g_wX^w\in R\mid \mathrm{ord_p}(w)\geq M|w|\}$$

Remarque 3.43.

* R_M est un $\mathbb{Q}_p$ espace de Banach.
* $R_0=\bigcup_{M>0}R_M$.
* Le lemme 3.37 montre que si $G\in R_M$, alors $G_q\in R_{\frac{M}{q}}$.
* Si $M_2<M_1$ alors $R_{M_1}\subseteq R_{M_2}$.
* Intéressons nous à la topologie sur $\mathbb{C}_p[[T]]$. On a plusieurs topologies :
  - La topologie associée à ord_T
  - Étant donné que $\mathbb{C}_p[[T]]\simeq\mathbb{C}_p^{\mathbb{N}}$, on peut donc munir $\mathbb{C}_p[[T]]$ de la topologie produit. C'est celle-ci que nous allons considérer. Pour cette topologie, on a
$$u_n=\sum_{k=0}^{+\infty}u_{n,k}T^k\to\sum_{k=0}^{+\infty}v_kT^k\text{ ssi }\forall k,u_{n,k}\to v_k\text{pour }|.|_p$$

Dans toute la suite, on considèrera donc la topologie produit.

Lemme 3.44. *L'application* $\exp: T\mathbb{C}_p[[T]\to\mathbb{C}_p[[T]]$ *est continue.*

Démonstration. Soit $f(T)=\sum_{i\geq1}a_iT^i$ pour $a_i\in\mathbb{C}_p$, alors $\exp(f(T))=\sum_{k\geq0}\frac{f(T)^k}{k!}=\sum_{s\geq0}b(s)T^s$. Or $\mathrm{ord}_T(f(T))\geq1$, il n'y a donc à s fixé qu'un nombre fini de termes

qui intervient pour calculer $b(s)$. De plus, cela montre aussi que l'application était bien définie (*i.e.* $\exp(f(T)) \in \mathbb{C}_p[[T]]$).

Ainsi $\sum_{s\leq k} b(s)T^s = \sum_{l\leq k} \frac{f(T)^l}{l!} =: \mathcal{E}_k(T)$. Pour s fixé, l'application $f \mapsto \mathcal{E}_s(T)$ est continue (car polynomiale en f) et donc l'application $f \mapsto b(s)$ est continue. ∎

Dans la suite, on notera E_k le sous-espace vectoriel des polynômes de degré inférieur ou égal à k de $\mathbb{C}_p[T]$. On a dès lors un projecteur $p_k : \mathbb{C}_p[[T]] \to E_k$ et on pose $\Psi_{|k} := p_k \circ \Psi \circ i_k$ où $i_k : E_k \to \mathbb{C}_p[[TT]$ est l'injection canonique.

On pose enfin $\mathcal{T}(\Psi) = -\sum_{s=1}^{+\infty} \frac{\mathrm{Tr}(\Psi^s)}{s} T^s$ et $\mathcal{D}(\Psi) = \det(1 - \Psi T)$. On sait que $\mathcal{D}(\Psi_{|k})$ correspond au polynôme caractéristique de $\Psi_{|k}$ et que $\mathcal{D}(\Psi_{|k}) = \mathcal{T}(\Psi_{|k})$ par la partie de dimension finie qui précède. Pour terminer, il suffit donc de montrer que $\mathcal{D}(\Psi_{|k}) \to \mathcal{D}(\Psi) \in \mathbb{C}_p[[T]]$ quand $k \to +\infty$ (et respectivement $\mathcal{T}(\Psi_{|k}) \to \mathcal{T}(\Psi)$).

Lemme 3.45.

$$\mathcal{T}(\Psi_{|k}) \underset{k\to+\infty}{\longrightarrow} \mathcal{T}(\Psi)$$

Démonstration. Il suffit de montrer la convergence terme à terme. Or d'après la démonstration de la proposition 3.40, $\Psi^s = \Psi_{q^s, GG_q \dots G_{q^s-1}}$. Ainsi, en posant $H = G \dots G_{q^s-1}$, on a $H \in R_{\frac{M}{q^s-1}}$ par stabilité par multiplication (même preuve que pour R_0). En écrivant $H = \sum_{u\in\mathbb{N}^n} h_u X^u$, par convergence on a $\mathrm{Tr}(\Psi^s) = \sum_{u\in\mathbb{N}^n} h_{(q-1)u}$. Dès lors,

$$\mathrm{Tr}(\Psi^s) - \mathrm{Tr}(\Psi^s_{|k}) = \underbrace{\mathrm{Tr}(\Psi_s) - \mathrm{Tr}(p_k \circ \Psi^s \circ i_k)}_{=: C_1(\Psi)} + \underbrace{\mathrm{Tr}(p_k \circ \Psi^s \circ i_k) - \mathrm{Tr}(\Psi^s_{|k})}_{=: C_2(\Psi)}$$

Pour $C_1(\Psi)$: D'après le cas $s = 1$ de la proposition 3.40, on a $C_1(\Psi) = \sum_{\substack{u\in\mathbb{N}^n \\ |u|\geq k+1}} h_{(q^s-1)u}$ et $\mathrm{ord}_p(C_1(\Psi)) \geq \frac{(q^s-1)|u|M}{q^s-1} \geq M(k+1)$. Ainsi, si $k \to +\infty$, alors $C_1(\Psi) \to 0$.

Pour $C_2(\Psi)$: On a $\Psi_{u,w} = g_{qw-u} = \Psi_{|k_{u,w}}$ si $|u| \leq k$ et $|w| \leq k$.

— Comme $G \in R_M \subseteq R_0$ alors les coefficients de G sont bornés, il existe $A > 0$ tel que pour tout $u \in \mathbb{N}^n$, $\mathrm{ord}_p(g_u) \geq -A$.

