Università degli Studi di Padova

Dipartimento Di Matematica "Tullio Levi-Civita"

Corso Di Laurea Magistrale in Master in Mathematics

Rationality Of Zeta-Functions For Algebraic Varieties Over Finite Fields

Supervisor
Prof. Olivier Brinon
University of Bordeaux

Master Candidate
Fandeferana Tsirimihanta
N: 1161830

27 September 2019

Abstract

Let p a prime number, q a power of p and V a scheme of finite type over $\mathbb{F}_q$. In this thesis we present Dwork's proof of the rationality of zeta function of V. It is based on methods of p-adic analysis.

Contents

1 Introduction

1.1 Objective

The study of zeta functions is very important, some applications of zeta functions are in number theory, in algebraic geometry and also in physics.

There is a long list of zeta functions, most of them are analogous to the **Riemann zeta function**:

$$\zeta(s) = \sum_{s=0}^{\infty} \frac{1}{n^s},$$

where s is a complex variable. In this work we are precisely interested in zeta functions which are analogous to Riemann zeta function.

Definition 1.1.1. Let K be a field. A scheme of finite type over K is a scheme with a finite cover of spectra of finitely generated K-algebras.

Let p be a prime number. Fix a power q of p. Let V be a scheme of finite type over $\mathbb{F}_q$. Denote by $|V|$ the set of closed points of V.

Definition 1.1.2. If $x \in |V|$, the residue field $\mathcal{K}(x)$ is a finite extension of $\mathbb{F}_q$. The **degree** of x is $\deg(x) := [\mathcal{K}(x) : \mathbb{F}_q]$.

Remark 1.1.3. A **point** of V with values in $\mathbb{F}_{q^k}$ is a morphism of $\mathbb{F}_q$-schemes $\mathrm{Spec}(\mathbb{F}_{q^k}) \to$

V. The data of such a point is equivalent to that of its image $x \in |V|$ and of the local morphism of $\mathbb{F}_q$-algebras $\mathcal{O}_{V,x} \to \mathbb{F}_{q^k}$ *i.e* of a $\mathbb{F}_q$-morphism $\mathcal{K}(x) \to \mathbb{F}_{q^k}$.

The closed point x being fixed, there are $\deg(x)$ such points.

We denote by $V(\mathbb{F}_{q^k})$ the set of $\mathbb{F}_{q^k}$-points of V.

Lemma 1.1.4. If $d \in \mathbb{Z} > 0$, there are finitely many closed points of degree d in V.

Proof. V is of finite type over $\mathbb{F}_q$: it can be covered by finitely many affine $\mathbb{F}_q$-schemes of finite type so we can reduce to the case $V = \mathrm{Spec}(A)$ where $A \simeq \mathbb{F}_q[X_1, \ldots, X_r]/I$ for some ideal I.

The result follows from the fact that there are finitely many $\mathbb{F}_q$-morphisms $A \to \mathbb{F}_{q^d}$ (at most q^{dr}). □

Definition 1.1.5. The **zeta-function** of V is

$$Z_V(T) = \prod_{x \in |V|} \frac{1}{1 - T^{\deg(x)}} \in \mathbb{Z}[[T]]$$

(the product converges in $\mathbb{Z}[[T]]$ thanks to lemma 1.1.4).

Lemma 1.1.6. We have $Z_V(T) = \exp\Big(\sum_{k=1}^{\infty} \frac{\#V(\mathbb{F}_{q^k})T^k}{k}\Big)$.

Proof. Taking logarithm in $\mathbb{Q}[[T]]$ we have:

$$\log(Z_V(T)) = \sum_{x \in |V|} -\log(1 - T^{\deg(x)}) = \sum_{x \in |V|} \sum_{k=1}^{\infty} \frac{T^{\deg(x)k}}{k} = \sum_{d=1}^{\infty} \frac{N_d(V)}{d} T^d$$

where $N_d(V) = \sum_{x \in |V|, \deg(x) | d} \deg(x) = \#V(\mathbb{F}_{q^d})$. □

Remark 1.1.7.

$$\begin{aligned} Z_V(q^{-s}) &= \prod_{x \in |V|} \frac{1}{1 - q^{-s \deg(x)}} \\ &= \prod_{x \in |V|} \frac{1}{1 - N(x)^{-s}} \end{aligned}$$

where $N(x) = \#\mathcal{K}(x)$.

The purpose of this work is to give the detailed proof of the following theorem:

Theorem 1.1.8. *(Dwork, 1960 [1])*

$$Z_V(T) \in \mathbb{Q}(T).$$

Remark 1.1.9.

If V is of finite type over $\mathbb{F}_q$ then it is also of finite type over $\mathbb{F}_p$ so we may restrict to varieties over $\mathbb{F}_p$. Indeed, we have $[\mathcal{K}(x) : \mathbb{F}_p] = [\mathcal{K}(x) : \mathbb{F}_q]d$ with $d = [\mathbb{F}_q : \mathbb{F}_p]$, so

$$\begin{aligned} Z_{V/\mathbb{F}_p}(T) = \prod_{x \in |V|} \frac{1}{1 - T^{[\mathcal{K}(x):\mathbb{F}_p]}} &= \prod_{x \in |V|} \frac{1}{1 - T^{d \deg(x)}} \\ &= Z_{V/\mathbb{F}_q}(T^d). \end{aligned}$$

If theorem 1.1.8 is known when $q = p$, then we have $Z_{V/\mathbb{F}_q}(T^d) \in \mathbb{Q}(T) \cap \mathbb{Z}[[T^d]]$ and theorem 1.1.8 follows from next lemma.

Lemma 1.1.10. $\mathbb{Q}(T) \cap \mathbb{Z}[[T^d]] \subset \mathbb{Q}(T^d)$.

Proof. It suffices to show that $\mathbb{C}(T) \cap \mathbb{Z}[[T^d]] \subset \mathbb{C}(T^d)$. Let $\frac{P(T)}{Q(T)} \in \mathbb{C}(T) \cap \mathbb{Z}[[T^d]]$ with $P, Q \in \mathbb{C}(T)$ and $\gcd(P, Q) = 1$. Let ζ a primitive d-th root of unity. Then we have

$$\begin{aligned} \frac{P(\zeta T)}{Q(\zeta T)} = \frac{P(T)}{Q(T)} &\implies P(\zeta T)Q(T) = P(T)Q(\zeta T) \\ &\implies P(T) | P(\zeta T) \text{ by Gauss's theorem} \\ &\implies P(T) = P(\zeta T) \end{aligned}$$

Therefore $P(\zeta^i T) = P(T)$, so $P(T) = \frac{1}{d} \sum_{i=0}^{d-1} P(\zeta^i T) \in \mathbb{C}[T^d]$, and similarly $Q(T) \in \mathbb{C}[T^d]$. □

1.2 Reduction to the case where V is a hypersurface

Lemma 1.2.1. If $V = V' \cup V''$ where V', V'' are subschemes then

$$Z_V(T) = \frac{Z_{V'}(T) Z_{V''}(T)}{Z_{V' \cap V''}(T)}.$$

Proof. Follows from the definition of $Z_V(T)$. □

Lemma 1.2.2. The theorem follows from the special case where $V = V(f) \subset \mathbb{A}^d_{\mathbb{F}_p}$: zero locus of f, for some polynomial $f(\underline{X}) \in \mathbb{F}_p[X_1, \ldots, X_d]$.

Proof. As seen above we may restrict to the case $q = p$.

As V is of finite type over $\mathbb{F}_p$, we can write $V = \cup_{i=1}^r V_i$ where $V_1, \ldots, V_r$ are affine subschemes. By the previous lemma, we have

$$Z_V(T) = \prod_{I \subset \{1,\ldots,r\}, I \neq \emptyset} Z_{V_I}(T)^{(-1)^{\#I-1}}$$

where $V_I = \cap_{i \in I} V_i$ for all $I \subset \{1, \ldots, r\}$; it is enough to show that $I \neq \emptyset \implies Z_{V_I}(T) \in \mathbb{Q}(T)$.

As V_I is a subscheme of an affine scheme when $I \neq \emptyset$, it is separated: we may reduce to the case where V is separated. Then all the V_I are affine (cf [2], Chap 3.3, Prop 3.6): we can restrict to the case where V is affine.

