

THE WEIL CONJECTURES

ZHIWEN DONG

ABSTRACT. This is a memoir of M1 at Sorbonne Université for a TER project on the Weil conjectures under the supervising of professor Jean-François Dat. We give a introduction on the background and the applications of Weil conjectures and provide Dwork's original proof of the rationality of zeta function using p -adic analysis methods, essentially following Colmez, Dwork, Koblitz, Serre and Tao.

CONTENTS

1. Introduction	1
2. Dwork's proof	6
2.1. Preliminaries of p -adic analysis	6
2.2. Reduction of the problem	13
2.3. Criteria of rationality	14
2.4. Θ function	16
2.5. Trace and determinant for infinite matrices	18
2.6. End of the proof	20
Acknowledgements	21
References	21

1. INTRODUCTION

Our story began from the *Disquisitiones Arithmeticae* (1801) of Gauss, where Gauss introduced the Gauss sum and gave one of his proofs of the law of quadratic reciprocity using the Gauss sum.

In the terms of motives considered by Grothendieck, or more generally the theory of exponential motives, we can give the definition of exponential sum as follows.

Let p be a prime number, K a finite field of characteristic p with q elements, $K \subset K_n \subset \overline{K}$, where K_n/K is the unique field extension of degree n . Let X be a smooth algebraic variety over K , and $f : X \rightarrow \mathbb{A}_K^1$ a regular function. We choose a non trivial additive character (the choice is not canonical) $\Psi : (K, +) \rightarrow (\mathbb{C}^\times, \times)$, then Ψ induces a character $\Psi_n :$

$$\begin{aligned} \Psi_n : K_n &\rightarrow \mathbb{C}^\times \\ x &\mapsto \Psi(\text{Tr}_{K_n/K}(x)) \end{aligned}$$

Definition 1.1. Under the above notations, a exponential sum $S_n(X, f, \Psi)$ is defined by :

$$S_n(X, f, \Psi) := \sum_{x \in X(K_n)} \Psi_n(f(x)).$$

We note that each summand is a q -th root of the unit.

Example 1.2. If we take $f = 0$, then the exponential sum is the point-counting function:

$$S_n(X, f, \Psi) = |X(K_n)|.$$

We will see that this is our case of ζ function

Example 1.3. Let $X = \mathbb{A}_K^1$, and $f = X^2$, we get the quadratic Gauss sum:

$$S_n(X, f, \Psi) = \sum_{x \in K_n} \Psi(x^2).$$

If we further pose $n = 1$ and $K = \mathbb{F}_p$, then we have the exact value of Gauss sums for the Legendre symbols.

Theorem 1.4. (Gauss)

$$\sum_{x \in \mathbb{F}_p} \Psi(x^2) = \sum_{x \in \mathbb{F}_p} (1 + (\frac{x}{p}))\Psi(x) = \sum_{x \in \mathbb{F}_p} (\frac{x}{p})\Psi(x) = \begin{cases} \sqrt{p} & p \equiv 1 \pmod{4} \\ i\sqrt{p} & p \equiv 3 \pmod{4} \end{cases}.$$

However, it's extremely rare to be able to obtain a closed formula like this. The following theorem shows that apart from the two special point $1, i$ given by Gauss, the coefficients are uniformly distributed on $\mathbb{S}^1$.

Theorem 1.5. (Deligne, Katz) As $p \rightarrow \infty$, these points are uniformly distributed on $\mathbb{S}^1$ if est, for every continuous function $\varphi : \mathbb{S}^1 \rightarrow \mathbb{C}$,

$$\int_{\mathbb{S}^1} \varphi(x) \mu(x) = \lim_{p \rightarrow \infty} \frac{1}{p-2} \sum_{\chi \in \widehat{\mathbb{F}_p^\times}} \varphi(\theta_{\chi,p}).$$

where $\theta_{\chi,p} = \frac{G(\Psi, \chi)}{\sqrt{p}}$, and $G(\Psi, \chi) = \sum_{x \in \mathbb{F}_p} \Psi(x) \chi(x)$ is the Gauss sum.

Example 1.6. Let $X = \mathbb{G}_m$, $f = X + \frac{a}{x}$, and $a \in K^\times$, we get the Kloosterman sum.

$$S_n(X, f, \Psi) = \sum_{x \in K^\times} \Psi(x + \frac{a}{x}) =: \text{Kl}_2(a, |K|).$$

Here, we take $\Psi(x) = e^{\frac{2i\pi x}{p}}$. We have the following generalization:

$$\text{Kl}_n(a, |K|) := \sum_{x_1 \dots x_n = a} \Psi(x_1 + \dots + x_n).$$

The Kloosterman sum have a optimal bound.

Theorem 1.7. (Weil bound)

$$\text{Kl}_2(a, |K|) \leq 2\sqrt{|K|}.$$

Our story of exponential sums should continue with the following slogan:

$$S_n(X, f, \Psi) = \sum_{x \in X(K_n)} \Psi(f(x)) = \sum_i (-1)^i \text{Tr}(\text{Fr}^* | H_c^i(X_{\overline{K}}, f^* \mathcal{L}_\Psi)).$$

Which indicates that the exponential sum is the alternating sum of the traces of the geometric Frobenius acting on $H_c^i(X_{\overline{K}}, f^* \mathcal{L}_\Psi)$.

This is in fact a direct application of the Grothendieck-Lefschetz fixed point formula, where the cohomology groups are the ℓ -adic étale cohomology of compact support.

We now give the definition of Artin-Schreier sheaves, which leads to the geometric interpretation of the exponential sum, we consider étale fundamental group and étale sheaves.

We consider the Artin-Schreier covering of the affine line:

$$\begin{aligned} \wp_0 : \mathbb{A}_K^1 &\rightarrow \mathbb{A}_K^1 \\ x &\mapsto x^{|K|} - x. \end{aligned}$$

This defines a geometrically irreducible, étale Galois covering of $\mathbb{A}_K^1$. The Galois group of this covering is canonically isomorphic to the additive group K . It is a quotient group of the fundamental group $\pi_1(\mathbb{A}_K^1, \bar{x})$, for some fixed base point $\bar{x}$. Hence any character $\Psi : K \rightarrow \overline{\mathbb{Q}}_l^\times \simeq \mathbb{C}^\times$ induces a character

of this fundamental group and thus defines an étale local system of rank 1 noted $\mathcal{L}_\Psi$, which is called the *Artin-Schreier sheaf*.

For any element $x \in K$, and Ψ be a non trivial character let Ψ_x denote the character

$$\begin{aligned}\Psi_x : K &\rightarrow \overline{\mathbb{Q}_l}^\times \\ y &\mapsto \Psi(xy).\end{aligned}$$

Then $x \mapsto \Psi(x)$ identifies the additive group of the base field K and the character group of the Artin-Schreier extension defined by $\wp_0$.

Remark 1.8. *Let Ψ be a nontrivial character of K , then*

$$\wp_{0*}(\overline{\mathbb{Q}_l}) = \bigoplus_{x \in K} \mathcal{L}_{\Psi_x}$$

In fact the statement is not that closely related to the étale cohomology, but rather a theory of *Weil cohomology*, which demands a finiteness theorem, a Kunneth formula, the Poincaré's duality theorem, the theory of algebraic cycles and a Lefschetz fixed point formula, results similar to the cases of the Betti or the De Rham cohomology. The ℓ -adic étale cohomology, is the first Weil cohomology constructed by Grothendieck. But this is not the only known Weil cohomology, in fact the crystalline and rigid cohomology are also Weil cohomologies for schemes or algebraic varieties, in which case we talk about isocrystals and Dwork isocrystal (or Artin-Schreier isocrystals) in place of étale $\overline{\mathbb{Q}_l}$ sheaves and Artin Schreier sheaves mentioned above. Without specific indication, we always consider the ℓ -adic étale cohomology.

Remark 1.9. (6-functor formalism) *To be more precise, in a more categorical point of view, the Kunneth formula, and the Poincaré's duality theorem are more of a corollary of the 6-functor formalism, id est the 3-functors $\otimes$, f^* , and $f_!$, combined with the existence of their right adjoint $\underline{\mathrm{Hom}}$, f_* , $f^!$ with certain comptability conditions, namely the functoriality, f^* commutes with $\otimes$, the proper base change theorem, and the projection formula.*

Formally, a 3-functor formalism is a lax symmetric monoidal functor $\mathcal{D} : \mathrm{Corr}(C, E) \rightarrow \mathrm{Cat}_\infty$. Moreover, to recover the 6-functor formalism, one can reduce to the case of the construction of a lax symeetric monoidal functor $\mathcal{D}_0 : \mathrm{Corr}(C, \mathrm{Isom}) \simeq C^{op} \rightarrow \mathrm{Cat}_\infty$ imposing conditions on classes I , and P , and that $f_!$ is the left (resp.right) adjoint of f^ if f in I (resp. P).*

We can now talk about generating sums (ζ functions)

Definition 1.10. *Under the above assumptions, we define for the number counting function or exponential sums the ζ function.*

$$Z(X, T) := \exp\left(\sum_{n=1}^{\infty} |X(K_n)| \frac{T^n}{n}\right)$$

$$Z(X, f, \Psi, T) := \exp\left(\sum_{n=1}^{\infty} S_n(X, f, \Psi) \frac{T^n}{n}\right).$$

Example 1.11. *For $X = \mathrm{Spec}(K)$,*

$$Z(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n}\right) = \frac{1}{1-T}.$$

Let P be a closed point of X , $N(P) = |\kappa_P|$ the number of elements of the residue field, $\deg(P) = d$ is the degree of this extension, id est $N(P) = q^{\deg(P)}$. We consider the conjugates of the K_d -points P , they are $P = P_1, \dots, P_d$, by definition $P = (p_1, \dots, p_n)$, $p_{i,j} = \sigma(p_i)$ for $j = 1, \dots, d$, these points are different, in fact if there exist some $j \neq 1$ such that $\sigma_j(p_i) = p_i$ for all $i = 1, \dots, n$, then P lies in a smaller field, the fixed field of σ_j .