— Si $|w| \geq k+1$ et $|u| \leq k$, alors :

$$\mathrm{ord}_p(\Psi_{u,w}) = \mathrm{ord}_p(g_{qw-u}) \geq \frac{q|w| - |u|}{M} \geq \frac{(q-1)k + q}{M} \geq \frac{(q-1)k}{M}$$

— On a d'une part $\Psi^s_{u,u} = \sum_{w_1,\dots,w_{s-1}\in\mathbb{N}^n} \Psi_{u,w_1}\Psi_{w_1,w_2}\dots\Psi_{w_{s-1},u}$ et respectivement d'autre part $\Psi^s_{|k_{u,u}} = \sum_{\substack{w_1,\dots,w_{s-1}\in\mathbb{N}^n \\ |w_1|\leq k,\ \dots,\ |w_{s-1}|\leq k}} \Psi_{u,w_1}\Psi_{w_1,w_2}\dots\Psi_{w_{s-1},u}$. Dès lors, en notant $\mathcal{E}_{u,u}(S)$ la différence des deux termes définis ci-dessus. On obtient :

$$\mathcal{E}_{u,u}(S) = \sum_{\substack{w_1,\dots,w_{s-1}\in\mathbb{N}^n \\ \exists i, |w_i|\geq k+1}} \Psi_{u,w_1}\Psi_{w_1,w_2}\dots\Psi_{w_{s-1},u}$$

Ainsi, pour chaque $(s-1)$-uplet de cette somme, on a $|w_1| \geq k+1$ ou alors il existe un plus petit indice vérifiant $|w_j| \leq k$ et $|w_{j+1}| \geq k+1$. On en

conclut donc par le point précédent que :

$$\mathrm{ord}_p(\Psi_{u,w_1} \dots \Psi_{w_{s-1},u}) \geq \frac{(q-1)k}{M} - (s-1)A$$

D'où finalement la même inégalité sur $\mathrm{ord}_p(\mathcal{E}_{u,u}(S))$ et donc cela nous permet de conclure que $C_2(\Psi) \to 0$ si $k \to +\infty$.

On a ainsi bien montré que $\mathcal{T}(\Psi^s_{|k}) \to \mathcal{T}(\Psi^s)$. ∎

Lemme 3.46.

$$\mathcal{D}(\Psi_{|k}) \underset{k\to+\infty}{\longrightarrow} \mathcal{D}(\Psi)$$

Démonstration. On commence par écrire $\det(1-\Psi T) = \sum_{j=0}^{+\infty} b_j T^j$ où $b_j = (-1)^j \sum_{\substack{u_1,\dots,u_j\in\mathbb{N}^n \\ \sigma\in S_j}} \varepsilon(\sigma) \prod_{i=1}^{j} \Psi_{u_i,u_{\sigma(i)}}$.

De même, on a $\det(1-\Psi_{|kT}) = \sum_{j=0}^{+\infty} b_{j,k} T^j$ où $b_{j,k} = (-1)^j \sum_{\substack{u_1,\dots,u_j\in\mathbb{N}^n \\ |u_1|\leq k,\ \dots,\ |u_j|\leq k \\ \sigma\in S_j}} \varepsilon(\sigma) \prod_{i=1}^{j} \Psi_{u_i,u_{\sigma(i)}}$.

Ainsi en considérant la différence des deux, on obtient :

$$\det(1-\Psi T) - \det(1-\Psi_{|k}T) = \sum_{j=0}^{+\infty} \gamma_{j,k} T^j$$

où $\gamma_{j,k} = (-1)^j \sum_{\substack{u_1,\dots,u_j\in\mathbb{N}^n \\ \exists i, |u_i|\geq k+1 \\ \sigma\in S_j}} \varepsilon(\sigma) \prod_{i=1}^{j} \Psi_{u_i,u_{\sigma(i)}}$.

Comme $\Psi_{u_i,u_{\sigma(i)}} = g_{qu_i-u_{\sigma(i)}}$, on obtient ainsi comme précédemment que

$$\mathrm{ord}_p(\gamma_{j,k}) \geq M(q-1) \sum_{j=1}^{i} |u_j| \geq M(q-1)(k+1+(i-1) = M(q-1)(k+i)$$

Ainsi quand $k \to +\infty$, on peut conclure que $\mathcal{D}(\Psi_{|k}) \to \mathcal{D}(\Psi)$. ∎

3.3.4 Relèvement de caractères $\mathbb{C}_p$-valués

Définition 3.47. Soit G un groupe fini et K un corps. On appelle caractère $K-$valué de G tout homomorphisme $\varphi : G \to K^\times$.

Remarque 3.48.

- Du théorème de Lagrange et de la définition d'un caractère, on obtient que $\mathrm{Im}(\varphi)$ est inclus dans l'ensemble des racines de l'unité de $K^\times$.
- Si L/K est une extension de corps et $\alpha \in L$ tel que $[K(\alpha) : K] = m$ et $[L : K(\alpha)] = n$. On rappelle que la trace de α de L sur K est

$$\mathrm{Tr}_{L/K}(\alpha) = n \sum_{i=1}^{m} \alpha_i$$

où les α_i sont les conjugués de α sur K. De plus, si L/K est galoisienne alors

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha)$$

* Dans le cas de $L = \mathbb{F}_q$ avec $q = p^s$ et $K = \mathbb{F}_p$, on sait qu'il y a $s = [\mathbb{F}_q : \mathbb{F}_p]$ automorphismes $\sigma_0, \ldots, \sigma_{s-1}$ de $\mathbb{F}_q$ donné par $\sigma_i(a) = a^{p^i}$ pour $a \in \mathbb{F}_q$. Ainsi, si $a \in \mathbb{F}_q$, alors

$$\mathrm{Tr}(a) = \sum_{i=0}^{s-1} a^{p^i}$$

Proposition 3.49. *Soit $\omega \in \mathbb{C}_p$ une racine p-ème de l'unité et $q = p^s$. Alors l'application*

$$\begin{array}{rccc} \varphi : & \mathbb{F}_q & \to & (\mathbb{C}_p)^\times \\ & a & \mapsto & \omega^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)} \end{array}$$

est bien définie et est un caractère $\mathbb{C}_p$-valué non-trivial du groupe additif de $\mathbb{F}_q$. L'exposant $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)$ doit être compris au sens du plus petit résidu positif entier.