We can write $V = V(I) \subset \mathbb{A}^d_{\mathbb{F}_p}$ where $I = \langle f_1, \ldots, f_m \rangle \subset \mathbb{F}_p[X_1, \ldots, X_d]$ is an ideal. Assume $m > 1$ and let $V' = V(\langle f_1, \ldots, f_m \rangle)$, $V'' = V(f_m)$. Then $V = V' \cap V''$: by the previous lemma, we have

$$Z_V(T) = \frac{Z_{V'}(T) Z_{V''}(T)}{Z_{V' \cup V''}(T)}$$

as $V = V' \cup V'' = V(\langle f_1, \ldots, f_{m-1} f_m \rangle)$ an induction reduces to the case $m = 1$. □

The theorem 1.1.8 is the first part of the **Weil conjectures** which were proposed in 1949 by André Weil. We recall these conjectures:

Conjecture 1.2.3. (Weil conjectures,1949) Suppose that X is a non-singular n-dimensional projective algebraic variety over the field $\mathbb{F}_q$ with q elements. The zeta function $Z_X(T)$ of X is the same as above with $T = q^{-s}$ and denoted also $Z(X, s)$. Then we have:

(1) (**Rationality**) Z_V is a rational function. More precisely, Z_V can be written as a finite alternating product:

$$\prod_{i=0}^{2n} P_i(T)^{(-1)^{i+1}} = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T) \cdots P_{2n}(T)},$$

where each $P_i(T) \in \mathbb{Z}[T]$. Moreover, $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$ and for $1 \leq i \leq 2n-1$, $P_i(T) = \prod_j (1 - \alpha_{ij} T)$ with $\alpha_{ij} \in \mathbb{C}$.

(2) (**Functional equation and Poincaré duality**) The zeta function satisfies $Z(X, n-s) = \pm q^{\frac{nE}{2} - Es} Z(X, s)$ or equivalently $Z(X, q^{-n}T^{-1}) = \pm q^{\frac{nE}{2}} Z_X(T)$ where X is the Euler characteristic of X. In particular, for each i, the numbers $\alpha_{2n-i,i}, \alpha_{2n-i,2}, \ldots$ equal the numbers $q^n \alpha_{i,1}, q^n \alpha_{i,2}, \ldots$ in some order.

(3) **(Analogue of Riemann hypothesis)** $|\alpha_{ij}| = q^{i/2}$ for $1 \leq i \leq 2n-1$ and for all j. Thus all zeros of $P_i(T)$ are on the line of complex numbers s with real part $i/2$.

(4) **(Betti numbers)** If X is the reduction modulo p of a non-singular projective variety Y defined over a number field embedded in the field of complex numbers, then the degree of P_i is the i^{th} Betti number of the space of complex points of Y.

The functional equation was proved by Alexander Grothendieck (1965), and the analogue of the Riemann hypothesis by Pierre Deligne (1974).

It is now worth illustrating this theorem with some examples:

Example 1.2.4.

1) Consider $V = \mathbb{A}^n_{\mathbb{F}_q}$ the n-dimensional affine space over $\mathbb{F}_q$.

The number of $\mathbb{F}_{q^s}$-rational points of V is

$$\begin{aligned} N_s &= \#V(\mathbb{F}_{q^s}) \\ &= \#\{x \in \mathbb{A}^n | x \in \mathbb{F}_{q^s}\} \\ &= q^{ns}. \end{aligned}$$

We have

$$\begin{aligned} Z_{\mathbb{A}^n}(T) &= \exp\Big(\sum_{s=1}^{\infty} \frac{N_s}{s} T^s\Big) \\ &= \exp\Big(\sum_{s=1}^{\infty} \frac{q^{ns}}{s} T^s\Big) = \exp\Big(\sum_{s=1}^{\infty} \frac{(q^n T)^s}{s}\Big) \\ &= \exp\Big(-\log(1 - q^n T)\Big) = \frac{1}{1 - q^n T} \in \mathbb{Q}(T). \end{aligned}$$

2) Consider the n-dimensional projective space $V = \mathbb{P}^n_{\mathbb{F}_q}$. We know that $\mathbb{P}^n = \mathbb{P}^{n-1} \sqcup \mathbb{A}^n$, so $V(\mathbb{F}_{q^s}) = \mathbb{P}^{n-1}(\mathbb{F}_{q^s}) \sqcup \mathbb{A}^n(\mathbb{F}_{q^s})$.

By lemma 1.2.1 we have

$$Z_{\mathbb{P}^n}(T) = Z_{\mathbb{P}^{n-1}}(T) Z_{\mathbb{A}^n}(T).$$

By induction, we obtain

$$Z_{\mathbb{P}^n}(T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^nT)}.$$

1.3 Plan of the work

- At the beginning we explained how we can reduce the zeta function for any algebraic varieties into zeta functions defined on hypersurfaces. Then we shall see some definitions and results about the terms in which we will use throughout this work.
- Secondly we introduce the criteria for rationality.
- Finally, we will see the construction of a power series that relates the character of finite field and the p-adic expression of the zeta function. After that we complete the proof of the theorem.

2

Backgrounds

This chapter is devoted to all definitions and properties of the mathematical objects that we are going to use in the rest of this text.

2.1 Cyclotomic polynomials

Definition 2.1.1. Let F be a field and $n \in \mathbb{Z}_{>0}$ prime to $\mathrm{char}(F)$. A primitive n-th root of 1 is an element $\zeta \in F$ such that $\zeta^n = 1$ and $\zeta^m \neq 1$ if $0 < m < n$.

The n-th **roots of unity** in $\mathbb{C}$ are $\zeta = e^{2i\pi\frac{k}{n}}$ where $k \in \{0, \ldots, n-1\}$.

Definition 2.1.2. Let n be a positive integer, the n-th **cyclotomic polynomial** is defined by

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (X - e^{2i\pi\frac{k}{n}}).$$

Proposition 2.1.3. *For all $n \in \mathbb{Z}_{>0}$, we have:*

(i) $X^n - 1 = \prod_{d|n} \Phi_d(X)$

(ii) $\Phi_n(X) \in \mathbb{Z}[X]$.

2.2 Teichmüller representatives

Teichmüller representatives are induced from a canonical map lifting elements in $\overline{\mathbb{F}_p}^\times$ into roots of unity in characteristic 0.

Let $\overline{\mathbb{Q}_p}$ be an algebraic closure of $\mathbb{Q}_p$.

The absolute value $|.|_p$ extends uniquely to $\overline{\mathbb{Q}_p}$: denote by $\mathbb{C}_p$ the completion of $\overline{\mathbb{Q}_p}$ with respect to $|.|_p$. This is an algebraically closed field, and its residue field coincides with that of $\overline{\mathbb{Q}_p}$: it is isomorphic to $\overline{\mathbb{F}_p}$.

Proposition 2.2.1. *There exists a unique map $\overline{\mathbb{F}_p} \xrightarrow{[.]} \mathcal{O}_{\mathbb{C}_p}$ such that:*

(i) For all $x \in \overline{\mathbb{F}_p}$ $[x]$ maps to x in the residue field $\overline{\mathbb{F}_p}$.

(ii) $(\forall x, y \in \overline{\mathbb{F}_p})$ $[xy] = [x][y]$.

Proof. (i) Let $x \in \overline{\mathbb{F}_p}$. There exists $n \in \mathbb{Z}_{>0}$ such that x is a root of $P_n(X) = X^{p^n} - X \in \mathbb{Z}[X]$. If $\tilde{x} \in \mathcal{O}_{\mathbb{C}_p}$ lifts x then $P_n(\tilde{x})$ maps to 0 in $\overline{\mathbb{F}_p}$ and $P_n'(\tilde{x}) = p^n \tilde{x}^{p^n - 1} - 1$ maps to $-1 \in \overline{\mathbb{F}_p}^\times$. By Newton's lemma, there exists a unique $[x] \in \mathcal{O}_{\mathbb{C}_p}$ such that $P_n([x]) = 0$ and $[x]$ maps to x in $\overline{\mathbb{F}_p}$.

(ii) Let $y \in \overline{\mathbb{F}_p}$. We may assume that $y \in \mathbb{F}_{p^n}$: we have $P_n([y]) = 0 \Rightarrow [y]^{p^n} = [y]$ and $[x]^{p^n} = [x]$ so $([x][y])^{p^n} = [x][y]$. As $[x][y]$ maps to xy in $\overline{\mathbb{F}_p}$, we have $[x][y] = [xy]$ by unicity.

□

Definition 2.2.2. $[x]$ is called the **Teichmüller representative** of x.

Example 2.2.3.