Since $K_d \subset K_n$ if and only if $d|n$ (K_n is the fixed point of $X^{qn} - 1 = 0$, and $(X^{qd} - 1)|(X^{qn} - 1)$ if and only if $d|n$), the contribution of these points occurs only in $K_d, K_{2d} \dots$, hence

$$\exp\left(\sum_{j=1}^{\infty} d \frac{T^{jd}}{jd}\right) = \frac{1}{1 - T^d}$$

Remark 1.12. *In the above notions, we have*

$$Z(X, T) = \prod_P \frac{1}{1 - T^{\deg(P)}}.$$

In particular, $Z(X, T)$ has positive integer coefficients.

Remark 1.13. *If we do a change of variables $T = q^{-s}$, then*

$$\zeta(s) = \prod_P \frac{1}{1 - N(P)^{-s}}.$$

This Euler product resemble the definition of a Dedekind ζ function.

By our interpretation of the exponential sum as a trace, we can use the important identity for arbitrary matrices M that $\det(\exp(M)) = \exp(\text{Tr}(M))$, hence the logarithmic derivative of $\det(1 - t\phi)^{-1}$ is $\sum_{v=1}^{\infty} \text{Tr}(\phi^v) t^{-1}$

Theorem 1.14. (Dwork, Grothendieck) (The first Weil conjecture) *For separate scheme of finite type X , $Z(X, T)$ is a rational function.*

Moreover, we have for d the dimension of X

$$Z(X, T) = \prod_{i=0}^{2d} \det(1 - \text{Fr}_K T | H_c^i(X_{\overline{K}}, \overline{\mathbb{Q}}_{\ell})^{(-1)^i})$$

$$Z(X, f, \Psi, T) = \prod_{i=0}^{2d} \det(1 - \text{Fr}_K T | H_c^i(X_{\overline{K}}, f^* \mathcal{L}_{\Psi})^{(-1)^i}).$$

Definition 1.15. (Hasse-Weil L -function) *Let X be a smooth projective variety over $\mathbb{Q}$, then for almost all prime number p is est ($p \notin S, S$ finite), the reduction modulo p , $X_{\mathbb{F}_p}$ is smooth projective. Fix a degree i , we define :*

$$P_{p,i}(T) := \det(1 - \text{Fr}_K T | H_c^i(X_{\overline{K}}, \overline{\mathbb{Q}}_{\ell}))$$

and the Euler product :

$$L(H^i(X), s) := \prod_{p \notin S} \frac{1}{P_{p,i}(p^{-s})}.$$

We find the Riemann ζ function as follows:

Example 1.16. *For $X = \text{Spec}(\mathbb{Q}), X_{\mathbb{F}_p} = \text{Spec}(\mathbb{F}_p)$,*

$$L(H^0(X), s) = \prod_p \frac{1}{1 - p^{-s}} = \prod_p Z(X_{\mathbb{F}_p}, p^{-s}) = \zeta(s).$$

This also explain why we define the Z function as above.

Remark 1.17. *The Hasse-Weil L -function defined above converges absolutely and hence defines a holomorphic function on $\{\Re(s) > 1 + \frac{i}{2}\}$.*

Conjecture 1.18. *$L(H^i(X), s)$ has a meromorphic continuation to the complex plane.*

The only known case for this conjecture is the case of dimension 0, and some cases of dimension 1. Apart from the genus 0 cases, the genus 1 case is a consequence of the modularity of elliptic curves, proved by Wiles et al., which the semistable case is used as a crucial part of his famous proof for the Fermat's Last Theorem. The case of genus 2 curves is proved by Boxer, Calegari, Gee and Pilloni in 2021.

For the cases above, to modify the modularity or potentially modularity for elliptic curves or abelian surfaces. This is historically the beginning of the Langlands program, aiming to attach an automorphic form for motivic L functions or for suitable Galois representations, for we know the functional equation for L functions of automorphic forms. The Langlands original conjecture will allow us to obtain the Hasse-Weil conjecture on the motive or Galois representation side and the Ramanujan-Petersson conjecture on the automorphic forms side.

We can associate the Hasse-Weil L -function with factors at bad primes and factors at infinity.

Conjecture 1.19. (Functional equation)

$$\Lambda(H^i(X), s) = \pm \Lambda(H^i(X), i + 1 - s).$$

Theorem 1.20. (Grothendieck, Deligne) (the second and the third Weil conjectures) *Let X be a smooth projective variety over $\mathbb{F}_q$, then we have the functional equation:*

$$Z(X, \frac{1}{q^d T}) = \varepsilon q^{\chi d/2} T^\chi Z(X, T).$$

where $\varepsilon = \pm 1$ and $\chi = \sum_i (-1)^i B_i$ the Euler-Poincaré characteristic.

(Riemann hypothesis) *For every i , $P(T) := \det(1 - \text{Fr}_K T | H_c^i(X, \overline{\mathbb{Q}}_\ell))$ have integer coefficients independent of ℓ . The complex roots α of this polynomial (The eigenvalues of Fr) have absolute value $|\alpha| = q^{i/2}$*

It's always interesting to talk about conjecture of type Riemann Hypothesis, the only known cases are on function fields and finite fields. Hasse has proved the case of elliptic curve, Weil the case of function fields and general curves, and finally Deligne the case of smooth projective varieties using the theory of Lefschetz pencil and later Deligne has generalised his proof to a weight theory and gave several important applications like the Ramanujan conjecture and the BBDG decomposition theorem for perverse sheaves using the hard Lefschetz theorem.

The Riemann hypothesis and hard Lefschetz have applications in a rather optimal estimation of the number of points in $\mathbb{F}_q$, and in the curve case, these estimations, namely the Hasse-Weil bounds can even prove the Riemann hypothesis.

Let $N = |X(K)|$ the number of K -point of X .

Theorem 1.21. (Hasse bound) *If X is an elliptic curve over a finite field $K = \mathbb{F}_q$, then*

$$|N - q - 1| \leq 2\sqrt{q}.$$

One can use the Hasse bound to prove the Riemann Hypothesis for elliptic curves. The proof by Tate pairing and Tate modules is discussed in the elliptic curves courses given by Javier Fréan or Jean-François Dat.

Theorem 1.22. (Hasse-Weil bound) *If X is a curve of genus g over a finite field $K = \mathbb{F}_q$, then*

$$|N - q - 1| \leq 2g\sqrt{q}.$$

Once again, one can apply the Hasse-Weil bound to obtain the analogue of Riemann hypothesis for curves. A proof using the Hodge index theorem is given in the course on cohomology of coherent sheaves on schemes by Matteo Tamiozzo.

Remark 1.23. *As a consequence of the Deligne's theorem, the Hasse-Weil bound of rational points, the Weil bound for Kloosterman sum and the equidistribution theorem of Gauss sum can all be generalised to higher dimension.*

We shall end the introduction with a brief remark on the analytic properties, *id est* residue or the vanishing order at $s = 1$. We remind that $q^{-s} = T$. In the case of Riemann ζ function or the Dedekind ζ function, the result is the class number formula, and in our case of Weil conjectures, this can be computed explicitly by the closed formula. However, for the vanishing of global Hasse-Weil L -function of elliptic curves, it is the BSD conjecture, consisting three parts. The first part is that $\text{rank} E(K) = \text{ord}_{s=1} L(E, s)$, the second part is that the Tate-Shafarevich group is finite, and the last one is an analogy of the class number formula. One generalise the problem of class number formula to the Bloch-Kato conjecture for motives, indeed the first BSD conjecture is equivalent to the Bloch-Kato conjecture under the assumption of the second BSD conjecture. There's also the p -adic version of this problem, the Kubota-Leopoldt p -adic L -function, is linked to the arithmetic and algebraic version by the Iwasawa main conjecture, there the vanishing order at 1 is the p -adic BSD conjecture, some cases are known using the p -adic hight pairing.

2. DWORK'S PROOF

Dwork has given the first proof of the rationality of ζ function which merited him the Cole prize in number theory in 1962. Dwork's original proof used the method of p -adic analysis that in first sight looks different compared to the theory of Weil cohomology and the Lefschetz fixed point formula. Another remarkable point is that the proof of Dwork works already for seperate algebraic varieties *id est* algebraic varieties defined by a finite covering of affine varieties whose intersection is affine, exempli grata projective varieties or affine varieties *without the smooth assumption!* The proof is rather direct, we find a suitable criteria of rationality and apply it to the zeta function $Z(X, T)$. However, using such a criteria will make our rational function implicit in some extend, but it's nonetheless elementary and economic compared to the proof of Grothendieck. Furthermore, the Dwork's proof is in fact effective, one can do numerical calculations with methods used by Dwork. Last but not least, The method of Dwork is later generalised into the theory of crystalline cohomology and rigid cohomology, that can also lead to Weil II.

2.1. Preliminaries of p -adic analysis. Here we give the construction of the algebraically closed complete field $\mathbb{C}_p$ using a generalised form of the Hensel's lemma, then talk about the Teichmüller lifting and the p -adic Weierstrass preparation theorem.

Let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ for the p -adic norm (ring of Cauchy sequences quotient by the ideal of Cauchy sequences that converge to 0), and $\mathbb{Z}_p$ the ring of elements with positive valuation. We consider norms in the topological sense, a norm is said to be ultrametric if the metric it satisfies $|x + y| \leq \max\{|x|, |y|\}$. An ultrametric field is a normed field whose norm is ultrametric.

Analogously, one can define the notion of valuation, here in our case, our valuation can by definition be embedded in the totally ordered abelian group $\mathbb{R}_{>0}$, hence we're in height at most one case, which by definition indicates that our valuation is of rank lesser than 1, in fact the rank 0 is the trivial case, hence we have *the equivalence between the notion of topological nilpotent and norm strictly lesser than 1*.

Example 2.1. For the lexicographic order for $\mathbb{R}^2$, the height of $\mathbb{R}^2$ is 2 so is the rank of the lexicographic order. In this case, and (x is topological nilpotent) $\Rightarrow (|x| < 1)$, **but the reciprocal is false.** It is also false that (x^n bounded) $\Rightarrow (|x| \leq 1)$. These phenomenons gave us the motivation of defining adic spaces.