Démonstration. On a tout d'abord que $\mathbb{F}_q/\mathbb{F}_p$ est galoisienne de groupe de galois $G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ engendré par le morphisme de Frobenius $x \mapsto x^p$. On a donc :

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)^p = \left(\sum_{\sigma \in G} \sigma(a)\right)^p = \sum_{\sigma \in G} \sigma(a)^p = \sum_{\sigma \in G} \sigma(a) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)$$

Comme chaque $\sigma \in G$ est une puissance du Frobenius, on voit que $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)$ est fixée par tout les éléments de G. Ainsi, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) \in \mathbb{F}_p$. De plus, comme le Frobenius et toutes ses puissances sont des homomorphismes, on voit que pour tout $(a, b) \in \mathbb{F}_q$:

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a+b) = \sum_{\sigma \in G} \sigma(a+b) = \sum_{\sigma \in G} (\sigma(a) + \sigma(b)) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) + \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(b)$$

On obtient ainsi que φ est un homomorphisme de $\mathbb{F}_q$ dans $(\mathbb{C}_p)^\times$, c'est à dire que φ est un caractère $\mathbb{C}_p$-valué du groupe additif de $\mathbb{F}_q$. ∎

Remarque 3.50. On rappelle que pour tout $a \in \mathbb{F}_q$ où $q = p^s$, il existe un unique représentant multiplicatif de a donné par $\tau_s(a)$ (relèvement multiplicatif) dans une extension non-ramifiée K de $\mathbb{Q}_p$ engendré par une racine $(p^s - 1)$-ème primitive de l'unité satisfaisant

$$\tau_s(a)^p = \tau_s(a) \text{ et } \tau_s(a) = a \mod [p\mathcal{O}_K]$$

Comme K est le corps de décomposition du q-ème polynôme cyclotomique sur $\mathbb{Q}_p$, alors $K/\mathbb{Q}_p$ est galoisien. Notons $G = \mathrm{Gal}(K/\mathbb{Q}_p)$, on obtient que

$$\mathrm{Tr}_{K/\mathbb{Q}_p}(\tau_s(a)) = \sum_{\sigma \in G} \sigma(\tau_s(a)) \in \mathcal{O}_K$$

En réduisant alors modulo p, et le fait que $\tau_s(a) = a \mod [p\mathcal{O}_K]$ on obtient que :

$$\mathrm{Tr}_{K/\mathbb{Q}_p}(\tau_s(a)) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) \mod [p\mathcal{O}_K]$$

Ainsi, étant donné une racine p-ème de l'unité ω, on obtient que

$$\omega^{\mathrm{Tr}_{K/\mathbb{Q}_p}(\tau_s(a))} = \omega^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}$$

On chercher une série entière p-adique $\Theta(T) \in \mathbb{C}_p[[T]]$ satisfaisant $\Theta(\tau_s(a)) = \omega^a$. Si l'on arrive à trouver une telle série, on pourra alors retrouver le caractère de la trace comme suit :

$$\Theta(\tau_s(a))\Theta(\tau_s(a)^p)\cdots\Theta(\tau_s(a)^{p^{s-1}}) = \omega^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}$$

On appellera pour la suite Θ un relèvement du caractère φ à une fonction de $\mathbb{C}_p$.

Théorème 3.51. *Soit ω une racine p-ème de l'unité et notons $\lambda = \omega - 1$, et notons φ le caractère de la proposition 3.49, alors la série entière p-adique suivante est un relèvement du caractère φ à une fonction de $\mathbb{C}_p$*

$$\Theta(T) = F(T,\lambda) = (1+\lambda)^T(1+\lambda^p)^{(T^p-T)/p}(1+\lambda^{p^2})^{(T^{p^2}-T^p)/p^2}\cdots$$

Démonstration. On commence par rappeler qu'on a vu dans le chapitre 1 que $F(X,Y) \in \mathbb{Z}_p[[X,Y]]$. De plus, on considère $F(X,Y)$ comme une série en X avec Y fixé :

$$F(X,Y) = \sum_{n=0}^{+\infty}\left(\sum_{m=n}^{+\infty} a_{m,n}Y^m\right)X^n \quad \text{avec } a_{m,n} \in \mathbb{Z}_p$$

En substituant T à X et λ à Y, on obtient que $\Theta(T) = \sum\limits_{n=0}^{+\infty} a_n T^n$ avec $a_n = \sum\limits_{m=n}^{+\infty} a_{m,n}\lambda^m$. On obtient en utilisant le lemme 1.17 à ω que

$$\mathrm{ord_p}(a_n) = \mathrm{ord_p}\left(\sum_{m=n}^{+\infty} a_{m,n}\lambda^m\right) \geq \mathrm{ord_p}(\lambda^n) = \mathrm{ord_p}((\omega-1)^n) = n\,\mathrm{ord_p}(\omega-1) = \frac{n}{p-1}$$

On obtient donc que $\Theta(T) \in \mathbb{C}_p[[T]]$ converge au moins sur le disque $D(p^{-1/(p-1)-})$.