(1) $[0] = 0$

(2) If $x \in \mathbb{F}_{p^n}^\times$ then $[x]$ is a $(p^n - 1)$-th root of unity.

Remark 2.2.4.

- In general $[x + y]$ is not equal to $[x] + [y]$ i.e $[.]$ is not a ring homomorphism.
- If $n \in \mathbb{Z}_{>0}$, the elements $\{[x]\}_{x \in \mathbb{F}_{p^n}}$ generate the unique unramified extension of degree n of $\mathbb{Q}_p$.

2.3 Characters

Let Ω be an algebraically closed field of characteristic 0.

Definition 2.3.1. [3] A **character** on a group G is a group homomorphism χ from G to the multiplicative group $\Omega^\times$. The set of characters of G form an abelian group called the **dual** of G, denoted by $\widehat{G}$.

A character is trivial if $\chi(g) = 1$ for every $g \in G$.

Let G be a finite abelian group. Set $n = \#G$.

We have $\chi(G) \subset \mu_n := \{x \in \Omega | x^n = 1\}$.

Indeed, for every $g \in G$, we have $g^n = 1$ therefore $\chi(g)^n = \chi(g^n) = \chi(1) = 1$.

Lemma 2.3.2. Let $H < G$ a subgroup of G and let $\widehat{G} \xrightarrow{f} \widehat{H}$ be the restriction map. Then f is surjective.

Proof. Let $\chi \in \widehat{H}$, let's show that there exists $\eta \in \widehat{G}$ such that $\eta_{\big| H} = \chi$.

It suffices to show this in the case where G is generated by H and an element g_0. If $g \in G$, there exist $h \in H$ and $k \in \mathbb{Z}$ such that $g = hg_0^k$.

If η exists then $\eta(g) = \chi(h)\eta(g_0)^k$, we need to construct $\eta(g_0)$.

Let $r = \min\{k \in \mathbb{N}_{>0} | g_0^k \in H\}$.

It follows that $\{k \in \mathbb{Z}_{>0} | g_0^k \in H\} = r\mathbb{Z}$.

Yet

$$g_0^r \in H \implies \chi(g_0^r) = \eta(g_0^r) = \eta(g_0)^r.$$

Let $\zeta \in \not{<}^\times$ such that $\zeta^r = \chi(g_0^r)$.
Set

$$G \xrightarrow{\eta} \mathbb{C}^\times$$
$$g = hg_0^k \mapsto \chi(h)\zeta^k,$$

- η is well-defined:

$hg_0^k = h'g_0^{k'} \implies h^{-1}h' = g_0^{k-k'} \implies k - k' \in r\mathbb{Z}$ *i.e* $k' = k + rz$ for some $z \in \mathbb{Z}$.
Then $hg_0^k = h'g_0^{k+rz} \implies h = h'(g_0^r)^z$, and so

$$\chi(h) = \chi(h')(\chi(g_0^r))^z = \chi(h')\zeta^{rz},$$

hence

$$\chi(h)\zeta^k = \chi(h')\zeta^{rz+k} = \chi(h')\zeta^{k'}.$$

- η is a group homomorphism: let $g_1 = h_1 g_0^{k_1}$, $g_2 = h_2 g_0^{k_2}$ then $\eta(g_1 g_2) = \chi(h_1 h_2)\zeta^{k_1 k_2} = \chi(h_1)\chi(h_2)\zeta^{k_1}\zeta^{k_2} = \eta(g_1)\eta(g_2)$.

□

Proposition 2.3.3. *$\widehat{G}$ is non canonically isomorphic to G.*

Proof. G can be written as a finite product of cyclic groups: we may restrict to the case where $G = \mathbb{Z}/n\mathbb{Z}$. Then we have an isomorphism

$$\begin{aligned} \mu_n &\to \widehat{G} \\ \zeta &\mapsto (\bar{k} \mapsto \zeta^k). \end{aligned}$$

This result follows from the existence of a non canonical isomorphism $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$. □

Consider the following map:

$$\begin{aligned} G &\xrightarrow{ev} \widehat{\widehat{G}} \\ g &\mapsto \Big(ev_g : \chi \mapsto \chi(g)\Big). \end{aligned}$$

It is straightforward to see that ev is a group homomorphism.

We have further the following lemma:

Theorem 2.3.4. *ev is an isomorphism.*

2.3.2

Proof. As $\#\widehat{\widehat{G}} = \#\widehat{G} = \#G$ by proposition 2.3.3, it is enough to show that ev is injective. Let $g \in G \setminus \{e\}$ with e the neutral element of G. Put $H = \langle g \rangle \cong \mathbb{Z}/a\mathbb{Z}$. We have $\widehat{H} \simeq \mu_a$,

$$(\exists\ \varphi \in \widehat{H}),\ \varphi(g) = e^{\frac{2\pi i}{a}}.$$

By lemma 2.3.3, there exists $\chi \in G$ such that $\chi_{|<g>} = \varphi$ so that $\chi(g) = \varphi(g) \neq 1$. $\square$

Example 2.3.5. Additive characters of finite fields Let p be a prime number and $q = p^k$.

1) Let $\varepsilon \in \Omega^\times$ is a primitive p-th root of unity. The map

$$\begin{aligned} \chi : \mathbb{F}_p &\to \Omega^\times \\ a &\mapsto \varepsilon^a \end{aligned}$$

is a non trivial character of the additive group of $\mathbb{F}_p$.

2) Recall that the trace map is defined by:

$$\begin{aligned} \mathrm{Tr} : \mathbb{F}_q &\to \mathbb{F}_q \\ a &\mapsto \sum_{i=0}^{k-1} \sigma_i(a), \end{aligned}$$

where $\sigma_i(a) = a^{p^i}$, are all the automorphisms of the finite field extension $\mathbb{F}_q/\mathbb{F}_p$. So $\mathrm{Tr}(a) = a + a^p + a^{p^2} + \cdots + a^{p^{k-1}}$ and

$$\begin{aligned} (\mathrm{Tr}(a))^p &= \Big(\sum_{i=0}^{k-1} \sigma_i(a) \Big)^p \\ &= \sum_{i=0}^{k-1} \sigma_i(a)^p = \sum_{i=0}^{k-1} (a^{p^i})^p \end{aligned}$$

This implies that $\mathrm{Tr}(a) \in \mathbb{F}_p$ so that the trace induces a map $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$. Therefore we have the following composition which provides a non trivial character of the additive group of $\mathbb{F}_q$:

$$\begin{aligned} \mathbb{F}_q \to \mathbb{F}_p &\to \Omega^\times \\ a \mapsto \mathrm{Tr}(a) &\mapsto \varepsilon^{\mathrm{Tr}(a)}. \end{aligned}$$

2.4 Sylvester relation

Definition 2.4.1. Let R be a ring and $A = (a_{i,j})_{0 \leq i,j \leq m} \in M_{m+1}(R)$.

The determinant of A is $\det(A)$, equal to $\sum_{i=0}^{m}(-1)^{i+j}a_{ij}M_{ij}$ where M_{ij} is the determinant of minor matrix (the determinant of A by deleting the row i and column j): homogeneous polynomial of degree $m+1$ with respect to the whole variables a_{ij} and of degree 1 with respect to each variable a_{ij}.

It can also be expressed by the Leibniz formula:

$$\det(A) = \sum_{\sigma \in S_n} \left(\operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma_i} \right)$$

where $\operatorname{sgn}(\sigma)$ is the signature of the permutation.

Lemma 2.4.2. (Sylvester relation,[4]) Let $A \in M_{m+1}(R)$ and let $D = \det(A)$. Set $A_{ij} = (-1)^{i+j}M_{ij}$. Let d be the determinant of the matrix obtained by removing the extreme rows and columns. Then:

$$Dd = A_{0,0}A_{m,m} - A_{0,m}A_{m,0}. \tag{3.3}$$

Proof. Without loss of generality, we may assume that $R = \mathbb{Z}[X_{i,j}]_{0\leq i,j\leq m}$ and $A = (X_{i,j})_{0\leq i,j\leq m}$.