Definition 2.2. Let, K be a ultrametric field, We define the Gauss norm for the ring of polynomials and hence its fraction ring of rational functions. Let $P(X) = \sum_{i=0}^n a_i X^i$, then

$$|P|_G = \sup_i (|a_i|).$$

We also have the analogue definition for the ring of formal series.

Remark 2.3. The Gauss norm is multiplicative.

Definition 2.4. Two norms are said to be equivalent if they induce the same topology.

Proposition 2.5. *Two norms $|\cdot|_1$ and $|\cdot|_2$ are equivalent if there exist a $s \in \mathbb{R}_+^\times$, such that $|x|_1 = |x|_2^s$, for all $x \in K^\times$.*

Proof. Since we're in the case of topological rings, we consider only a basis of nilvoisinages. If a such s exist, one can see easily the homeomorphism or even equality using the logarithm between the open balls.

Suppose that the norms are equivalent, as discussed above, we have the equivalence between (x is topological nilpotent) and ($|x| < 1$), hence we deduce that $(|x|_1 < 1) \Leftrightarrow (|x|_2 < 1)$. Let $K^{\circ\circ}$ denote the set of these topological nilpotent object. If $K^{\circ\circ} = \{0\}$, then the norm is the trivial norm that send every element to 1. We are hence in the case that we can choose $x \in K^{\circ\circ}$, and for all $y \in K^\times, a \in \mathbb{Z}, b \in \mathbb{N}$,

$$|y^b x^{-a}|_1 < 1 \Leftrightarrow |y^b x^{-a}|_2 < 1.$$

Taking logarithm on both sides, we obtain :

$$\{r \in \mathbb{Q}, r < \frac{\log |y|_1}{\log |x|_1}\} = \{r \in \mathbb{Q}, r < \frac{\log |y|_2}{\log |x|_2}\}.$$

The construction of the real numbers by Dedekind cuts tell us that $\frac{\log |y|_1}{\log |x|_1} = \frac{\log |y|_2}{\log |x|_2}$ because they define the same Dedekind cut. Thus, the function $y \mapsto \frac{\log |y|_1}{\log |y|_2}$ is the constant function for all $y \in K^\times$. $\square$

Proposition 2.6. *Let K be a complete normed field and V a K -vector space of finite dimension. Then every norm on V compatible with the norm on K , id est $\forall \lambda \in K, x \in V, \|\lambda x\| = |\lambda| \|x\|$ is equivalent. In particular, V is complete regardless of the norm.*

Proof. It suffice to prove that all norms are equivalent to the norm sup. Do a proof by induction on the dimension of V . In the dimension one case, every norm is trivially equal to the norm sup. Suppose that $n > 1$, let $(e_1 \dots e_n)$ be a basis, then we have the following inequality.

$$\|x_1 e_1 + \dots + x_n e_n\| \leq (\|e_1\| + \dots + \|e_n\|) \sup(|x_1|, \dots, |x_n|)$$

We have thus one direction, we prove by contradiction, suppose that there exist a sequence $x_k = x_{1k} e_1 + \dots + x_{nk} e_n$ that converge to 0 for the norm $\|\cdot\|$ but not for the norm sup, then there exist $C > 0, i \in \{1, \dots, n\}$ such that the sequence x_{ik} satisfy $|x_{ik}| \geq C$. Hence the sequence $v_k = \frac{1}{x_{ik}} x_k \rightarrow 0$ for the norm $\|\cdot\|$, id est $e_i \in \overline{\text{Vect}(e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n)} = \text{Vect}(e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n)$ by completeness, hence we obtain a contradiction since $(e_1, \dots, e_n)$ is a basis. $\square$

There's a generalised version of the proposition 2.6 to topological vector spaces as follows which can give an alternative proof to the theorem 2.20 different from our proof by Hensel's lemma.

Lemma 2.7. *Let K be a complete normed field with non discrete topology, V a Hausdorff topological vector space of finite dimension n , let $(e_1, \dots, e_n)$ be a basis, then the linear bijection $K^n \rightarrow V, (\lambda_1, \dots, \lambda_n) \mapsto \lambda_1 e_1, \dots, \lambda_n e_n$ is a isomorphism of topological vector space.*

In particular, V is isomorphic to K^n as topological vector space.

Proposition 2.8. *Let A be a discrete valuation ring, $K = \text{Frac}(A)$ its fraction ring which is complete for the topologie induced by the valuation. Let L/K be a finite separable extension, B the integral closure of A in L , then B is also a discrete valuation ring, and L is complete for the topology defined by the valuation.*

However, we will not use the approach of using lemma 2.7 to prove proposition 2.8. We'll stick to the normed vector space case and use the Hensel's lemma to prove a equivalent result. We first define the notion of resultant.

Let K be a complete field with a valuation v , and $\mathcal{O}_K$ its ring of integers. We note $K[X]_{\leq s}$ the polynomials with coefficients in K with degree less than s , it is a K vector space of dimension $s + 1$ with the canonical basis $(1, X, \dots, X^s)$.

Definition 2.9. Let $g \in K[X], h \in K[X]$ with degree respectively $\leq n, \leq m$, we note $\theta_{g,h}$ the application from $K[X]_{\leq m-1} \oplus K[X]_{\leq n-1}$ to $K[X]_{\leq m+n-1}$ that send (u, v) to $ug + vh$. We define $\text{Res}(g, h) := \text{Res}_{m,n}(g, h)$ the determinant of the matrix of $\theta_{g,h}$ with respect to the basis (e_m, e_n) and (e_{m+n}) . Without further specification, the resultant is always $\text{Res}_{m,n}(g, h)$.

Lemma 2.10. $\text{Res}(g, h) := \text{Res}_{m,n}(g, h) = 0$ if and only if one or both of the following cases are met.

- (i) $\deg g \leq n - 1$ and $\deg h \leq m - 1$.
- (ii) g and h are not relatively prime.

Proof. If we're in the (i) case, then $\theta_{g,h}(K[X]_{\leq m-1} \oplus K[X]_{\leq n-1}) \subset K[X]_{\leq m+n-2}$. Hence $\theta_{g,h}$ not bijective, and $\text{Res}(g, h) = 0$. If we're in the (ii) case, then let g and h be divisible by w with $\deg w \geq 1$, then $\theta_{g,h}(\frac{h}{w} - \frac{g}{w}) = 0$, hence $\theta_{g,h}$ is not injective, then $\text{Res}(g, h) = 0$. Reciprocally, if g and h are relatively prime, a solution of the equation $gu + hv = 0$ is an element of the kernel have to satisfy $g|v$ and $h|u$, if (u, v) are not nil, then we must have $\deg u \geq \deg h$, and $\deg v \geq \deg g$ but this is impossible when $\deg g = n$ and $\deg h = m$. Thus we show that $\theta_{g,h}$ is injective and in the finite dimensional case bijective, we have also that $\text{Res}(g, h) = 0$. $\square$

Definition 2.11. If $f = \sum_{i=0}^n a_i X^i \in K[X]$, we define the Gauss valuation the valuation associated to the Gauss norm by $v_G(f) = \inf_{0 \leq i \leq n} v(a_i)$.

Theorem 2.12. (strong version of the Hensel's lemma) Let $C > 0$, and let $f, g, h \in \mathcal{O}_K[X]$ satisfying

- (i) $\deg g = n, \deg h = m$, and $\deg(f - gh) \leq n + m - 1$.
- (ii) $v_G(f - gh) \geq C + 2v(\text{Res}(g, h))$.

Then, there exist unique polynomials $\tilde{g}, \tilde{h} \in \mathcal{O}_K[X]$ such that we have:

- (i) $\deg(\tilde{g} - g) \leq n - 1$, and $\deg(\tilde{h} - h) \leq m - 1$.
- (ii) $v_G(\tilde{g} - g) \geq C + v(\text{Res}(g, h))$, and $v_G(\tilde{h} - h) \geq C + v(\text{Res}(g, h))$.
- (iii) $f = \tilde{g}\tilde{h}$.

Proof. We can assume that g, h is relatively prime. Our goal is to search $u \in K[X]_{\leq m-1}$, and $v \in K[X]_{\leq n-1}$ which correspond respectively to $\tilde{g} - g$ and $\tilde{h} - h$, that satisfy

$$f = (g + v)(h + u) \Leftrightarrow f - gh - uv = gu + hv \Leftrightarrow (u, v) = \theta_{g,h}^{-1}(f - gh - uv).$$

Let $\varphi(u, v) := \theta_{g,h}^{-1}(f - gh - uv)$, then we want to find the fixed point of φ .

Let $B := \{(u, v) \in K[X]_{\leq m-1} \oplus K[X]_{\leq n-1}, \inf(v_G(u), v_G(v)) \geq C + v(\text{Res}(g, h))\}$ Then the theorem 2.12 is a immediate corollary of the following lemma and the completeness of K .

Lemma 2.13. φ is a contraction mapping from B to itself.

Proof. Let $(u, v) \in B$, then

$$\begin{aligned} v_G(f - gh - uv) &\geq \inf(v_G(f - gh), v_G(uv)) \\ &\geq \inf(C + 2v(\text{Res}(g, h)), 2C + 2v(\text{Res}(g, h))) = C + 2v(\text{Res}(g, h)). \end{aligned}$$

We then try to calculate $v(\theta_{g,h}^{-1}(f - gh - uv))$. Since, g and h have coefficients in $\mathcal{O}_K$, $\theta_{g,h}$ have all its coefficients in $\mathcal{O}_K$ and the matrix $\theta_{g,h}^{-1}$ hence have coefficients in $\frac{1}{\text{Res}(g, h)} \mathcal{O}_K$ and hence for all $x \in K[X]_{\leq m+n-1}$ we have $v_G(\theta_{g,h}^{-1}(x)) \geq v_G(x) - v(\text{Res}(g, h))$. Combine the two calculation we have that φ send B to B .