Si $\tau = \tau_s(a) \in \mathbb{C}_p$ est le représentant multiplicatif de $a \in \mathbb{F}_{p^s}$ dans $\mathbb{C}_p$, alors

$$\begin{aligned}
\prod_{i=1}^{p^{s-1}}\Theta(\tau^i) &= \prod_{i=1}^{p^{s-1}}(1+\lambda)^{\tau^i}(1+\lambda^p)^{(\tau^{pi}-\tau^i)/p}\cdots \\
&= (1+\lambda)^{\tau+\tau^p+\cdots+\tau^{p^{s-1}}}(1+\lambda^p)^{(\tau^{p^s}-\tau)/p}(1+\lambda^{p^2})^{(\tau^{p^{s+1}}-\tau^p)/p^2}\cdots \\
&= (1+\lambda)^{\tau+\tau^p+\cdots+\tau^{p^{s-1}}} \quad \text{car } \tau^{p^s} = \tau \\
&= \omega^{\mathrm{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(a)}
\end{aligned}$$

On a donc bien obtenue que Θ est un relèvement du caractère φ à une fonction de $\mathbb{C}_p$. ∎

Maintenant que nous avons construit le relèvement, on montre qu'il donne lieu à une série entière de R_0 et qu'on peut donc appliquer les résultats de la section précédente.

Proposition 3.52. *Soit $w \in \mathbb{N}^n$ et $a \in D(1)$, alors $\Theta(aX^w) \in R_0$.*

Démonstration. La preuve du théorème précédent nous a assuré que $\Theta(T) = \sum_{i=0}^{+\infty} b_i T^i$ avec $\mathrm{ord_p}(b_i) \geq \frac{i}{p-1}$. Alors, en considérant $\Theta(aX_1^{w_1} \dots X_n^{w_n}) = \sum_{i=0}^{+\infty} b_i a^i X_1^{iw_1} \dots X_n^{iw_n}$, avec les notations des sections précédentes, on obtient

$$\mathrm{ord_p}(g_{iw}) = \mathrm{ord_p}(b_i a^i) \geq \mathrm{ord_p}(b_i) \geq \frac{i}{p-1} = \frac{i|w|}{|w|(p-1)} = M|iw|$$

où $M = \frac{1}{|w|(p-1)}$. On obtient donc que $\Theta(aX^w) \in R_0$. ∎

3.3.5 Méromorphie de la fonction zêta

Nous allons maintenant montrer dans cette sous-section que la fonction zêta est p-adiquement méromorphe à l'aide des résultats des deux sous-sections précédentes.

Lemme 3.53. *Soit $\varphi : \mathbb{F}_{q^s} \to (\mathbb{C}_p)^\times$ un caractère $\mathbb{C}_p$-valué non-trivial du groupe additif de $\mathbb{F}_{q^s}$. Alors, $\sum_{x \in \mathbb{F}_{q^s}} \varphi(x) = 0$.*

Démonstration. En effet, comme φ est non-trivial, il existe $x_0 \in \mathbb{F}_{q^s}$ tel que $\varphi(x_0) \neq 1$. Alors, en effectuant le changement de variable $y = x - x_0$, on obtient

$$\sum_{x \in \mathbb{F}_{q^s}} \varphi(x) = \sum_{y \in \mathbb{F}_{q^s}} \varphi(y + x_0) = \varphi(x_0) \sum_{y \in \mathbb{F}_{q^s}} \varphi(y)$$

On en déduit donc comme $\varphi(x_0) \neq 1$ que $\sum_{x \in \mathbb{F}_{q^s}} \varphi(x) = 0$. ∎

Lemme 3.54. *Soit ω une racine p-ème de l'unité dans $\mathbb{C}_p$, alors en considérant le caractère $\mathbb{C}_p$-valué de $\mathbb{F}_{q^s}$ suivant étudié plutôt :*

$$\begin{array}{rccc} \varphi : & \mathbb{F}_{q^s} & \to & (\mathbb{C}_p)^\times \\ & x & \mapsto & \omega^{\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(x)} \end{array}$$

Alors

$$\sum_{x \in \mathbb{F}_{q^s}} \varphi(xu) = \begin{cases} 0 & si\ u \in (\mathbb{F}_{q^s})^\times \\ q^s & si\ u = 0 \end{cases}$$

Démonstration.

* Si $u = 0$, alors pour tout $x \in \mathbb{F}_{q^s}$, $\varphi(xu) = 1$. On obtient ainsi $\sum_{x \in \mathbb{F}_{q^s}} \varphi(xu) = q^s$.
* Sinon, on reprend la preuve du lemme précédent, comme φ est un caractère $\mathbb{C}_p$ valué non trivial, il existe $x_0 \in \mathbb{F}_{q^s}$ tel que $\varphi(x_0) \neq 1$. Mais, comme u est inversible, en considérant le changement de variable $y = x - x_0 u^{-1}$, on obtient ainsi
$$\sum_{x \in \mathbb{F}_{q^s}} \varphi(xu) = \varphi(x_0) \sum_{y \in \mathbb{F}_{q^s}} \varphi(yu)$$
et finalement $\sum_{x \in \mathbb{F}_{q^s}} \varphi(xu) = 0$.

∎

Proposition 3.55. *Soit H_f une hypersurface affine définie par $f \in \mathbb{F}_q[X_1, \dots, X_n]$, alors la fonction zêta $Z(H_f/\mathbb{F}_q; T) \in \mathbb{Z}[[T]] \subseteq \mathbb{C}_p[[T]]$ est p-adiquement méromorphe.*

Démonstration. Procédons par récurrence sur n le nombre d'indéterminées définissant f.

$\underline{n = 0 :}$ L'hypersurface sur $\mathbb{F}_q$ consiste en un unique point et sa fonction zêta est donnée par

$$Z(H_f/\mathbb{F}_q; T) = \exp\left(\sum_{s=1}^{+\infty} \frac{T^s}{s}\right) = \exp(-\log(1-T)) = \frac{1}{1-T}$$

qui est p-adiquement méromorphe.