We prove this by considering D' the determinant D' of $B = (b_{ij})_{0\leq i,j\leq m}$ defined by:

$$b_{0j} = A_{0j}, b_{mj} = A_{mj}, \text{ and if } \ i \neq 0, b_{ij} = 1 \text{ if } i = j, \ 0 \text{ otherwise.}$$

We have

$$D' = \det(B) = \begin{vmatrix} A_{0,0} & A_{0,1} & A_{0,2} & \dots & A_{0,m} \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 1 & 0 \\ A_{m,0} & A_{m,1} & A_{m,2} & \dots & A_{m,m} \end{vmatrix}$$

and it is equal to

$$A_{0,0}A_{m,m} - A_{0,m}A_{m,0}.$$

We have as before

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & \dots & \dots & a_{0,m} \\ a_{1,0} & a_{1,1} & \dots & \dots & a_{1,m} \\ \vdots & \vdots & \dots & \dots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \dots & \dots & a_{m-1,m} \\ a_{m,0} & a_{m,1} & \dots & \dots & a_{m,m} \end{pmatrix}.$$

Yet $\det(AB) = \det(A)\det(B) = DD'$ and $C = \mathrm{com}(A) = (A_{ij})_{0 \le i,j \le m}$ and

$$D\,\mathrm{I_{n+1}} = AC^t.$$

We have

$$AC^t = \begin{pmatrix} a_{0,0} & a_{0,1} & \dots & \dots & a_{0,m} \\ a_{1,0} & a_{1,1} & \dots & \dots & a_{1,m} \\ \vdots & \vdots & \dots & \dots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \dots & \dots & a_{m-1,m} \\ a_{m,0} & a_{m,1} & \dots & \dots & a_{m,m} \end{pmatrix} \begin{pmatrix} A_{0,0} & A_{1,0} & A_{2,0} & \dots & A_{m,0} \\ A_{0,1} & A_{1,1} & A_{2,1} & \dots & A_{m,1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ A_{0,m} & A_{1,m} & A_{2,m} & \dots & A_{m,m} \end{pmatrix}.$$

By identification, we get for instance

$$a_{0,0}A_{0,0} + a_{1,0}A_{1,0} + \cdots + a_{m,0}A_{m,0} = D \text{ and } \; a_{0,0}A_{0,1} + a_{1,0}A_{1,1} + \cdots + a_{m,0}A_{m,1} = 0.$$

Therefore

$$\begin{aligned} \det(BA) &= \begin{vmatrix} D & 0 & \dots & \dots & 0 \\ a_{1,0} & a_{1,1} & \dots & \dots & a_{1,m} \\ \vdots & \vdots & \dots & \dots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \dots & \dots & a_{m-1,m} \\ 0 & \dots & \dots & 0 & D \end{vmatrix} \\ &= D^2 \begin{vmatrix} a_{1,0} & a_{1,1} & \dots & \dots & a_{1,m} \\ \vdots & \vdots & \dots & \dots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \dots & \dots & a_{m-1,m} \end{vmatrix} = D^2 d. \end{aligned}$$

Therefore it follows that:

$$DD' = D^2 d.$$

Since $DD' = D(A_{0,0}A_{m,m} - A_{0,m}A_{m,0})$ and as $D \neq 0$ and R is a domain then we proved Sylvester's relation. $\square$

3

Conditions for rationality

In the following we will see the criteria for rationality of power series.

3.1 Criteria from linear algebra

Consider a power series $F(T) = \sum_{i=0}^{\infty} a_i T^i \in K[[T]]$ where K is a field.

Let m, s be two integers with $m, s \geq 0$ and let $A_{s,m}$ be a matrix $m \times m$ given by $(a_{s+i+j})_{0 \leq i,j \leq m}$.

Denote by $N_{s,m}$ the **determinant** of the matrix $A_{s,m}$.

Proposition 3.1.1. *The following are equivalent:*

(i) *F is a rational function, i.e it can be written in the form $F(T) = \frac{P(T)}{Q(T)}$ where $P(T), Q(T) \in K[T]$ with $Q(T) \neq 0$.*

(ii) *There exist two integers $m \geq 0$ and $S \geq 0$ such that whenever $s \geq S$ we have $N_{s,m} = 0$.*

Proof. (i)⇒ (ii)

Write $F(T) = \frac{P(T)}{Q(T)}$. So we get

$$F(T)Q(T) = P(T). \tag{3.1}$$

Write $Q(T) = \sum_{i=0}^{N} c_i T^i$ and put $M = \deg(P)$: the LHS (left hand side) is

$$\sum_{i=0}^{\infty} \Big(\sum_{j=0}^{N} a_{i-N+j} c_{N-j} \Big) T^i.$$

The equality (3.1) implies that for all $i > \max(M, N)$ we have

$$\sum_{j=0}^{N} a_{i-N+j} c_{N-j} = 0. \tag{3.2}$$

Therefore we obtain a system of dependent linear equations. Take $S = \max(M-N+1, 1)$ and $m = N$. Put $X = (c_N, c_{N-1}, \ldots, c_0)$: if $s \geq S$, equations (3.2) imply that $XA_{s,m} = 0$, as $X \neq 0$ then $N_{s,m} = 0$.

(ii) $\Rightarrow$ (i)

Suppose that there exist integers $m \geq 0$ and S such that $N_{s,m} = 0$ when $s \geq S$, choose m to be the minimal satisfying this property. We may assume that $(a_n)_{n\in\mathbb{N}}$ is not stationary, so that $m > 0$.

We first claim that $N_{s,m-1} \neq 0$ for all $s \geq S$.

By contradiction, let $S' \geq S$ such that $N_{S',m-1} = 0$.

Applying Sylvester's relation to $D = N_{s,m}$ and

$$\begin{aligned} d &= \det(a_{s+2+i+j})_{0\leq i,j\leq m-2} = N_{s+2,m-2} \\ A_{00} &= \det(a_{s+2+i+j})_{0\leq i,j\leq m-1} = N_{s+2,m-1} \\ A_{mm} &= \det(a_{s+i+j})_{0\leq i,j\leq m-1} = N_{s,m-1} \\ A_{0m} &= \det(a_{s+1+i+j})_{0\leq i,j\leq m-1} = N_{s+1,m-1} = A_{m0}. \end{aligned}$$

So we have

$$N_{s,m}N_{s+2,m-2} = N_{s+2,m-1}N_{s,m-1} - (N_{s+1,m-1})^2 \text{ for } m \geq 2.$$

Let $s \geq S'$.

Assume $N_{s,m-1} = 0$: we have $N_{s,m} = 0$ thus $N_{s+1,m-1} = 0$. By induction, this implies that $N_{s,m-1} = 0$ for all $s \geq S'$. This contradicts the minimality of m.

As $N_{s,m} = 0$ and $N_{s,m-1} \neq 0$, the rank of the matrix $A_{s,m}$ is m. This implies that the K-vector space $\ker(A_{s,m}) = \{X \in K^{m+1} | XA_{s,m} = 0\}$ has dimension 1. As $N_{s,m-1} \neq 0$ and $N_{s+1,m-1} \neq 0$, this space coincides with the kernel of the matrix obtained by removing the first or the last line. This shows that $\ker(A_{s,m}) = \ker(A_{s+1,m})$.

Let $X = (c_m, c_{m-1}, \ldots, c_0)$ be a generator of $\ker(A_{s,m})$. If $c_m = 0$ then $\tilde{X} A_{s+1,m-1} = 0$ where $\tilde{X} = (c_{m-1}, \ldots, c_0) \neq 0$ implying that $N_{s+1,m-1} = 0$ which is a contradiction. So we have $c_m \neq 0$.

Put

$$Q(T) = \sum_{i=0}^{m} c_i T^i.$$

What precedes shows that $Q(T)F(T) \in K[T]$, so $F(T)$ is rational.

□

3.2 Analytic criteria

Now let Ω be an algebraically closed, complete valued field which contains $\mathbb{Q}_p$. The usual p-adic absolute value on $\mathbb{Q}_p$ extends into an absolute value $|.|_p : \Omega \longrightarrow \mathbb{R}_{\geq 0}$.

Definition 3.2.1. Let a power series $F(t) = \sum_{i=0}^{\infty} a_i t^i \in \Omega[[t]]$.

We say that:

- F is **holomorphic** in the disc $|t|_p < r$ if it converges absolutely in this disc.
- A **meromorphic** function is a quotient of two holomorphic functions.

Proposition 3.2.2. *(Weirstrass Preparation Theorem) If F is holomorphic in the disc $|t|_p < r$ and if $r' < r$ then $F = P.h$ where P is a polynomial, h is an invertible holomorphic power series in the disc $|t|_p < r'$.*

The proof of this is more sophisticated since we have to use the Newton polygon so we refer the idea of the proof in the chapter 4 of [5].

Lemma 3.2.3. Let $x \in \mathbb{Z}$. If $|x|.|x|_p < 1$ then $x = 0$.