Finally, if (u, v) and (u', v') are two element from B ,

$$\begin{aligned} v_G(\varphi(u, v) - \varphi(u', v')) &= v_G(\theta_{g,h}^{-1}(uv - u'v')) \\ &\geq v_G(u(v - v') + v'(u - u')) - v(\text{Res}(g, h)) \\ &\geq \inf(v_G(u) + v_G(v - v'), v_G(v') + v_G(u - u')) - v(\text{Res}(g, h)) \\ &\geq C + \inf(v_G(u - u'), v_G(v - v')). \end{aligned}$$

Which prove that φ is a contraction mapping. $\square$

□

Corollary 2.14. *Let $f, g, h \in \mathcal{O}_K[X]$ that satisfy the following conditions : g is monic of degree n , $\deg h \leq m$, and $\deg(f - gh) \leq n + m - 1$. The reductions $\bar{g}$ and $\bar{h}$ of g and h modulo $\mathfrak{m}_K$ are relatively prime, and $v_G(f - gh) > 0$. Then there exist unique $\tilde{g}, \tilde{h} \in \mathcal{O}_K[X]$ that satisfy $\deg(\tilde{g} - g) \leq n - 1$, $\deg(\tilde{h} - h) \leq m - 1$, $v_G(\tilde{g} - g) > 0$, $v_G(\tilde{h} - h) > 0$ and $f = \tilde{g}\tilde{h}$.*

Proof. Since $\bar{g}$ is of degree n and $\bar{g}$ and $\bar{h}$ are relatively prime, we have $\text{Res}(\bar{g}, \bar{h}) \neq 0$, this implies $v(\text{Res}(g, h)) = 0$. We are thus in the case of the previous theorem for no matter which $C \in \mathbb{R}$ that verifies $v_G(f - gh) \geq C > 0$, then it suffice to let C tend to 0 to deduce the corollary. □

One particular interesting case is the case where g is of degree 1 : we get the following result that allows us to localise a zero of a polynomial knowing a point where the polynomial is "small". This is an analogy of the *Newton's method*.

Proposition 2.15. (Hensel's lemma) *Let $f \in \mathcal{O}_K[X]$ and $\alpha \in \mathcal{O}_K$ satisfy $v(f(\alpha)) > 2v(f'(\alpha))$, then there exists a unique $\tilde{\alpha} \in \mathcal{O}_K$ satisfies $v(\tilde{\alpha} - \alpha) > v(f'(\alpha))$ and $f(\tilde{\alpha}) = 0$.*

Proof. Let d be the degree of f and $C \in (0, v(f(\alpha)) - 2v(f'(\alpha))]$, the interval is not null by hypothesis. Let $g, h \in \mathcal{O}_K[X]$ given by the formulas $g(X) = X - \alpha$

$$h(X) = \frac{f(X) - f(\alpha)}{X - \alpha} = f^{[1]}(\alpha) + f^{[2]}(\alpha)(X - \alpha) + \dots + f^{[d]}(\alpha)(X - \alpha)^{d-1}$$

Where $f^{[i]}$ is the normalised i -th derivative of f (in characteristic 0, we have $f^{[i]} = \frac{1}{i!}f^{(i)}$). The matrix of $\theta_{g,h} : K[X]_{\leq d-2} \oplus K[X]_{\leq 0} \rightarrow K[X]_{\leq d-1}$ in the basis $(1, X - \alpha, \dots, (X - \alpha)^{d-1})$ is

$$\begin{pmatrix} 0 & \dots & \dots & 0 & f^{[1]}(\alpha) \\ 1 & 0 & \dots & 0 & f^{[2]}(\alpha) \\ 0 & 1 & \dots & 0 & f^{[3]}(\alpha) \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & f^{[d]}(\alpha) \end{pmatrix}.$$

The determinant of the matrix is thus $\pm f^{[1]}(\alpha) = f'(\alpha)$. The resultant $\text{Res}_{d-1,1}(g, h)$ has hence the valuation $v(f'(\alpha))$. On the other hand, we know that $v_G(f - gh) = v(f(\alpha)) \geq C + 2v(\text{Res}_{d-1,1}(g, h))$ by our choice of C , and also $\deg(f - gh) \leq d - 1$. We are thus in the right case to apply theorem 2.12 and there exists a unique $\tilde{g}$ that divide f such that $\deg(\tilde{g} - g) = 0$ and $v_G(\tilde{g} - g) \geq C + v(f'(\alpha))$. Hence there exists a unique $\tilde{\alpha} \in \mathcal{O}$ such that we have $g(X) = X - \tilde{\alpha}$ and also $f(\tilde{\alpha}) = 0$, and $v(\tilde{\alpha} - \alpha) \geq C + v(f'(\alpha))$. It then suffice to let C tend to 0 to conclude. □

Remark 2.16. *Another proof of the Hensel's lemma 2.15 can be done using the Newton's method $(x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}, x_0 = \alpha)$.*

Corollary 2.17. (Hensel's lemma, the characterisation of henselian rings) *Let $f \in \mathcal{O}_K[X]$ be a monic polynomial and $\bar{f}$ the reduction of f modulo $\mathfrak{m}_K$. If $\bar{\alpha}$ is a simple root of $\bar{f}$ in k , the residue field, then there exists a unique $\tilde{\alpha} \in \mathcal{O}_K$, whose reduction modulo $\mathfrak{m}_K$ is $\bar{\alpha}$ and verifies $f(\tilde{\alpha}) = 0$.*

Proof. Take $\alpha \in \mathcal{O}_K$ a lifting of $\bar{\alpha}$. The hypothesis that $\bar{\alpha}$ is a simple root of $\bar{f}$ is noting but $v(f(\alpha)) > 0$ and $v(f'(\alpha)) = 0$, this allows us to utilise the proposition 2.15 and we're done. □

Definition 2.18. *A local ring A that satisfies the characterisation 2.17 is called a Henselian ring.*

Our goal introducing the Hensel's lemma here is to prove and apply the following proposition.

Proposition 2.19. *Let $f \in K[X]$ be a monic irreducible polynomial satisfying $f(0) \in \mathcal{O}_K$. Then all its coefficients are in $\mathcal{O}_K$.*

Proof. We proof the proposition by contradiction. Suppose the contrary and let $f \notin \mathcal{O}_K[X]$, and $i := \max_{k=1}^n \{k, v(a_k) = v_G(f)\}$. Then, the polynomial $a_i^{-1}f$ is written in the form of

$$b_n X^n + \cdots + b_{i+1} X^{i+1} + X^i + b_{i-1} X^{i-1} + \cdots + b_0$$

where all the b_k are elements of $\mathcal{O}_K$, and for all $k \in \{i+1, \dots, n\}$, we also have $v(b_k) > 0$. We can thus apply the corollary 2.14 to $g(X) = X^i + \cdots + b_0$ and $h = 1 + b_n X^{n-i}$ to show that there exist polynomials $\tilde{g}$ and $\tilde{h}$ with respectively the degree i and j such that we have $f = a_i \tilde{g} \tilde{h}$. This is in contradiction with the hypothesis that f is irreducible. $\square$

We have now all the ingredients to prove the existence and uniqueness of extensions of a valuation.

Theorem 2.20. *Let K be a complete field for a valuation v , and let L be a finite extension of K . Then there exists a unique way to prolong v to a valuation of L . Moreover, if $s \in L$, then*

$$v(x) = \frac{1}{[L : K]} v(N_{L/K}(x)).$$

Proof. We start by the uniqueness. We can think of L as a finite dimensional vector space over K of dimension $[L : K]$. By proposition 2.6, if v_1 and v_2 are two valuation that prolong v to L , then they define the same topology on L . Then, the proposition 2.5 implies that there exists a $s \in \mathbb{R}_+^\times$ such that $v_2(x) = s v_1(x)$ for all $x \in L$. Since $v_1(x) = v_2(x)$ for $x \in K$, $s = 1$. We have thus the uniqueness of extension.

We now pass to existence, we only have to show that our formula gives a well-defined extension of valuation. The multiplicativity and the restriction part are automatically satisfied, what we need to prove is just $(v(N_{L/K}(x)) \geq 0) \Rightarrow (v(N_{L/K}(1+x)) \geq 0)$.

Let $f(X) = X^d + \cdots + a_0$ be the minimal polynomial of x over K , this implies that $d \mid [L : K]$ and $N_{L/K}(x) = ((-1)^d a_0)^{\frac{[L:K]}{d}}$, and hence $v(N_{L/K}(x)) \geq 0$ implies that $a_0 \in \mathcal{O}_K$ and f is irreducible implies that all coefficients of f are in $\mathcal{O}_K$ by the proposition 2.19. On the other hand the minimal polynomial for $1+x$ is $f(X-1)$, and hence $N_{L/K}(1+x) = ((-1)^d f(-1))^{\frac{[L:K]}{d}} \in \mathcal{O}_K$, this is what we want. $\square$

Corollary 2.21. *If $\overline{K}$ is one algebraic closure of K , there exists one unique way to prolong v to $\overline{K}$. Moreover, $\text{Aut}(\overline{K}/K)$ act on $\overline{K}$ by isometries.*

The uniqueness is a direct consequence of the preceding theorem. The rest come from that if $x \in \overline{K}$, and if $\sigma \in \text{Aut}(\overline{K}/K)$, then $N_{K(x)/K}(x) = N_{K(\sigma(x))/K}(\sigma(x))$.

Corollary 2.22. *If $P \in K[X]$ is irreducible, then all its roots in $\overline{K}$ have the same valuation.*

Proof. The roots of a irreducible polynomial is permuted transitively by $\text{Aut}(\overline{K}/K)$, and the preceding corollary let us to conclude. $\square$

We are now in the case that we know there exists a unique way to prolong a valuation to the algebraic closure of a complete valuated field. But this algebraic closure have no reason to be complete (and it is not complete in the general cases), hence we can do a completion and then take the algebraic closure and redo a completion. . . The next theorem will show that this procedure converges very fast.