$\underline{k \leq n-1 :}$ On suppose l'assertion vrai pour toute hypersurface affine définie via f en $k \leq n-1$ variables. On définit l'ensemble suivant

$$\begin{aligned} N'_s &= \text{Card}\left(\left\{(x_1, \dots, x_n) \in \mathbb{F}_{q^s}, f(x_1, \dots, x_n) = 0 \text{ et } \forall i \in \{1, \dots, n\}, x_i \neq 0\right\}\right) \\ &= \text{Card}\left(\left\{(x_1, \dots, x_n) \in \mathbb{F}_{q^s}, f(x_1, \dots, x_n) = 0 \text{ et } \forall i \in \{1, \dots, n\}, x_i^{q^s-1} = 1\right\}\right) \end{aligned}$$

On commence par montrer que pour conclure, on peut réduire la p-adique méromorphie de $Z(H_f/\mathbb{F}_q; T)$ à celle de

$$Z'(H_f/\mathbb{F}_q; T) := \exp\left(\sum_{s=1}^{+\infty} \frac{N'_s}{s} T^s\right)$$

En effet, on peut tout d'abord écrire que

$$Z(H_f/\mathbb{F}_q; T) = Z'(H_f/\mathbb{F}_q; T) \exp\left(\sum_{s=1}^{+\infty} \frac{(N_s - N'_s)}{s} T^s\right)$$

Or en notant $H_i = \left\{(x_1, \dots, x_n) \in H_f, x_i = 0\right\}$, qui est une hypersurface affine de $\mathbb{A}^{n-1}_{\mathbb{F}_q}$, on obtient que :

$$\begin{aligned} N_s - N'_s &= \text{Card}\left(\bigcup_{i=1}^{n} H_i(\mathbb{F}_{q^s})\right) \\ &= \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \text{Card}(H_{i_1}(\mathbb{F}_{q^s}) \cap \cdots \cap H_{i_k}(\mathbb{F}_{q^s}))\right) \end{aligned}$$

Or $H_i \cap H_j$ est une hypersurface affine de $\mathbb{A}^{n-2}_{\mathbb{F}_q}$, et de même en intersectant d'avantage, en réduisant le $n-2$. On obtient ainsi par hypothèse de récurrence que

$$\begin{aligned} \exp\left(\sum_{s=1}^{+\infty} \frac{(N_s - N'_s)}{s} T^s\right) &= \prod_{k=1}^{n} \left(\prod_{1 \leqslant i_1 < \cdots < i_k \leqslant n} Z(H_{i_1} \cap \cdots \cap H_{i_k}/\mathbb{F}_q; T)\right)^{(-1)^{k+1}} \\ &= \frac{\prod_{i=1}^{n} Z(H_i/\mathbb{F}_q; T) \cdot \prod_{i<j<k} Z(H_i \cap H_j \cap H_k/\mathbb{F}_q; T) \cdots}{\prod_{i<j} Z(H_i \cap H_j/\mathbb{F}_q; T)} \end{aligned}$$

est p-adiquement méromorphe. On a donc observé qu'il suffisait de montrer la p-adique méromorphie de $Z'(H_f/\mathbb{F}_q; T)$ pour pouvoir conclure, c'est ce que

nous allons donc montrer maintenant.

Pour ce faire, fixons un entier $s \geq 1$ et $q = p^r$ pour $r \geq 1$. Considérons $a \in \mathbb{F}_{q^s}$ et $\tau = \tau_s(a)$ son représentant multiplicatif dans $\mathbb{C}_p$. Étant donné une racine p-ème de l'unité ω, nous avons vu par le théorème 3.51 qu'il existe Θ un relèvement du caractère φ à une fonction de $\mathbb{C}_p$, *i.e.*

$$\Theta(\tau)\Theta(\tau^p)\cdots\Theta(\tau^{p^{rs-1}}) = \omega^{\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(a)}$$

Or, par le lemme 3.54, en enlevant le terme $x_0 = 0$, on obtient l'égalité

$$\sum_{x_0 \in (\mathbb{F}_{q^s})^\times} \omega^{\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(x_0 u)} = \begin{cases} -1 & \text{si } u \in (\mathbb{F}_{q^s})^\times \\ q^s - 1 & \text{si } u = 0 \end{cases}$$

En appliquant cette égalité à $u = f(x_1, x_2, \ldots, x_n)$ où f est le polynôme définissant H_f, et en sommant sur toutes les $(x_1, \ldots, x_n) \in (\mathbb{F}_{q^s}^\times)^n$, on obtient donc

$$\begin{aligned}
\sum_{\substack{(x_1,\ldots,x_n)\in(\mathbb{F}_{q^s}^\times)^n \\ x_0\in(\mathbb{F}_{q^s})^\times}} \omega^{\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(x_0 f(x_1,\ldots,x_n))} &= \sum_{\substack{(x_1,\ldots,x_n)\in N_s' \\ x_0\in(\mathbb{F}_{q^s})^\times}} \omega^{\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(x_0 f(x_1,\ldots,x_n))} \\
&\quad + \sum_{\substack{(x_1,\ldots,x_n)\in(\mathbb{F}_{q^s}^\times)^n\setminus N_s' \\ x_0\in(\mathbb{F}_{q^s})^\times}} \omega^{\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(x_0 f(x_1,\ldots,x_n))} \\
&= (q^s-1)N_s' + ((q^s-1)^n - N_s')(-1) \\
&= q^s N_s' - (q^s-1)^n
\end{aligned}$$