Proof. Suppose $x \neq 0$, we have $x = \pm \prod_q q^{v_q(x)}$ then $|x| = \prod_q q^{v_q(x)}$ and $|x|_p = p^{-v_q(x)}$. Thus $|x|.|x|_p = \prod_{q \neq p} q^{v_q(x)} \geq 1$ which is a contradiction. □

Proposition 3.2.4. *Let $F(t) = \sum_{i=0}^{\infty} A_i t^i \in \mathbb{Z}[[t]]$ and let p a prime number.*

Suppose there exist R and $r \in \mathbb{R}$ with $Rr > 1$, such that F is meromorphic in the disc $|t| < R$ of $\mathbb{C}$ and also in the disc $|t|_p < r$ of Ω. Then F is rational.

Proof. Since by hypothesis, F is meromorphic in the disc $|t|_p < r$ then F can be written of the form $F(t) = \frac{B(t)}{A(t)}$ where $A(t) = \sum_{i=0}^{\infty} a_i t^i$, $B(t) = \sum_{i=0}^{\infty} B_i t^i \in \Omega[[t]]$ are holomorphic in the disc $|t|_p < r$.

This implies that

$$B(t) = A(t)F(t). \tag{3.2}$$

By using the proposition (3.2.2), we may reduce r a little and assume that A is a polynomial and that $a_0 = 1$.

Reducing r and R a little, then we obtain the inequalities for s large enough:

$$|B_s|_p < r^{-s} \tag{3.3}$$
$$|A_s| < R^{-s}. \tag{3.4}$$

Now we are going to apply the criterion of proposition (3.1.1) for rationality.

We need to find $m \geq 0$ such that we have $N_{s,m} = 0$ for s large enough.

So let e be the degree of the polynomial A, since $Rr > 1$, choose m such that $R^{m+1} r^{m+1-e} = k$ is greater than 1.

By the equality (3.2), we have

$$\sum_{i=0}^{\infty} B_i t^i = \sum_{i=0}^{\infty} \Big(\sum_{j=0}^{e} a_{e-j} A_{i+j-e} \Big) t^i.$$

By identification for the monomial of degree $s+e$ we have:

$$B_{s+e} = A_{s+e} + \cdots + a_{e-1} A_{s+1} + a_e A_s.$$

Recall

$$N_{s,m} = \det \begin{pmatrix} A_s & A_{s+1} & \dots & A_{s+e-1} & A_{s+e} & \dots & A_{s+m} \\ A_{s+1} & A_{s+2} & \dots & \dots & \dots & \dots & A_{s+m+1} \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots \\ A_{s+m} & A_{s+m+1} & \dots & \dots & \dots & \dots & A_{s+2m} \end{pmatrix}.$$

We can replace A_{s+i+j} by B_{s+i+j} for $j \geq e$, it doesn't change the determinant $N_{s,m}$.

By the relation (3.3) and as $|A_s|_p \leq 1$, we have

$$|N_{s,m}|_p \leq r^{-(m-e+1)s}$$

for s large enough Also we have for s large enough

$$|N_{s,m}| \leq R^{-(m+1)(s+2m)}.$$

Indeed, we make use of the inegality of Hadamard which says that $|N_{s,m}|^2 \leq \prod_{i=0}^{m} \Big(\sum_{j=0}^{m} A_{s+i+j}^2 \Big)$: we have

$$\begin{aligned} |N_{s,m}|^2 &\leq \prod_{i=0}^{m} \Big(\sum_{j=0}^{m} R^{-2(s+i+j)} \Big) = \prod_{i=0}^{m} R^{-2(s+i)} (1 + R^{-2} + \cdots + R^{-2m}) \\ &\leq (1 + R^{-2} + \cdots + R^{-2m})^{m+1} R^{-2\sum_{i=0}^{m}(s+i)} \\ &\leq (1 + R^{-2} + \cdots + R^{-2m})^{m+1} R^{-(m+1)(2s+m)} \end{aligned}$$

then $|N_{s,m}| \leq k_1 R^{-(m+1)}$ where $k_1 = (1 + R^{-2} + \cdots + R^{-2m})^{\frac{m+1}{2}} R^{-\frac{m(m+1)}{2}}$ doesn't depend on s. Since $|N_{s,m}|.|N_{s,m}|_p < 1$ for s large enough therefore by lemma (3.2.3) $N_{s,m} = 0$. $\square$

We will be building a power series that can factorize the additive character seen in the example (2.3.5).

4

Rationality

4.1 Construction: factorization of additive characters of the finite field $\mathbb{F}_q$

Let Ω be the completion of the algebraic closure of the field of p-adic numbers, it is algebraically closed. Let $\varepsilon = \lambda + 1 \in \Omega$ be a primitive p-th root of unity.

Lemma 4.1.1. Let $\varepsilon = \lambda + 1$ be a p-th root of unity as above. Then $\mathrm{ord}(\lambda) = \frac{1}{p-1}$.

Proof. Since $(X-1)^p = X^p - 1 + p(X-1)A[X]$ with $A[X] \in \mathbb{Z}[X]$ of degree $p-1$ then

$$(X-1)^{p-1} = \frac{X^p - 1}{X-1} + pA(X) \text{ and } A(1) = -1.$$

At $X = \varepsilon$, we have $\lambda^{p-1} = pA(\varepsilon)$ therefore $(p-1)\,\mathrm{ord}(\lambda) \geq 1$ and this implies that $\mathrm{ord}(\lambda) > 0$. By the Taylor expansion of A we have: $A(\varepsilon) - A(1) = \sum_{i=1}^{p-2} \frac{A^{(i)}(1)}{i!}(\varepsilon - 1)^i$. So $\mathrm{ord}(A(\varepsilon) - A(1)) \geq \mathrm{ord}(\lambda) > 0$, $A(1) = -1 \implies \mathrm{ord}(A(\varepsilon)) = 0$. Hence $\mathrm{ord}(\lambda) = \frac{1}{p-1}$. □

Let $a \in \mathbb{F}_q^\times$ and $t = [a] \in \mathbb{Z}_q$ (where $\mathbb{Z}_q$ is the ring of integers of the unramified extension $\mathbb{Q}_p$ of $\mathbb{Q}$ lifting $\mathbb{F}_q/\mathbb{F}_p$) its Teichmüller representative: t is a $(q-1)$-th root of 1 lifting a.

Remark 4.1.2. The conjugates of the Teichmüller representative of a are the conjugates of t in Ω: these are the Teichmüller representatives of the conjugates of a.

We will be looking for a power series with indeterminate variable T whose value $T = t$ is $\varepsilon^{Tr(a)}$.

The easiest power series is $(1+Y)^{t+t^p+\cdots+t^{p^s-1}}$: at $Y = \lambda$ this gives $\varepsilon^{Tr(a)}$. Unfortunately this series is not convergent, we will have to find a suitable one.

Put $H(T,Y) = (1+Y)^T = \sum_{i=0}^{\infty} \binom{T}{i} Y^i$ so $H(T,Y) \in \mathbb{Q}[[T,Y]]$ and

$$\begin{aligned} F(T,Y) &= H(T,Y)H\Big(\frac{T^p - T}{p}, Y^p\Big)H\Big(\frac{T^{p^2} - T^p}{p^2}, Y^{p^2}\Big)\cdots \\ &= F(T,Y) = (1+Y)^T(1+Y^p)^{\frac{T^p-T}{p}}(1+Y^{p^2})^{\frac{T^{p^2}-T^p}{p^2}}\cdots \end{aligned} \tag{2.4}$$

infinite product of power series. It is easily seen that $F(T,Y)$ is a convergent power series in $(\mathbb{Q}[T])[[Y]]$ *i.e* we have $F(T,Y) = \sum_{m=0}^{\infty} P_m(T)Y^m$. In particular, we can evaluate $F(T,Y)$ at $T = t$ and get $F(t,Y) \in \mathbb{Q}_q[[Y]]$.

Remark 4.1.3. $\deg(P_m) \leq m$ for all $m \in \mathbb{N}$.

Lemma 4.1.4. (Dwork) Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in \mathbb{Q}_q[X]$ with $a_0 = 1$. Let σ be the Frobenius automorphism of $\mathbb{Q}_q$. Then $f(X) \in 1 + X\mathbb{Z}_q[X]$ if and only if $(\sigma f(X^p))/(f(X))^p \in 1 + pX\mathbb{Z}_q[X]$.