Theorem 2.23. *Let K be a algebraically closed field equipped with a valuation, its completion $\widehat{K}$ is algebraically closed.*

The standard proof in the adic world is using the Krasner's lemma. However, we'll give an alternative proof that work in both archimedian and non-archimedian cases **not** using the Krasner's lemma.

Lemma 2.24. (Krasner's lemma) *Let $\alpha \in \overline{K}$, where K is a ultrametric field. We impose*

$$d_\alpha := \min\{|\alpha - \alpha'|, \alpha' \neq \alpha \text{ is a conjugation of } \alpha\}.$$

If $\beta \in \overline{K}$ such that $|\beta - \alpha| < d_\alpha$, then $K[\alpha] \subset K[\beta]$.

Proof. (proof of the theorem in both archimedean and ultrametric cases) Let $P(X) = X^d + \dots + a_0 \in \widehat{K}[X]$, it suffice to find one root in $\widehat{K}$. By construction, $P(X) = \lim_{n \rightarrow \infty} P_n(X)$, where $P_n(X) = X^d + a_{d-1,n}X^{d-1} + \dots + a_{0,n}$, with $a_{i,n} \rightarrow a_i$, when $n \rightarrow \infty$.

Then K is algebraically closed implies that P_n admit d roots $z_{1,n}, \dots, z_{d,n}$ in K . Moreover, the set $\{z_{i,n}, 1 \leq i \leq d, n \in \mathbb{N}\}$ is uniformly bounded since the coefficients $\{a_{i,n}\}$ are bounded and $P_n(z_{i,n}) = 0$.

We have then $P_n(z_{i,m}) = P_n(z_{i,m}) - P_m(z_{i,m}) \rightarrow 0$ as $n, m \rightarrow \infty$, because all the coefficient of $P_n - P_m \rightarrow 0$ when $n, m \rightarrow \infty$.

Now, write $P_n(z_{i,m}) = \prod_{j=i}^n (z_{i,m} - z_{j,n})$, then $d(z_{i,m}, \{z_{1,n}, \dots, z_{d,n}\}) \rightarrow 0$ when $n, m \rightarrow \infty$. Thus, we can extract a sub-Cauchy sequence $\{z_{i_j, n_j}\}$ that converge to $z \in \widehat{K}$ when $n_j \rightarrow \infty$. This is the root that we want to find. $\square$

Here we prove some useful lemmata on the residue field before focusing on $\mathbb{C}_p$.

Lemma 2.25. *Let K be a complete ultrametric field and L a finite extension of K , then k_L the residue field of L is a algebraic extension of k_K of degree less or equal to $[K : L]$.*

Proof. We have $\mathcal{O}_K \cap \mathfrak{m}_L = \mathfrak{m}_K$ and hence k_K inject in k_L . Let $\overline{\alpha}_1, \dots, \overline{\alpha}_d$ elements of k_L that consist a free family over k_K . Choose for each $i \in \{1, \dots, d\}$ a lifting α_i . Suppose that the family is dependent over K hence we find $(\lambda_1, \dots, \lambda_d)$ not all nil in K such that $\lambda_1 \alpha_1 + \dots + \lambda_d \alpha_d = 0$. We then divide the λ_i by the one with the biggest norm, and hence everyone have norm less or equal than 1, id est valuation greater or equal to 1, thus in $\mathcal{O}_K$. We can hence suppose that they are all in $\mathcal{O}_K$ and one of them is 1, but this gives us a contradiction after the reduction modulo $\mathfrak{m}_L$, this allows us to conclude. $\square$

Lemma 2.26. *Let K be a ultrametric algebraically closed field, then k_K is algebraically closed.*

Proof. Let $\overline{P}(X) \in k_K[X]$ monic of degree $n \geq 1$ and $P(X) \in \mathcal{O}_K[X]$ monic of degree n a lifting of $\overline{P}$. Let $\alpha \in K$ a root of P . We have $\alpha \in \mathcal{O}_K$ and $\overline{\alpha}$ is a root of $\overline{P}$, by definition of ideals. $\square$

Lemma 2.27. *If K is a ultrametric field and $\widehat{K}$ its completion, then $k_K = k_{\widehat{K}}$.*

Proof. $\mathcal{O}_K \cap \mathfrak{m}_{\widehat{K}} = \{x \in \mathcal{O}_K, v(x) > 0\} = \mathfrak{m}_K$, and hence the natural mapping from k_K to $k_{\widehat{K}}$ is injective. On the other hand, since $\mathcal{O}_K$ is dense in $\mathcal{O}_{\widehat{K}}$, this mapping is surjective, and we're done. $\square$

Corollary 2.28. *Let K be a complete valued field, then the residue field $\widehat{\widehat{K}}$ is a algebraic closure of k_K .*

Let $\overline{\mathbb{Q}_p}$ be a algebraic closure of $\mathbb{Q}_p$. We've shown that v_p is prolonged by a unique medium to a valuation on $\overline{\mathbb{Q}_p}$.

Definition 2.29. *One denote $\mathbb{C}_p$ the completion of $\overline{\mathbb{Q}_p}$ for the valuation v_p .*

We here gives some interesting remark on the analytic or the point-set topology side, that will not be used in the Dwork's proof.

Remark 2.30. *One can use ultrafilter to construct a universal field Ω_p (bounded sequence with coefficient in $\overline{\mathbb{Q}_p}$ quotient by the ideal of sequences that the limit along the ultrafilter is zero), the Dwork's proof work for both Ω_p and $\mathbb{C}_p$, we just need a algebraically closed complete ultrametric field.*

- (i) *By arguments of cardinality and the axiom of choice $\mathbb{C}_p \simeq \mathbb{C}$. The isomorphism is non canonical.*
- (ii) *$\mathbb{C}_p$ is not spherically complete.*
- (iii) *Ω_p is spherically complete.*
- (iv) *The residue field of $\mathbb{C}_p$ is $\overline{\mathbb{F}_p}$, we've proved above, for Ω_p it is uncountable, noted k_{Ω} .*
- (v) *The image under the norm of non zero values of the field (a totally ordered abelian group) $\mathbb{C}_p$ is $p^{\mathbb{Q}}$, for Ω_p , it is $\mathbb{R}_{>0}$.*

We will now consider only $\mathbb{C}_p$, always keep in mind that most of the properties also work for Ω_p .

We now pass to the discussion of Teichmüller representative, and the Witt vectors.

Proposition 2.31. *Let $x \in \overline{\mathbb{F}_p}^\times$, then there exists a root of the unit $[x]$ of order prime to p in $\mathcal{O}_{\mathbb{C}_p}$, whose reduction in $\overline{\mathbb{F}_p}$ is x .*

Proof. By definition, there exists a n such that $x \in \mathbb{F}_{p^n}$, a finite field whose non zero elements are exactly the roots of polynomial $f = X^{p^n-1} - 1$. Its determinant is $\prod_{\zeta^{p^n-1}=1} f'(\zeta) = \pm(p^n - 1)^{p^n-1}$. We have hence the roots of f after the reduction modulo $\mathfrak{m}_{\mathbb{C}_p}$ is distinct. We have thus an injection between roots in $\mathbb{C}_p$ and roots modulo $\mathfrak{m}_{\mathbb{C}_p}$, hence a bijection. $\square$

Definition 2.32. *We pose $[0] = 0$. We call $[x]$ the Teichmüller representative of $\overline{\mathbb{F}_p}$ in $\mathcal{O}_{\mathbb{C}_p}$.*

Remark 2.33. *By the uniqueness of $[x]$, we have $[xy] = [x][y]$. The Teichmüller representative is multiplicative.*

Remark 2.34. *One can express the p -adic integers as series with coefficient the Teichmüller representative.*

Definition 2.35. *Let R be a commutative ring. The ring of Witt vectors $W(R) = \prod_{i=1}^\infty R$ is the unique ring whose ghost components $W_n = \sum_{i=1}^n p^i X_i^{p^{n-i}}$ define a homomorphism of ring $W(R) \rightarrow \prod_{i=1}^n R$.*

The notion of Witt vectors are very useful, the functor $W(\cdot)$ from the category of $\mathbb{F}_p$ -perfect algebras to the category of p -adic complete rings is the left adjoint of the tilt $(\cdot)^\flat$, which allows us to obtain the notion of untilt.

We shall now state and prove the Weierstrass division and preparation theorem in our case of one variables for simplification, but this result also hold and is useful for Tate algebras of multiple variables for rigid geometry.

Definition 2.36. *We define a Tate algebra with d variables with coefficient in K as follows.*

$$K\{X_1, \dots, X_n\} = T_d := \{f(X) = \sum_{i \in \mathbb{Z}_{\geq 0}^d} a_i X^i \in K[[X_1, \dots, X_d]] : a_i \rightarrow 0 \text{ when } i \rightarrow \infty\}.$$

In our case, we consider $d = 1$ $K = \mathbb{C}_p$ (or Ω_p). This is also the ring of sequences that converge on the ball $\{v_p(x) \geq 0\}$. This is also the completion of $K[X]$ for the Gauss valuation. We will note $v^{[0]}$ in place of v_G .

Theorem 2.37. (Weierstrass division theorem) *Let $P \in \mathcal{O}_K[X]$ be a monic polynomial, then all element $f \in T_1$ can be written in a unique way under the form of $f = Pq(f) + r(f)$, where $q(f) \in T_1$ and $r(f) \in T_1$ is of degree $\leq \deg P - 1$. Moreover, $v^{[0]}(q(f)) \geq v^{[0]}(f)$, and $v^{[0]}(r(f)) \geq v^{[0]}(f)$. (We call the polynomial $r(f)$ the reminder of the euclidean division of f by P , $q(f)$ the quotient of the euclidean division of f by P .)*

Proof. Uniqueness: It suffice to verify the application $(g, R) \rightarrow Pg + R$ is injective. Hence, let $Pg = -R$ then we want to have $g = R = 0$. Let P be monic with integer coefficients, for a root x , we prove by contradiction that $v_p(x) \geq 0$. Suppose the contrary, we have $v_p(x^n + \dots + a_0) = +\infty$, but we suppose that $v_p(x) \geq 0$, we know by definition that $v_p(x^n + \dots + a_0) = nv_p(x)$, thus a contradiction. But R have at most $\deg P - 1$ roots if R is not zero, hence R is zero.