Notons $F(X_0, X_1, \ldots, X_N) = X_0 f(X_1, \ldots, X_n) \in \mathbb{C}_p[X_0, X_1, \ldots, X_n]$ où les coefficients de $\mathbb{F}_q$ ont été remplacés par leur représentants multiplicatifs dans $\mathbb{C}_p$. En écrivant $F(X_0, X_1, \ldots, X_n) = \sum_{i=1}^{N} a_i X^{w_i}$, on obtient

$$\begin{aligned}
q^s N_s' &= (q^s-1)^n + \sum_{\substack{(x_1,\ldots,x_n)\in N_s' \\ x_0\in(\mathbb{F}_{q^s})^\times}} \omega^{\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(x_0 f(x_1,\ldots,x_n))} \\
&= (q^s-1)^n + \sum_{\substack{x\in\mathbb{N}^{n+1} \\ x^{q^s-1}=1}} \prod_{i=1}^{N} \Theta(a_i x^{w_i})\Theta(a_i^p x^{w_i p})\cdots\Theta(a_i^{p^{rs-1}} x^{w_i p^{rs-1}}) \\
&= (q^s-1)^n + \sum_{\substack{x\in\mathbb{N}^{n+1} \\ x^{q^s-1}=1}} G(x)G(x^q)\cdots G(x^{q^s-1})
\end{aligned}$$

où $G(X_0, X_1, \ldots, X_n) = \prod_{i=1}^{N} \Theta(a_i X^{w_i})\Theta(a_i^p X^{w_i p})\cdots\Theta(a_i^{p^{r-1}} X^{w_i p^{r-1}})$. Comme les a_i sont des représentants multiplicatifs de $\mathbb{F}_{q^s}$, ils sont en particulier dans $D(1)$, on en déduit donc par la proposition 3.52 que $\Theta(a_i^k X^{w_i p^k}) \in R_0$, et comme cet ensemble est stable par multiplication, on en déduit que $G \in R_0$. Dès lors, en utilisant la proposition 3.40 (formule de la trace de Dwork) appliqué à G, on en

déduit que

$$q^s N'_s = (q^s - 1)^n + (q^s - 1)^{n+1} \operatorname{Tr}(\Psi^s)$$

On peut donc maintenant diviser par q^s et appliquer le binôme de Newton pour obtenir l'égalité suivante :

$$N'_s = \sum_{i=0}^{n} \binom{n}{i} (-1)^i q^{s(n-i-1)} + \sum_{i=0}^{n+1} \binom{n+1}{i} (-1)^i q^{s(n-i)} \operatorname{Tr}(\Psi^s)$$

Maintenant en utilisant la proposition 3.41, et en notant

$$\Delta(T) := \det(1 - \Psi T) = \exp\left(- \sum_{s=1}^{+\infty} \frac{\operatorname{Tr}(\Psi^s)}{s} T^s \right)$$

On peut finalement conclure que

$$\begin{aligned}
Z'(H_f/\mathbb{F}_q; T) &= \exp\left(\sum_{s=1}^{+\infty} \frac{N'_s}{s} T^s \right) \\
&= \prod_{i=0}^{n} \left[\exp\left(\sum_{s=1}^{+\infty} \frac{q^{s(n-i-1)}}{s} T^s \right) \right]^{(-1)^i \binom{n}{i}} \cdot \prod_{i=0}^{n+1} \left[\exp\left(\sum_{s=1}^{+\infty} \frac{q^{s(n-i)} \operatorname{Tr}(\Psi^s)}{s} T^s \right) \right]^{(-1)^i \binom{n+1}{i}} \\
&= \prod_{i=0}^{n} \left[\exp(-\log(1 - q^{n-i-1} T)) \right]^{(-1)^i \binom{n}{i}} \cdot \prod_{i=0}^{n+1} \left[\Delta(q^{n-i} T) \right]^{(-1)^i \binom{n+1}{i}} \\
&= \prod_{i=0}^{n} \left[1 - q^{n-i-1} T \right]^{(-1)^i \binom{n}{i}} \cdot \prod_{i=0}^{n+1} \left[\Delta(q^{n-i} T) \right]^{(-1)^i \binom{n+1}{i}}
\end{aligned}$$

Chaque terme du produit est p-adiquement méromorphe, ce qui nous permet donc de conclure que la fonction zêta est elle-même p-adiquement méromorphe.

■

3.3.6 Rationalité de la fonction zêta

Théorème 3.56 (Dwork). *Étant donné une hypersurface affine H_f sur un corps fini $\mathbb{F}_q$, la fonction zêta de H_f est un quotient de polynômes à coefficients dans $\mathbb{Q}$.*

Démonstration. Nous allons appliquer le théorème 3.9 de Borel-Dwork. On considère ici $K = \mathbb{Q}$ et on va appliquer le théorème à la fonction zêta. On considère la partie finie $P_1(\mathbb{Q}) = \{p\mathbb{Z}\}$ de $\operatorname{Spec}(\mathbb{Z})$, et vérifions les hypothèses du théorème :

i) Soit p_1 un nombre premier différent de p, alors pour tout $n \geq 0$, comme les coefficients de zêta sont entiers par le lemme 3.31, on a $|a_n|_{p_1} \leq 1$.

ii) Il n'y a qu'une place infinie de $\mathbb{Q}$, c'est la norme usuelle $|.|$, alors en considérant $R_1 = \frac{1}{q^n} = \frac{1}{p^{sn}}$, par la remarque 3.33, on obtient que zêta définit une fonction holomorphe donc méromorphe dans le disque ouvert de centre 0 et de rayon R_1.

iii) Étant donné $p\mathbb{Z} \in P_1(\mathbb{Q})$, nous avons vu que la fonction zêta définit une fonction p-adiquement méromorphe donc en particulier sur un disque ouvert de centre 0 et de rayon $R_p > p^{sn}$.

iv) Le produit R=$R_p \times R_1$ vérifie bien $R > 1$.