Proof. ($\Rightarrow$) Write $F(X) = 1 + XG(X)$ with $G(X) \in \mathbb{Z}_q[[X]]$: we have

$$\sigma F(X^p) = 1 + X^p \sigma G(X^p).$$

As σ is congruent to the p-th power map modulo p, we have

$$\sigma F(X^p) \equiv G(X)^p \mod p\mathbb{Z}_q[[X]]$$

so that $\sigma F(X^p) \equiv 1 + X^p G(X^p) \mod pX\mathbb{Z}_q[[X]]$. As $F(X)^p = (1+G(X))^p \equiv 1 + X^p G(X^p) \mod pX\mathbb{Z}_q[[X]]$, we have

$$\begin{aligned} \sigma F(X^p) &\equiv F(X)^p \mod pX\mathbb{Z}_q[[X]] \\ i.e\ \frac{\sigma F(X^p)}{F(X)^p} &\equiv 1 \mod pX\mathbb{Z}_q[[X]] \text{ since } F(X) \in 1 + X\mathbb{Z}_q[[X]] \subset \mathbb{Z}_q[[X]]^\times. \end{aligned}$$

Whence $\frac{\sigma F(X^p)}{F(X)^p} \in 1 + pX\mathbb{Z}_q[[X]]$.

($\Leftarrow$) Write $\frac{\sigma F(X^p)}{F(X)^p} = \sum_{i=0}^{\infty} b_i X^i$: we have $b_0 = 1$ and $b_i \in p\mathbb{Z}_q$ if $i > 0$.

We prove by induction on n that $a_i \in \mathbb{Z}_q$ for all $i \in \{0, \ldots, n\}$. This holds for $n = 0$ since $a_0 = 1$ by hypothesis: assume $n > 0$. We have $\sigma F(X^p) = F(X)^p \sum_{i=0}^{\infty} b_i X^i$

$$i.e \sum_{j=0}^{\infty} \sigma(a_j) X^{pj} = \Big(\sum_{k=0}^{\infty} a_k X^k\Big)^p \Big(\sum_{i=0}^{\infty} b_i X^i\Big).$$

The coefficient of X^n in the LHS is $\begin{cases} 0 \text{ if } p \nmid n \\ \sigma(a_{n/p}) \text{ if } p|n. \end{cases}$

The coefficient of X^n in the RHS is equal to that of

$$\Big(\sum_{k=0}^{\infty} a_k X^k\Big)^p \Big(\sum_{i=0}^{\infty} b_i X^i\Big)$$

$i.e$ to that of $\Big((\sum_{k=0}^{\infty} a_k X^k)^p + p a_n X^n\Big)\Big(\sum_{i=0}^{\infty} b_i X^i\Big)$ $i.e$ to pa_n plus to that of $\Big((\sum_{k=0}^{n-1} a_k X^k)^p\Big)\Big(1 + \sum_{i=1}^{n} b_i X^i\Big)$. The latter belongs to $\mathbb{Z}_q$ and it is congruent to the coefficient of $\sum_{k=0}^{n-1} a_k^p X^{kp}$ modulo p which is equal to 0 if $p \nmid n$ and $a_{n/p}^p$ if $p|n$.

Finally we have

$$0 \equiv pa_n \mod p\mathbb{Z}_q if p \nmid n$$
$$\sigma(a_{n/p}) \equiv pa_n + a_{n/p}^p \mod p\mathbb{Z}_q \text{ if } p|n.$$

As $\sigma(a_{n/p}) \equiv a_{n/p}^p \mod p\mathbb{Z}_q$ when $p|n$ we have $pa_n \in p\mathbb{Z}_q$ in all cases $i.e$ $F(X) \in 1 + X\mathbb{Z}_q[[X]]$. □

Similarly:

Lemma 4.1.5. Let $f(T, Y) \in \mathbb{Q}_q[[T, Y]]$ such that $f(0, 0) = 1$. Then $f(T, Y) \in 1 + T\mathbb{Z}_q[[T, Y]]$ if and only if $\frac{\sigma f(T^p, Y^p)}{f(T,Y)^p} \in 1 + pT\mathbb{Z}_q[[T, Y]] + pY\mathbb{Z}_q[[T, Y]]$.

Lemma 4.1.6. $F(T, Y) \in \mathbb{Z}_p[[T, Y]]$.

Proof. Let's computes $F(T^p, Y^p)/F(T,Y)^p$:

$$F(T^p, Y^p) = (1+Y^p)^{T^p}(1+Y^{p^2})^{\frac{T^{p^2}-T^p}{p}}(1+Y^{p^3})^{\frac{T^{p^3}-T^{p^2}}{p^2}}\dots,$$

and

$$F(T,Y)^p = (1+Y)^{Tp}(1+Y^p)^{T^p-T}(1+Y^{p^2})^{\frac{T^{p^2}-T^p}{p}}\dots,$$

therefore we have

$$F(T^p, Y^p)/F(T,Y)^p = (1+Y^p)^T/(1+Y)^{pT}.$$

Yet by the lemma (4.1.4) applied to $F(Y) = 1+Y$, the series $(1+Y^p)/(1+Y)^p$ is of the form $1+pG$ where G is a power series without constant term where the coefficients is in $\mathbb{Z}_q$. So $F(T^p, Y^p)/F(T,Y)^p$ is of the same form.
It follows from the lemma (4.1.4) that $F(T,Y) \in \mathbb{Z}_q[[Y]]$. □

Proposition 4.1.7. *For every $s \geq 1$, the additive character $\varepsilon^{\mathrm{Tr}(a)}$ can be written as*

$$\theta(t)\theta(t^p)\cdots\theta(t^{p^{s-1}}),$$

where t is the Teichmüller representative of a and where $\theta(T) = \sum_{m=0}^{\infty} \beta_m T^m \in \mathbb{Q}_q(\varepsilon)[[T]]$ satisfies $\mathrm{ord}(\beta_m) \geq \frac{m}{p-1}$ for all $m \in \mathbb{N}$.

Proof. Recall that

$$F(T,Y) = (1+Y)^T(1+Y^p)^{\frac{T^p-T}{p}}(1+Y^{p^2})^{\frac{T^{p^2}-T^p}{p^2}}\cdots = \sum_{m=0}^{\infty} P_m(T)Y^m$$

where $P_m(T) \in \mathbb{Q}_p[X]$ has degree $\geq m$. Thus

$$F(T,Y) = \sum_{m=0}^{\infty} \alpha_m(Y)T^m$$

where $\alpha_m(Y)$ is a formal series whose first term has degree $\geq m$, with coefficients in $\mathbb{Z}_p$.

Indeed, each term in the binomial series $(1+Y^{p^n})^{\frac{T^{p^n}-T^{p^{n-1}}}{p^n}}$:

$$\Big(\frac{T^{p^n}-T^{p^{n-1}}}{p^n}\Big)\Big(\frac{T^{p^n}-T^{p^{n-1}}}{p^n}-1\Big)\dots\Big(\frac{T^{p^n}-T^{p^{n-1}}}{p^n}-k+1\Big)\frac{Y^{p^n k}}{k!}$$

has a degree $\leq p^n k$ on T, $p^n k$ exponent of Y.

We have $\lambda = \varepsilon - 1$ and $\mathrm{ord}(\lambda) = \frac{1}{p-1}$.

Set:

$$\theta(T) = F(T,\lambda) = \sum_{m=0}^{\infty} \beta_m T^m,$$

with $\beta_m = \alpha_m(\lambda)$ (this series converges as $\mathrm{ord}(\lambda) > 0$ by lemma 4.1.1).

We have as said above $\alpha_m(Y)$ starts with Y^m so

$$\mathrm{ord}(\beta_m) \geq \mathrm{ord}(\lambda^m) = \frac{m}{p-1}. \tag{2.6}$$

Therefore the series θ converges in the disc $\mathrm{ord}(T) > \frac{-1}{p-1}$.