Existence: Let P be monic with coefficients in $\mathcal{O}_K$, $Q = Pq(Q) + r(Q)$ for $Q \in \mathcal{O}_L[X]$ is the usual euclidean division, we have $r(Q), q(Q) \in \mathcal{O}_K[X]$. We obtain hence applications from $K[X]$ to $K[X]$ that satisfy $v^{[0]}(r(Q)) \geq v^{[0]}(Q)$, and $v^{[0]}(q(Q)) \geq v^{[0]}(Q)$. This application extends by continuity to T_1 and satisfies the same properties. $\square$

Theorem 2.38. (Weierstrass preparation theorem)(i) $g = \sum_{k \in \mathbb{N}} b_k X^k \in T_1$ is invertible in T_1 if and only if $b_0 \neq 0$ and $v_p(b_k) > v_p(b_0)$ if $k \geq 1$.

(ii) If $f = \sum_{k \in \mathbb{N}} a_k T^k \in T_1$ is non zero, then f can be written in a unique way in the forme of $f = Pg$, where $P \in \mathcal{O}_K[X]$ is a monic polynomial, and $g = \sum_{k \in \mathbb{N}} b_k X^k \in T_1$ is a unit of T_1 .

Proof. (i) Let $g \in T_1$ be invertible. After divided by a element of $K^\times$, we can suppose that $v^{[0]}(g) = 0$, hence we have $v^{[0]}(g^{-1}) = 0$. Therefore $gg^{-1} = 1 \pmod{\mathfrak{m}_K}$, which implies $\overline{gg}^{-1} = 1$ in $\kappa_K[X]$, where κ_K is the residue field. We obtain thus that $\overline{g}$ is a non zero constant. Hence we have one direction. Reciprocally, if $b_0 \neq 0$, and $v_p(b_k) > v_p(b_0)$, then $v^{[0]}(b_0^{-1}g - 1) > 0$, this implies that $b_0^{-1}g$ is invertible hence the same for g .

(ii) the series $v_p(a_k)$ tend to $+\infty$, there exists $d \in \mathbb{N}$ such that we have $v_p(a_d) \leq v_p(a_k)$ (respectively $v_p(a_d) < v_p(a_k)$) if $k \in \mathbb{N}$ (respectively for $k > d$). Let $\alpha_0 = a_d$ and $P_0 = \sum_{k=0}^d \frac{a_k}{a_d} X^k$. We will prove that we can find $R \in \mathfrak{m}_K[X]$, of degree $\leq d-1$, and $u \in \mathfrak{m}_K\{X\}$, such that we have $\alpha_0 f = (P_0 + R)(1 + u)$, which can be written in the form $\alpha_0^{-1}f = (P_0 + R)(1 + u)$.

To find these elements, we consider the application $\theta : (u, R) \mapsto \theta(u, R)$, the quotient and the reminder of $\alpha_0^{-1}f - P_0 - Ru$ divided by P_0 . Since $\alpha_0^{-1}f - P_0 \in \mathfrak{m}_K$ by construction, we obtain that $\theta : \mathfrak{m}_K\{X\} \oplus \mathfrak{m}_K[X]_{d-1} \rightarrow \mathfrak{m}_K\{X\} \oplus \mathfrak{m}_K[X]_{d-1}$ by the Weierstrass division theorem.

On the other hand, the same theorem tells us that:

$$\begin{aligned} v^{[0]}(\theta(u, R) - \theta(u', R')) &= v^{[0]}(uR - u'R') \geq \inf(v^{[0]}(u) + v^{[0]}(R - R'), v^{[0]}(R') + v^{[0]}(u - u')) \\ &\geq \inf(v^{[0]}(u - u'), v^{[0]}(R - R')) + \inf(v^{[0]}(u), v^{[0]}(R')). \end{aligned}$$

This allows us to show that θ is a contraction mapping of $\mathfrak{m}_K\{X\} \oplus \mathfrak{m}_K[X]_{d-1}$, its unique fixed point is what we want to find.

Now if $u_0 = \sum_{k \in \mathbb{N}} c_k x^k$, it suffice to take $P = P_0 + R_0$ and $g = \alpha f_0(1 + u_0)$

Uniqueness: If $Pg = P'g'$, with g, g' invertible in T_1 , $\frac{P}{P'}$ have no poles and no zeros in the ball $v_p(x) \geq 0$. P, P' are monic polynomials, all of there zeros are in this ball, therefore $P = P'$ and hence also $g = g'$. $\square$

Remark 2.39. *The Weierstrass division theorem is eventually equivalent to the Weierstrass preparation theorem.*

Remark 2.40. *We can apply the Weierstrass preparation theorem to prove the following properties of Tate algebras.*

- (i) T_n is noetherian.
- (ii) T_n is factorial and hence normal.
- (iii) (Noether normalisation lemma) *If $\mathfrak{a}$ is an ideal of T_n and B its quotient. Then there exist a integer d and a finite injective homomorphism $T_d \rightarrow B$.*
- (iv) *Let $\mathbb{B}^n(\overline{K})$ denote the ball $\{(x_1, \dots, x_n) : |x_i| \leq 1\}$, then there is a natural bijection.*

$$\mathbb{B}^n(\overline{K})/\text{Gal}(\overline{K}/K) \xrightarrow{\sim} \text{Sp}(T_n)$$

Here, Sp denotes the maximal spectrum.

- (v) T_n is a Jacobson ring.

2.2. Reduction of the problem. The proof of Dwork relies on explicit calculations on the ζ function of a hypersurface defined on the torus $\mathbb{T}^n = (\mathbb{G}_m)^n$, we will do some combinatorial work to reduce from algebraic varieties defined by a finite covering of affine varieties whose intersection is affine, exempli grata projective varieties to such cases.

We're back in the case of introduction that K is a finite field.

By the multiplicativity of exponential function and the inclusion-exclusion principle, we have the following remark.

Remark 2.41. *If V', V'' are subvarieties of V , such that $V' \cup V'' = V$ and $V' \cap V'' = W$, we have*

$$Z_V = Z_{V'} Z_{V''} Z_W^{-1}.$$

Since $V_{(f,g)} = V_f \cup V_g$ and $V_{fg} = V_f \cap V_g$, doing a induction we reduce the problem to varieties defined by one equation.

$$\begin{aligned} \mathbb{P}_K^n &= \mathbb{A}_K^n \sqcup \mathbb{A}_K^{n-1} \sqcup \dots \sqcup \mathbb{A}_K^1 \sqcup \{*\} \\ \mathbb{A}_K^n &= \{0\} \times \mathbb{A}_K^{n-1} \sqcup \mathbb{G}_m \times \mathbb{A}_K^{n-1} \end{aligned}$$

After a induction we see that it suffice to consider hypersurfaces defined on the torus. To conclude, we reduce ourselves to prove the following theorem.

Theorem 2.42. (Dwork 1960) (rationality of ζ function, the first Weil conjecture) *Let X be a hypersurface on the torus $\mathbb{T}^n = (\mathbb{G}_m)^n$, its zeta function $Z(X, T)$ is rational.*

Remark 2.43. *In the theory of étale cohomology, a similar reduction is often utilised to reduce the calculation to the case of a curve.*

2.3. Criteria of rationality. In this subsection, we will cite and prove several criteria of rationality essentially due to Borel, Dwork and Dieudonné, that we will apply to the zeta function $Z(X, T)$. Here the fields are arbitrary commutative fields.

Proposition 2.44. *Let $F = \sum_{k \in \mathbb{N}} a_k X^k \in K[[X]]$ is rational if and only if there exist two integers t and n_0 and $t + 1$ elements of K denoted $q_0, q_1, \dots, q_t$, with $q_0 \neq 0$, such that for all $n \geq n_0$ the coefficients a_n satisfy the relation.*

$$q_0 a_n + q_1 a_{n-1} + \dots + q_t a_{n-t} = 0.$$

Proof. If F is rational, let us write $F = \frac{P}{Q}$, with $Q = \sum_{i=0}^t q_i X^i$, $P \in K[X]$, $Q \in K[X]$, $\deg P = r$ we have the relation we want by equality of coefficient for $QF = P$ with $n \geq n_0 := \sup(r + 1, t)$.

Reciprocally, if we set $Q = \sum_{i=0}^t q_i X^i$, then the relation gives us $QF = P$ with $\deg P \leq n_0 - 1$, thus F is a rational series. $\square$

Theorem 2.45. (Borel, Hadamard criteria) *$F = \sum_{k \in \mathbb{N}} a_k X^k \in K[[X]]$ is rational if and only if there exist two integers $m, S \geq 0$, such that for $s \geq S$*

$$N_{s,m} := \det A_{s,m} = \det \begin{pmatrix} a_s & \dots & a_{s+m} \\ \vdots & \ddots & \vdots \\ a_{s+m} & \dots & a_{s+2m} \end{pmatrix} = 0.$$

Proof. If F is rational, let us write $F = \frac{P}{Q}$, with $Q = \sum_{i=0}^t q_i X^i$, $P \in K[X]$, $Q \in K[X]$, $\deg P = r$ we have the relations by equality of coefficient for $QF = P$ with $n \geq n_0 := \sup(r + 1, t)$.

$$q_0 a_n + q_1 a_{n-1} + \dots + q_t a_{n-t} = 0$$

Now, let $S = \max(r - s + 1, 1)$, and let $m = r$, if $s \geq S$, then we have the relations for $i = s + r, \dots, s + 2r$:

$$\begin{aligned} q_0 a_{s+t} + q_1 a_{s+t-1} + \dots + q_t a_s &= 0 \\ q_0 a_{s+t+1} + q_1 a_{s+t} + \dots + q_t a_{s+1} &= 0 \\ &\vdots \\ q_0 a_{s+2t} + q_1 a_{s+2t-1} + \dots + q_t a_{s+t} &= 0 \end{aligned}$$

We get a linear relation on columns which implies $N_{s,t} = 0$. We set $m = r$ and we have $N_{s,m} = N_{s,t} = 0$ for $s \geq S$.