Ainsi par le théorème 3.9 de Borel-Dwork, on obtient que la fonction zêta est une fraction ractionnelle. ■

Corollaire 3.57. *Étant donne $\tilde{H}_{\tilde{f}}$ une hypersurface projective sur un corps fini $\mathbb{F}_q$, la fonction zêta $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ de H_f est un quotient de polynômes à coefficients dans $\mathbb{Q}$.*

Démonstration. Procédons par récurrence sur n le nombre d'indéterminées définissant $\tilde{f}$.

$\underline{n = 0}$: Si $\tilde{f} = a$, alors $\tilde{H}_{\tilde{f}}$ est soit vide, soit réduit à un point. Onn a donc dès lors que $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ est rationnelle.

$\underline{n > 1}$: Supposons l'assertion vraie au rang n et montrons qu'elle persiste au rang $n+1$. On considère ainsi $\tilde{f}$ un polynôme en n indéterminées, homogène de degré d, et on considère, $f \in K[X_1, \dots, X_n]$ tel que pour tout $[u_0, u_1, \dots, u_n] \in \mathbb{P}^n_K$, $\tilde{f}(u_0, u_1, \dots, u_n) = f(\frac{u_1}{u_0}, \dots, \frac{u_n}{u_0}) \cdot u_0^d$. On peut écrire :

$$\begin{aligned}
\tilde{H}_{\tilde{f}} &= \{[u_0, \dots, u_n] \in \mathbb{P}^n_K, \tilde{f}(u_0, u_1, \dots, u_n) = 0\} \\
&= \{[0, u_1, \dots, u_n] \in \mathbb{P}^n_K, \tilde{f}(0, u_1, \dots, u_n) = 0\} \cup \{[1, u_1, \dots, u_n] \in \mathbb{P}^n_K, \tilde{f}(1, u_1, \dots, u_n) = 0\} \\
&= \{[u_1, \dots, u_n] \in \mathbb{P}^{n-1}_K, \tilde{f}(0, u_1, \dots, u_n) = 0\} \cup \{[1, u_1, \dots, u_n] \in \mathbb{P}^n_K, f(u_1, \dots, u_n) = 0\} \\
&= \tilde{H}_{\tilde{f}_{|\mathbb{P}^{n-1}_K}} \cup \{(x_1, \dots, x_n) \in \mathbb{A}^n_K, f(x_1, \dots, x_n) = 0\} \\
&= \tilde{H}_{\tilde{f}_{|\mathbb{P}^{n-1}_K}} \cup H_f
\end{aligned}$$

On obtient ainsi que :

$$\begin{aligned}
Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T) &= Z(\tilde{H}_{\tilde{f}_{|\mathbb{P}^{n-1}_K}} \cup H_f/\mathbb{F}_q; T) \\
&= Z(\tilde{H}_{\tilde{f}_{|\mathbb{P}^{n-1}_K}}/\mathbb{F}_q; T) Z(H_f/\mathbb{F}_q; T)
\end{aligned}$$

Or, d'une part, on a H_f qui est une hypersurface affine, donc par le théorème 3.56 de Dwork, on obtient que $Z(H_f/\mathbb{F}_q; T)$ est rationnelle. D'autre part, par hypothèse de récurrence, $Z(\tilde{H}_{\tilde{f}_{|\mathbb{P}^{n-1}_K}}/\mathbb{F}_q; T)$ est rationnelle. Ainsi $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q; T)$ est rationnelle, ce qui achève la récurrence.

■

3.4 Extension aux variétés affines/projectives

Définition 3.58. Soit K un corps et $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ des polynômes. On définit la variété affine définie par $f_1, \dots, f_m$ dans $\mathbb{A}^n_K$ comme étant l'ensemble suivant :

$$H_{f_1,\dots,f_m} = \left\{(x_1, \dots, x_n) \in \mathbb{A}^n_K,\ \forall 1 \leq i \leq n, f_i(x_1, \dots, x_n) = 0\right\} = \bigcap_{i=1}^{m} H_{f_i}$$

Définition 3.59. Comme précédemment, étant donné $H_{f_1,\dots,f_m}$ une variété affine, on définit

* $N_s := H_{f_1,\dots,f_m}(\mathbb{F}_{q^s})$ le nombre de points de $\mathbb{F}_{q^s}$ de $H_{f_1,\dots,f_m}$.

* La fonction zêta d'une variété affine comme étant :

$$Z(H_{f_1,\dots,f_m}/\mathbb{F}_q;T) := \exp\left(\sum_{s=1}^{+\infty}\frac{N_s}{s}T^s\right)$$

Proposition 3.60. *Étant donné une variété affine sur un corps fini $\mathbb{F}_q$, la fonction zêta de $H_{f_1,\dots,f_m}$ est une fraction rationnelle.*

Démonstration. Procédons par récurrence sur m le nombre de polynômes définissant la variété affine :

$\underline{m=1}$: On est donc ramené à une hypersurface affine associée à f_1. Or par le théorème 3.56 de Dwork, la fonction zêta est une fraction rationnelle.