Recall that

$$\mathrm{Tr}(t) = t + t^p + \dots + t^{p^{s-1}} \in \mathbb{Z}_p.$$

We have

$$(1+Y)^{\mathrm{Tr}(t)} = F(t,Y)F(t^p,Y)\cdots F(t^{p^{s-1}},Y).$$

Indeed,

$$F(t,Y)F(t^p,Y)\cdots F(t^{p^{s-1}},Y) = (1+Y)^t(1+Y^p)^{\frac{t^p-t}{p}}\cdots(1+Y)^{t^p}(1+Y^p)^{\frac{t^{p^2}-t^p}{p}}\cdots$$
$$(1+Y)^{t^{p^{s-1}}}(1+Y^p)^{\frac{t^{p^s}-t^{p^{s-1}}}{p}}\cdots$$
$$= (1+Y)^{t+t^p+\dots+t^{p^{s-1}}}(1+Y^p)^{\frac{t^{p^{s-1}}-t}{p}}(1+Y^{p^2})^{\frac{t^{p^{s+1}}-t^p}{p^2}}\cdots$$

Since $t^{p^s} = t$,

$$F(t,Y)F(t^p,Y)\cdots F(t^{p^{s-1}},Y) = (1+Y)^{\mathrm{Tr}(t)}.$$

Then by substitution with $Y = \lambda$ we have

$$(1+\lambda)^{\mathrm{Tr}(t)} = \theta(t)\theta(t^p)\cdots\theta(t^{s-1})$$

which gives $\varepsilon^{\mathrm{Tr}(t)} = \theta(t)\theta(t^p)\cdots\theta(t^{s-1})$. As ε is a p-th root of unity, we can reduce $\mathrm{Tr}(t)$ modulo p, this gives us $\mathrm{Tr}(a)$. Therefore we obtain

$$\varepsilon^{\mathrm{Tr}(a)} = \theta(t)\theta(t^p)\cdots\theta(t^{s-1}).$$

Finally, the coefficients of $\theta(T)$ belong to $\mathbb{Z}_q[\varepsilon]$ since we already know $F(T,\lambda) \in \mathbb{Z}_q[\lambda][[T]]$ and since $\mathbb{Z}_q[\lambda] = \mathbb{Z}_q[\varepsilon]$.

In conclusion, we have constructed a p-adic power series $\theta(T) = \sum_{m=0}^{\infty} \beta_m T^m$ with $\mathrm{ord}(\beta_m) \geq \frac{m}{p-1}$ such that $\varepsilon^{\mathrm{Tr}(a)} = \theta(t)\theta(t^p)\cdots\theta(t^{s-1})$ where $t = [a]$ the Teichmüller representative of $a \in \mathbb{F}_q$. □

4.2 Infinite matrices: Trace and determinant

Let L be a field and let n be an integer. Let $u = (u_1, \ldots, u_n) \in \mathbb{Z}^n$ and $X = (X_1, \ldots, X_n)$ be n variables, X^u is defined by the monomial $X_1^{u_1} \ldots X_n^{u_n}$. We say that $u \geq 0$ if for all i, $u_i \geq 0$ and put $c(u) = \sum_{i=0}^{n} u_i$. Let $E = L[[X]]$ the ring of formal series. For each element $G \in E$, we define an endomorphism of E: $f \mapsto G.f$ again denoted G.

We define ψ_q, $q \in \mathbb{N}_{\geq 2}$ another endomorphism of E by

$$\psi_q\Big(\sum_{v\geq 0} a_v X^v\Big) = \sum_{v\geq 0} a_{qv} X^v.$$

Let $G = \sum_{v\geq 0} g_v X^v$, the composition of ψ_q and G, $\psi_q \circ G$, is again an endomorphism of E. It is represented by the infinite matrix defined by $(g_{qv-u})_{u,v}$. We have the following properties:

- $\psi_q \circ \psi_{q'} = \psi_{qq'}$ (P_1)
- $G \circ \psi_q = \psi_q \circ G_q$ where $G_q(X) = G(X^q)$. (P_2)

Now consider $L = \Omega$ and a set

$$R = \{G = \sum_{v\geq 0} g_v X^v \in \Omega[[X]] | (\exists M > 0)(\forall v \geq 0), \mathrm{ord}(g_v) \geq M c(v)\}.$$

Let's recall the definition of a trace of a matrix. Let V a finite dimensional vector space over a field F, f a linear map $V \to V$ and $\{a_{ij}\}_{1\leq i,j\leq n}$ be the matrix of f over a basis. Then the trace of this matrix is the sum of all the diagonal entries: $\mathrm{Tr}(f) = \sum_{i=1}^{n} a_{ii}$. In the following, we extend this for some infinite matrices which is important for us.

Proposition 4.2.1. *Let $G \in R$ and let $\psi = \psi_{q,G}$. Then $\mathrm{Tr}(\psi^s)$ converges and for all integers $s \geq 1$*

$$(q^s - 1)^n \,\mathrm{Tr}(\psi^s) = \sum_{x^{q^s-1}=1} G(x)G(x^q)\cdots G(x^{q^{s-1}}),$$

where $x = (x_1, \ldots, x_n)$, $x_i \in \Omega$, and $x^{q^s-1} = 1$ means that, $x_i^{q^s-1} = 1$ for all $1 \leq i \leq n$.

Proof. 1. Case $s = 1$. First, by the definition of a trace of matrix we have

$$\mathrm{Tr}(\psi) = \sum_{u} g_{(q-1)u}$$

this series is convergent since $G \in R$.
On the other hand, $\sum_{x^{q-1}=1} G(x) = \sum_{x^{q-1}=1,\, v\geq 0} \sum g_v x^v$. We have

$$\sum_{v_i \geq 0} x^{v_i} = \begin{cases} q-1 \text{ if } q-1 \text{ divides } v_i \\ 0 \text{ otherwise} \end{cases}$$

for every $i = 1, 2, \ldots, n$. Therefore,

$$\sum_{v\geq 0} x^v = \sum_{v\geq 0} \prod_{i=1}^{n} x_i^{v_i} = \prod_{i=1}^{n} \sum_{v_i \geq 0} x_i^{v_i} = \begin{cases} (q-1)^n \text{ if } q-1 \text{ divides } v_i \text{ for all } i \\ 0 \text{ otherwise.} \end{cases}$$

Hence,

$$\sum_{x^{q-1}=1} G(x) = \sum_{v\geq 0} g_v \sum_{x^{q-1}=1} x^v = (q-1)^n \sum_{u\geq 0} g_{(q-1)u} = (q-1)^n \,\mathrm{Tr}(\psi).$$

2. General case $s > 1$. Since $\psi^s = \underbrace{\psi_q \circ G \circ \psi_q \circ G \circ \cdots \circ \psi_q \circ G}_{s \text{ times}} = \psi_q \circ \psi_q \circ G_q \circ G \circ \psi^{s-2}$

and then we have by the properties (P_1) and (P_2) :

$$\begin{aligned}\psi^s &= \psi_{q^2} \circ G.G_q \circ \psi^{s-2} = \psi_{q^2} \circ \psi_q \circ (G.G_q)_q G \circ \psi^{s-3} \\ &= \psi_{q^3} \circ G.G_q.G_{q^2} \circ \psi^{s-3} = \cdots = \psi_{q^s} \circ G.G_q.G_{q^2} \cdots G_{q^{s-1}} \\ &= \psi_{q^s, G.G_q.G_{q^2} \cdots G_{q^{s-1}}}.\end{aligned}$$

So we get the result by substituting q by q^s and G by the product $G.G_q.G_{q^2} \cdots G_{q^{s-1}}$ in the first case.

□

Lemma 4.2.2. Let K be a field, V a finite dimensional K-vector space and $\psi \in \mathrm{End}_K(V)$. Then $\det(\mathrm{Id}_V - T\psi) = \exp\Big(-\sum_{s=1}^{\infty} \mathrm{Tr}(\psi^s)\frac{T^s}{s}\Big)$.

Proof. We may assume that K is algebraically closed and $V = K^n$. Then ψ is given by a matrix $M \in M_n(K)$. So we have to show that $\log\det(\mathrm{Id}_n - TM) = -\sum_{s=1}^{\infty} \mathrm{Tr}(M^s)\frac{T^s}{s}$.

We know from linear algebra that when $K = \overline{K}$, every matrix $n \times n$ is triangularizable: we can arrange to find a basis in such a way that M is upper triangular. So we have

$$M = \begin{pmatrix} \lambda_1 & & & * \\ & \lambda_2 & & \\ & & \ddots & \\ & 0 & & \lambda_n \end{pmatrix} \text{ and } \mathrm{Id}_n - TM = \begin{pmatrix} (1-T\lambda_1) & & & * \\ & (1-T\lambda_2) & & \\ & & \ddots & \\ & 0 & & (1-T\lambda_n) \end{pmatrix}$$

So the determinant is $\det(\mathrm{Id}_n - TM) = (1-T\lambda_1)(1-T\lambda_2)\cdots(1-T\lambda_n)$.