Conversely, we suppose that $N_{s,m} = 0$ for $s \geq S$, we choose m such that it is the smallest m to satisfy $N_{s,m} = 0$ for all $s \geq S$. We claim that $N_{s,m-1} \neq 0$ for all $s \geq S$.

Suppose the contrary. Then some linear combination of the first m rows $r_0, r_1, \dots, r_{m-1}$ of $A_{s,m}$ vanish in all but perhaps the last column. Let r_{i_0} be the first row having non zero coefficient in this linear combination, id est the i_0 th row r_{i_0} can be expressed as $\alpha_1 r_{i_0+1}, \alpha_2 r_{i_0+2} + \dots + \alpha_{m-1} r_{i_0+m-1}$. We do an elementary row operation replacing r_{i_0} by $r_{i_0} - (\alpha_1 r_{i_0+1}, \alpha_2 r_{i_0+2} + \dots + \alpha_{m-1} r_{i_0+m-1})$, we consider the following two cases:

(1) $i_0 > 0$, the matrix is of the form:

$$\begin{pmatrix} a_s & \cdots & a_{s+m-1} & a_{s+m} \\ a_{s+1} & \cdots & a_{s+m} & a_{s+m+1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \beta \\ \vdots & \ddots & \vdots & \vdots \\ a_{s+m} & \cdots & a_{s+2m-1} & a_{s+2m} \end{pmatrix}$$

and when we erase the first line and last column, we know that $N_{s+1,m-1} = 0$.

(2) $i_0 = 0$. Then we have:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & \beta \\ a_{s+1} & a_{s+2} & \cdots & a_{s+m} & a_{s+m+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m-1} & a_{s+2m} \end{pmatrix}$$

We have two copies of $A_{s+1,m-1}$ in $A_{s,m}$, the one erasing the first row and last column is kept unchanged, the other one is the one erasing the last row and the first column, let note this matrix $B_{s+1,m-1}$. These two copies all have determinant $N_{s+1,m-1}$ because we've only done a elementary row operation. The development of the first row says that we have $(N_{s+1,m-1} = 0) \vee (\beta = 0)$, but if β is nil we also have the first line of $B_{s+1,m-1}$ is zero and hence $N_{s+1,m-1} = 0$.

Thus, we've proven that for $s \geq S$, we have $N_{s,m} = 0$ and $N_{s+1,m-1} \neq 0$. Hence there is a linear combination of the rows of $A_{s,m}$ that vanishes, for which the coefficient of the last row is non zero. Hence, the last row of $A_{s,m}$ for any $s \geq S$ is a linear combination of the preceding m rows. Hence any simultaneous solution to

$$\begin{aligned} a_S u_m + a_{S+1} u_{m-1} + \cdots + a_{S+m} u_0 &= 0 \\ &\vdots \\ a_{S+m-1} u_m + a_{S+m} u_{m-1} + \cdots + a_{S+2m-1} u_0 &= 0 \end{aligned}$$

is also a solution to

$$a_{S+m} u_m + a_{S+m+1} u_{m-1} + \cdots + a_{S+2m} u_0 = 0$$

By induction, to every

$$a_s u_m + a_{s+1} u_{m-1} + \cdots + a_{s+m} u_0 = 0$$

for $s \geq S$. Thus, we apply the preceding proposition and we're done. $\square$

In our discussion of convergent series, we can always reduce to the case of Weierstrass preparation theorem by multiplying a unit. Note that $p^{\mathbb{Q}}$ is dense in $\mathbb{R}$, hence each time we do such a reduction, we potentially reduce the radius of convergent by a $\varepsilon > 0$ arbitrary small.

Theorem 2.46. (Borel criteria) *Let $F = \sum_{k \in \mathbb{N}} a_k T^k$ have integer coefficients, and p a prime number. Suppose that there exist two positive number r and R , such that, F is meromorphic for $|z| < R$ as a complex function, and F is meromorphic for $|z|_p < r$ as a p -adic function, with $rR > 1$, then F is rational.*

Proof. Suppose that F is meromorphic, namely $F(T) = \frac{A(T)}{B(T)}$ with A, B convergent on the disc $D(0, r)$. Since $p^{\mathbb{Q}}$ is dense in $\mathbb{R}_+$, we may assume that $r = p^\alpha$ for some $\alpha \in \mathbb{Q}$, and that F is bounded on the p -adic sphere of radius r . then we can apply the Weierstrass preparation theorem to B , and we obtain $B = P \frac{1}{G}$, with $P = \sum_{i=1}^d q_i T^i$, where G also converges on the disc $D(0, r)$.

We set $H = AG$, which is also convergent on $D(0, r)$, write $H(T) = \sum_{k \in \mathbb{N}} b_k T^k$, then by consruc-tion, we have $H = PF$, $|a_k|_\infty < R^{-k}$, $|b_k| < r^{-k}$, and also the relation

$$b_n = a_n + q_1 a_{n-1} + \cdots + q_d a_{n-d}$$

Now let's calculate $|N_{s,m}|_\infty$ and $|N_{s,m}|_p$. We take a big m , id est $m > 2d$. Then the above relations give us that

$$N_{s,m} = \det \begin{pmatrix} a_s & \cdots & a_{s+m} \\ \vdots & \ddots & \vdots \\ a_{s+m} & \cdots & a_{s+2m} \end{pmatrix} = \det \begin{pmatrix} a_s & \cdots & a_{s+d} & b_{s+d+1} & \cdots & b_{s+m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{s+m} & \cdots & a_{s+m+d} & b_{s+m+d+1} & \cdots & b_{s+2m} \end{pmatrix}$$

From the first matrix, we get $|N_{s,m}|_\infty \leq (m+1)!R^{-\frac{1}{2}(2s+m)(m+1)}$, and from the second matrix that $|N_{s,m}|_p \leq \max(\prod |b_j|_p) \leq r^{-\frac{1}{2}(m-d)(s+2m-d-1)}$, for $a_i \in \mathbb{Z}$, hence $|a_i|_p \leq 1$. These bounds are far from optimal, but give us nonetheless that $|N_{s,m}|_\infty |N_{s,m}|_p \leq C(rR)^{-\frac{1}{2}(s+m)(m+1)}$. Now when we tend $s \rightarrow \infty$, we get $|N_{s,m}|_\infty |N_{s,m}|_p < 1$. But $N_{s,m} \in \mathbb{Z}$, hence $|N_{s,m}|_\infty |N_{s,m}|_p \in \mathbb{Z}_{\geq 0}$, we have then the existence of a S , such that $N_{s,m} = 0$, for $s \geq S$. $\square$

We now try to apply the criteria 2.46 to $Z(X, T)$, we're back to the case in which K denote a finite field. We already know that $Z(X, T)$ have coefficient in $\mathbb{Z}$ (see remark 1.12), we first find a radius of convergence as complex function.

Proposition 2.47. *For a affine variety X , $Z(X, T)$ is convergent on the disc $D(0, q^{-n})$ as complex function.*

Proof. Because $|\mathbb{A}_K^n| = q^n$, the number of K points are smaller than the number of the affine space. So the coefficients of $Z(X, T)$ are smaller than the coefficients of $Z(\mathbb{A}_K^n, T)$.

$$Z(\mathbb{A}_K^n, T) = \exp\left(\sum_{s=1}^{\infty} q^{ns} \frac{T^s}{s}\right) = \exp(-\log(1 - q^n T)) = \frac{1}{1 - q^n T} = \sum_{s=1}^{\infty} q^{ns} T^s.$$

$\square$

Hence we have reduced the problem to the search of a r , such that $rq^{-n} > 1$. In fact, the case if even better, Dwork proved that $Z(X, T)$ is meromorphic on the whole p -adic plane $\mathbb{C}_p$.

Theorem 2.48. (Dwork 1960) (rationality of ζ function, the first Weil conjecture) *For X a hypersurface on the torus $\mathbb{T}^n = (\mathbb{G}_m)^n$, the zeta function $Z(X, T)$ is meromorphic on $\mathbb{C}_p$.*

2.4. Θ function. Now we dive in to the analytic world. We construct a factorisation of the additive character which resemble the θ function in analytic number theories. The following theorem is our goal in this subsection.

Theorem 2.49. (Factorisation of a non trivial additive character) *Let $s \geq 1$ be an integer, we consider the field extension $\mathbb{F}_p \subset \mathbb{F}_{p^s}$. Let $\varepsilon \in \mathbb{C}_p$ be a p -th primitive root of the unit, $\varepsilon = 1 + \lambda$, then the additive character $t \mapsto \varepsilon^{\text{Tr}(t)}$ is non trivial. Moreover, for $[t]$ the Teichmüller representative of t , we have*

$$\varepsilon^{\text{Tr}(t)} = \Theta([t])\Theta([t]^p) \cdots \Theta([t]^{p^{s-1}})$$

Where $\Theta(t) = \sum_k \beta_k t^k$ is a power series in $\mathbb{C}_p$ such that $v_p(\beta_k) \geq \frac{k}{p-1}$. The definition of Θ is independent of s .

In fact, the coefficients of Θ is in the ring $\mathbb{Z}_p[\varepsilon] = \mathbb{Z}_p[\lambda]$.

We now need to define the Θ function above and then prove the theorem.

We start by considering the formal series $H(t, Y) = (1 + Y)^t = \sum_{k=0}^{\infty} \binom{t}{k} Y^k \in \mathbb{Q}[[t, Y]]$, where $\binom{t}{k} = \frac{t(t-1)\cdots(t-k-1)}{k!}$. The coefficients of this series is rational numbers, if $t \in \mathbb{Z}_p$, then we have $\binom{t}{k} \in \mathbb{Z}_p$. The series $(1 + Y)^t$ converges for $v_p(Y) > 0$, because in this case it is in the conventional case the t -th power of $(1 + Y)$.