$\underline{k \leq m-1}$: Supposons l'assertion vraie pour toute variété affine définie par au plus $m-1$ polynômes et vérifions qu'elle persiste pour les variétés affines définie par m polynômes.
Étant donné $H_{f_1,\dots,f_m}$ une variété affine définie par m polynômes, on sait tout d'abord que :

$$\begin{aligned}
\mathrm{Card}\left(\bigcup_{i=1}^{m}H_{f_i}(\mathbb{F}_{q^s})\right) &= \sum_{k=1}^{m}(-1)^{k+1}\left(\sum_{1\leqslant i_1<\cdots<i_k\leqslant m}\mathrm{Card}(H_{f_{i_1}}(\mathbb{F}_{q^s})\cap\cdots\cap H_{f_{i_k}}(\mathbb{F}_{q^s}))\right)\\
&= \sum_{k=1}^{m-1}(-1)^{k+1}\left(\sum_{1\leqslant i_1<\cdots<i_k\leqslant m-1}\mathrm{Card}(H_{f_{i_1}}(\mathbb{F}_{q^s})\cap\cdots\cap H_{f_{i_k}}(\mathbb{F}_{q^s}))\right)\\
&\quad+(-1)^{m+1}\mathrm{Card}(H_{f_1}(\mathbb{F}_{q^s})\cap\cdots\cap H_{f_m}(\mathbb{F}_{q^s}))\\
&= \sum_{k=1}^{m-1}(-1)^{k+1}\left(\sum_{1\leqslant i_1<\cdots<i_k\leqslant m-1}\mathrm{Card}(H_{f_{i_1}}(\mathbb{F}_{q^s})\cap\cdots\cap H_{f_{i_k}}(\mathbb{F}_{q^s}))\right)\\
&\quad+(-1)^{m+1}\mathrm{Card}(H_{f_1,\dots,f_m}(\mathbb{F}_{q^s}))
\end{aligned}$$

Or, $\bigcup_{i=1}^{m}H_{f_i}(\mathbb{F}_{q^s})$ correspond à l'hypersurface affine $H_{f_1f_2\dots f_m}$. On peut donc écrire le nombre de points de $H_{f_1,\dots,f_m}$ comme étant le nombre de points d'hypersurfaces et de variétés de dimension strictement inférieure à m. Alors par hypothèse de récurrence, et par le théorème 3.56 de Dwork, on en déduit que la fonction zêta de $H_{f_1,\dots,f_m}$ s'écrit comme produit de fonction zêta qui sont des fractions rationnelles. Plus précisément,

$$Z(H_{f_1,\dots,f_m}/\mathbb{F}_q;T) = \frac{Z(H_{f_1f_2\dots f_m}/\mathbb{F}_q;T)^{(-1)^{m+1}}}{\prod_{k=1}^{m-1}\left(\prod_{1\leq i_1<\cdots<i_k\leq m-1}Z(H_{f_{i_1},\dots,f_{i_k}}/\mathbb{F}_q;T)\right)^{(-1)^{m+k+2}}}$$

Ainsi $H_{f_1,\dots,f_m}$ est une fraction rationnelle. ∎

Définition 3.61. Soit K un corps et $\tilde{f}_1,\dots,\tilde{f}_m \in K[X_0,X_1,\dots,X_n]$ polynômes homogènes. On définit la variété affine projective définie par $\tilde{f}_1,\dots,\tilde{f}_m$ dans $\mathbb{P}^n_K$ comme étant l'ensemble suivant :

$$\tilde{H}_{\tilde{f}_1,\dots,\tilde{f}_m} = \left\{[x_0,x_1,\dots,x_n]\in\mathbb{P}^n_K, \forall 1\leq i\leq m, \tilde{f}_i(x_0,\dots,x_n)=0\right\} = \bigcap_{i=1}^{m}\tilde{H}_{\tilde{f}_i}$$

Définition 3.62. Comme précédemment, étant donné $\tilde{H}_{\tilde{f}_1,\dots,\tilde{f}_m}$ une variété projective, on définit

* $\tilde{N}_s := \tilde{H}_{\tilde{f}_1,\dots,\tilde{f}_m}(\mathbb{F}_{q^s})$ le nombre de points de $\mathbb{F}_{q^s}$ de $\tilde{H}_{\tilde{f}_1,\dots,\tilde{f}_m}$.
* La fonction zêta d'une variété projective comme étant :

$$Z(\tilde{H}_{\tilde{f}_1,\dots,\tilde{f}_m}/\mathbb{F}_q;T) := \exp\left(\sum_{s=1}^{+\infty}\frac{\tilde{N}_s}{s}T^s\right)$$

Proposition 3.63. *Étant donné une variété projective sur un corps fini $\mathbb{F}_q$, la fonction zêta de $\tilde{H}_{\tilde{f}_1,\dots,\tilde{f}_m}$ est une fraction rationnelle.*

Démonstration. On effectue la preuve par récurrence sur m le nombre de polynômes homogènes définissant la variété projective. C'est exactement la même preuve que pour les variétés affines mais en utilisant cette fois le corollaire 3.57 sur les hypersurfaces projectives. ■

Bibliographie

[1] Yvette Amice. *Les nombres p-adiques*. French. Collection SUP. Le mathematicien. 14. Paris : Presses Universitaires de Frances. 189 p. (1975). 1975.

[2] Bernard Dwork. « On the rationality of the zeta function of an algebraic variety ». English. In : *Am. J. Math.* 82 (1960), p. 631-648. issn : 0002-9327. doi : 10.2307/2372974.

[3] Neal Koblitz. *P-adic numbers, p-adic analysis, and zeta-functions*. English. T. 58. Grad. Texts Math. Springer, Cham, 1977.

[4] Jean-Pierre Serre. « Endomorphismes complètement continus des espaces de Banach *p*-adiques ». fr. In : *Publications Mathématiques de l'IHÉS* 12 (1962), p. 69-85. url : http://www.numdam.org/item/PMIHES_1962__12__69_0/.

[5] Jean-Pierre Serre. « Rationalité des fonctions ζ des variétés algébriques ». fr. In : *Séminaire Bourbaki : années 1958/59 - 1959/60, exposés 169-204*. Séminaire Bourbaki 5. talk :198. Société mathématique de France, 1960, p. 415-425. url : http://www.numdam.org/item/SB_1958-1960__5__415_0/.