Therefore, we have

$$\log\det(\mathrm{Id}_n - TM) = \sum_{i=1}^{n} \log(1-T\lambda_i) = -\sum_{i=1}^{n}\sum_{s=0}^{\infty} \frac{(T\lambda_i)^s}{s}.$$

In other hand, we recall that the product of upper triangular matrices is an upper trian-

gular matrix so M^s is an upper triangular matrix and we have $\mathrm{Tr}(M^s) = \sum_{i=1}^{n} \lambda_i^s$. Hence

$$\log \det(\mathrm{Id}_n - TM) = -\sum_{s=0}^{\infty} \mathrm{Tr}(M^s)\frac{T^s}{s}.$$

Thus we get the result. □

Lemma 4.2.3. Let $G \in R$ and $\psi = \psi_{q,G}$. Then we have:

(i) $\det(\mathrm{Id_E} - T\psi) = \exp\Big(-\sum_{i=1}^{\infty} \mathrm{Tr}(\psi^s)\frac{T^s}{s}\Big)$,

(ii) The radius of convergence of the power series $\det(\mathrm{Id_E} - T\psi)$ is infinite.

Proof. (i) Follows from the previous lemma by passing to the limit.

(ii) By (i) we have $\det(\mathrm{Id} - T\psi) = \exp\Big(-\sum_{i=1}^{\infty} \mathrm{Tr}(\psi^s)\frac{T^s}{s}\Big)$: a power series, written as

$$\det(\mathrm{Id} - T\psi) = \sum_{m=0}^{\infty} \alpha_m T^m,$$

with $\alpha_m = (-1)^m \sum \mathrm{sgn}(\sigma)\psi_{u_1,\sigma(u_1)}$ (where σ runs along the permutations of the u_i).

We must prove that $\frac{\mathrm{ord}(\alpha_m)}{m} \to \infty$ when $m \to \infty$.
Since $\psi \in R$ then we have $\mathrm{ord}(\alpha_m) \geq M(q-1)\inf\Big(\sum_{i=1}^{m} c(u_i)\Big)$. Put $d_m = \inf\Big(\sum_{i=1}^{m} c(u_i)\Big)$ where the infimum is taken over all the $u's$ which are positive and distinct. So we need to prove that $\frac{d_m}{m} \to \infty$ when $m \to \infty$.

We can arrange the sequence $u_i's$ in order to have $c(u_i) \leq c(u_{i+1})$, so we obtain $d_m = \sum_{i=1}^{m} c(u_i)$ and also $c(u_m)$ tends to ∞. Therefore $d_m \to \infty$, hence $\frac{d_m}{m} \to \infty$.

□

4.3 Analytic expression of zeta function and proof of theorem 1.1.8

Recall that we reduced the proof of theorem 1.1.8 to the case where V is an hypersurface defined by one equation $f(x) = 0$ where $f \in \mathbb{F}_p[X_1, \cdots, X_n]$. Arguing as in paragraph 1.2 and proceeding by induction on $\dim V$, we may remove from V its intersections with the coordinates hyperplanes, so we have

$$N_s = \#V(\mathbb{F}_p) = \#\{x \in \mathbb{F}_p^n |\ f(x) = 0 \text{ and } x^{p^s-1} = 1\}$$

where as before, $x^{p^s-1} = 1$ means that $x_i^{p^s-1} = 1$ for every $1 \leq i \leq n$.

Let's fix $s \geq 1$. For all $a \in \mathbb{F}_{p^s}$, let $\theta_s(a) = \varepsilon^{\mathrm{Tr}(a)}$ (with ε is a primitive p-th root of unity). Let $t = [a]$ be the Teichmüller representatives of a. We have seen in the examples 2.3.5 that θ_s is a non trivial character of $\mathbb{F}_{p^s}$ and so by using proposition 4.1.7 we have

$$\theta_s(a) = \theta(t)\theta(t^p)\cdots\theta(t^{p^{s-1}}). \tag{4.1}$$

Proposition 4.3.1. *Let ε be a primitive p-th root of unity. Then we have:*

$$\sum_{x_0 \in \mathbb{F}_{p^s}^\times} \theta_s(x_0 u) = \begin{cases} p^s - 1 \text{ if } u = 0 \\ -1 \text{ otherwise.} \end{cases}$$

Now we apply (4.3.1) by the change $u = f(x)$:

$$\sum_{x_0 \in \mathbb{F}_{p^s}^\times} \theta_s(x_0 f(x)) = \begin{cases} p^s - 1 \text{ if } f(x) = 0 \\ -1 \text{ otherwise.} \end{cases}$$

We sum this equality over all $x \in (\mathbb{F}_{p^s}^\times)^n$, and then we have:

$$\sum_{x \in (\mathbb{F}_{p^s}^\times)^n,\, x_0 \in \mathbb{F}_{p^s}^\times} \theta_s(x_0 f(x)) = p^s N_s - (p^s - 1)^n. \tag{4.2}$$

We express $X_0 f(X)$ as a finite sum of monomials $\sum_{w \in I} a_w X^w$ in $n+1$ variables $X = (X_0, X_1, \cdots X_n)$, where $a_w \in \mathbb{F}_p$.

Therefore the equality 4.2 becomes

$$p^s N_s = (p^s - 1)^n + \sum_{x^{p^s-1}} \prod_{w \in I} \theta_s(a_w x^w). \tag{4.3}$$

Let A_w, y in $\mathbb{Z}_p$ be the Teichmüller representatives of a_w and x respectively. Using the equalities (4.3) and (4.1) we get

$$p^s N_s = (p^s - 1)^n + \sum_{x^{p^s-1}} \prod_{w \in I} \prod_{j=0}^{s-1} \theta(A_w x^{p^j w}). \tag{4.4}$$

Put

$$G(X) = \prod_{w \in I} \theta(A_w X^w), \tag{4.5}$$

we obtain:

$$p^s N_s = (p^s - 1)^n + \sum_{x^{p^s-1}} G(x) G(x^p) \cdots G(x^{p^{s-1}}). \tag{4.6}$$

By construction of θ we can see that $\theta(A_w X^w) \in R$ so does $G(X)$. Therefore we can apply proposition 4.2.1 with $q = p$, we have:

$$p^s N_s = (p^s - 1)^n + (p^s - 1)^{n+1} \operatorname{Tr}(\psi^s) \tag{4.7}$$

$$= \sum_{i=0}^{n} (-1)^i \binom{i}{n} p^{s(n-i)} + \sum_{i=0}^{n+1} (-1)^i \binom{i}{n+1} p^{s(n+1-i)} \operatorname{Tr}(\psi^s). \tag{4.8}$$

Put

$$\Delta(T) = \det(\mathrm{Id} - T\psi) = \exp\Big(- \sum_{i=1}^{\infty} \operatorname{Tr}(\psi^s) \frac{T^s}{s} \Big).$$

Multiplying 4.7 by $\frac{T^s}{s}$ and summing gives

$$Z_V(pT) = \prod_{i=0}^{n} (1 - p^{n-i} T)^{(-1)^{i+1} \binom{i}{n}} \prod_{i=0}^{n+1} \Delta(p^{n+1-i} T)^{(-1)^{i+1} \binom{i}{n+1}}.$$

As we have seen in proposition (4.2.3), Δ converges in Ω. Hence Z_V is meromorphic in Ω. Thus by proposition (3.2.4) Z_V is rational.

References

[1] B. Dwork, "On the rationality of the zeta function of an algebraic variety," 1960.

[2] L. Qing, "Algebraic geometry and arithmetic curves," 2006.

[3] G. Peyré, *L'algèbre discrète de la transformée de Fourier*, 2004.

[4] Y. Amice, *Les nombres p-adiques.* Presses universitaires de France, 1975.

[5] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta- Functions.* Graduate Text in Mathematics, 2012.

Acknowledgments

First of all, a special thanks goes to God almighty, who give strength and healthy body and intelligence throughout my whole study.
I express my sincere gratitude and appreciation to my supervisor Prof. Olivier Brinon for having spend a lot of time on this thesis, for his numerous help and explanations and for his patience.
Thanks to all the staff members of Algant for their warm welcoming and to Erasmus and the University of Padova for funding my studies.
I would like to thank all the lecturers in Padova and in Bordeaux who have taught me and broadened my knowledge.
I thank my family and friends for their support, encouragements and prayers in all the challenges. My deepest thanks to my love, my fiancé Jean Claude for his comprehension and being always by my side.