Definition 2.50. We define $F(t, Y)$, $\alpha_i(Y)$ and $B_j(t)$ as follow.

$$\begin{aligned}
F(t, Y) &:= \prod_{k=0}^{\infty} H\left(\frac{t^{p^k} - t^{p^{k-1}}}{p^k}, Y^{p^k}\right) = H(t, Y)H\left(\frac{t^p - t}{p}, Y^p\right)H\left(\frac{t^{p^2} - t^p}{p^2}, Y^{p^2}\right) \dots \\
&= (1 + Y)^t (1 + Y^p)^{\frac{t^p - t}{p}} (1 + Y^{p^2})^{\frac{t^{p^2} - t^p}{p^2}} \dots \\
&= \sum_{k=0}^{\infty} B_k(t) Y^k \\
&= \sum_{k=0}^{\infty} t^k \alpha_k(Y).
\end{aligned}$$

Remark 2.51. We see by definition that $B_k(t)$ is a polynomial of degree $\leq k$, hence $\alpha_k(Y) \in \mathbb{Z}_p[[Y]]$ is a formal series that start with the terms of degree $\geq k$.

Here's a criteria by Dwork that shows the coefficients of F are in $\mathbb{Z}_p$.

Lemma 2.52. (Dwork, Dieudonné criteria) An element $F(X) = \sum_{i \in \mathbb{N}} a_i X^i \in 1 + X\mathbb{Q}_p[[X]]$ lies in $1 + X\mathbb{Z}_p[[X]]$ if and only if $\frac{F(x)^P}{F(x^p)}$ lies in $1 + pX\mathbb{Z}_p[[X]]$.

Proof. If $F \in 1 + X\mathbb{Z}_p[[X]]$, then $F(X)^p \equiv F(X^p) \pmod{p}$. Both series belong to $1 + X\mathbb{Z}_p[[X]]$, and $F(X^p) \in 1 + X\mathbb{Z}_p[[X]]$ is invertible, so that we have $\frac{F(X)^p}{F(X^p)}$ lies in $1 + pX\mathbb{Z}_p[[X]]$.

Conversely, assume that

$$F(X)^p = F(X^p)(1 + p \sum_{j \geq 1} b_j X^j)$$

. We have $a_0 = 1$ and $a_1 = b_1 \in \mathbb{Z}_p$. Let us assume by induction that $a_i \in \mathbb{Z}_p$ for $i < n$ and compare the coefficients of x^n in both sides of the equality.

The coefficient of LHS of X^n is the same to the coefficient of the polynomial

$$\left(\sum_{i \leq n} a_i X^i\right)^p = \sum_{i \leq n} a_i^p X^{ip} + p(\dots).$$

The non written monomials are products $a_{i_1} \dots a_{i_p} X^{i_1 + \dots + i_p}$ which have at least two distinct indices i, j . We want to determine them modulo $\mathbb{Z}_p$, and by the induction assumption the terms not containing a_n have coefficient in $\mathbb{Z}_p$, and with terms containing a_n , all the rest have to be $a_0 = 1$ because if it is not the case then the degree is strictly larger than n . This shows that if $ip = n$, we have

$$\text{LHS} \equiv a_i^p + pa_n \pmod{p\mathbb{Z}_p}.$$

With the convention $a_{\frac{n}{p}} = 0$ when n is not divisible by p , we have

$$\text{LHS} \equiv a_{\frac{n}{p}}^p + pa_n \pmod{p\mathbb{Z}_p}.$$

To calculate the coefficient of RHS we again consider only the polynomial

$$\sum_{i \leq \frac{n}{p}} a_i X^{pi} (1 + p \sum_{j \leq n} b_j X^j)$$

and the coefficient of X^n is

$$\text{RHS} \equiv a_{\frac{n}{p}} \pmod{p\mathbb{Z}_p}$$

Since $\frac{n}{p} < n$, the induction hypothesis shows that $a_{\frac{n}{p}} \in \mathbb{Z}_p$, and hence $a_{\frac{n}{p}}^p \equiv a_{\frac{n}{p}} \pmod{p\mathbb{Z}_p}$. By comparison we obtain that $pa_n \in p\mathbb{Z}_p$ and $a_n \in \mathbb{Z}_p$. $\square$

Corollary 2.53. For t a p -adic integer $F(t, Y) \in 1 + Y\mathbb{Z}_p[[Y]]$.

Proof. We compute $\frac{F(t,Y)^p}{F(t^p,Y^p)} = \frac{(1+Y)^{pt}}{(1+Y^p)^t}$. We see trivially that $\frac{(1+Y)^p}{(1+Y^p)} \in 1 + pY\mathbb{Z}_p[[Y]]$ and this is an ideal so its integer powers are also $\in 1 + pY\mathbb{Z}_p[[Y]]$, applying the Dwork Dieudonné criteria 2.52 allow us to conclude. $\square$

Definition 2.54. In the notations of theorem 2.49, we define the Θ function and β_k , its coefficients as follow.

$$\Theta(t) = F(t, \lambda) = \sum_{k=0}^{\infty} \beta_k t^k.$$

We observe that $\beta_k = \alpha_k(\lambda)$.

Remark 2.55. We have for π a root of $X^{p-1} + p = 0$, then $\Theta(t) = E_p(\pi t)$. Where $E_p(X) = \exp(x + \frac{1}{p}X^p + \frac{1}{p^2}X^{p^2} + \dots) = 1 + x + \dots$ is the Artin-Hasse exponential.

To consider the convergence of Θ , we need the following well known lemma.

Lemma 2.56. For $\varepsilon = 1 + \lambda$, we have $v_p(\lambda) = p - 1$.

Proof. Since the minimal polynomial for ε is $\Phi_p(X)$, the minimal polynomial for λ is $\Phi_p(X + 1)$, this is an Eisenstein polynomial hence correspond to a totally ramified extension of degree $p - 1$, we apply theorem 2.20 and get $v(\lambda) = \frac{1}{p-1}v_p(p) = \frac{1}{p-1}$. $\square$

Corollary 2.57. Θ is convergent on the disc $\{v_p(t) \geq \frac{1}{p-1}\}$.

Proof. Combining the remark 2.51 with lemma 2.56 gives us that $v_p(\beta_k) \geq \frac{k}{p-1}$. $\square$

Proposition 2.58. For $t \in \mathbb{F}_{p^s}$ $\text{Tr}_{\mathbb{Q}_{p^s}/\mathbb{Q}_p}([t]) = \sum_{\sigma} \sigma([t]) = \sum_{i=0}^{p-1} \text{Fr}^i([t]) = [t] + [t]^p + \dots + [t]^{p^{s-1}} \in \mathbb{Z}_p$. Where $\mathbb{Q}_{p^s}$ is a non ramified extension of degree s .

Proof. See Proposition 2.31. $\square$

Remark 2.59. By our definition of $F(t, Y)$, explicit calculation shows that

$$(1 + Y)^{\text{Tr}([t])} = F([t], Y)F([t]^p, Y) \dots F([t]^{p^{s-1}}, Y).$$

Proof. (proof of the theorem 2.49) In the above remark, let $Y = \lambda$, we get

$$\varepsilon^{\text{Tr}([t])} = \Theta([t])\Theta([t]^p) \dots \Theta([t]^{p^{s-1}}).$$

But we know that $\varepsilon^p = 1$, hence the left hand side relies only on the class of $\text{Tr}([t])$ modulo p , since $\text{Tr}([t]) \in \mathbb{Z}_p$, we obtain $\text{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(t) \equiv \text{Tr}_{\mathbb{Q}_{p^s}/\mathbb{Q}_p}([t]) \pmod{p}$. Thus,

$$\varepsilon^{\text{Tr}(t)} = \Theta([t])\Theta([t]^p) \dots \Theta([t]^{p^{s-1}}).$$

$\square$

2.5. Trace and determinant for infinite matrices. We define a trace and determinant for some special infinite matrices satisfying a convergence condition, to express the zeta function as a sum of traces.

Let L be a non archimedean field with valuation v_p .

Definition 2.60. We consider the Laurent series with n variables $L[X_1, \dots, X_n, X_1^{-1}, \dots, X_n^{-1}]$. Let $u \in \mathbb{Z}^n$, $X^u = X_1^{u_1} \dots X_n^{u_n}$. We say $u \geq 0$ if $u_i \geq 0$ for $i = 1, \dots, n$, and $\deg(u) = \sum_{i=1}^n u_i$.

Definition 2.61. Let $E = L[[X]]$ the formal series of n variables, For all $G \in E$, by abuse of notation we also use G to denote $G : \text{End}(E) \rightarrow \text{End}(E)$, $\varphi \mapsto G\varphi$.

We define $\Psi_q \in \text{End}(E)$ by

$$\Psi_q\left(\sum_{u \geq 0} a_u X^u\right) = \sum_{u \geq 0} a_{qu} X^u.$$

Remark 2.62. If $G = \sum_w g_w X^w$, then $\Psi_q \circ G \in \text{End}(E)$ is represented by the infinite matrix $\Psi_{q,G}(u, v) := g_{qv-u}$. We think $\{u\}, \{v\}$ as a topological basis, and $M(u, v)$ is coefficient of v for the image of u .

Proposition 2.63. In the above definition, we have:

- (i) $\Psi_q \circ \Psi_{q'} = \Psi_{qq'}$.
- (ii) $G \circ \Psi_q = \Psi_q \circ G_q$, where $G_q(X) = G(X^q)$.

Proof. (i) is trivial by definition. (ii) comes from explicit calculation: $G \circ \Psi_q(u, v) = g_{v-\frac{1}{q}u}$, and $\Psi_q \circ G_q(u, v) = g_{v-\frac{1}{q}u}$, where the coefficient $g_{v-\frac{1}{q}u} = 0$ if $q \nmid u$. $\square$

We now consider a convergence condition that allows us to define a trace that is convergent.

Definition 2.64. We say a series satisfy the convergence condition 2.64 if there exists a $M > 0$, such that $v_p(g_v) \geq M \deg(v)$.

Example 2.65. If $n = 1$, a series $G(x)$ satisfy the condition 2.64 if and only if there exist $r > 0$, such that g is convergent on $\{v_p(x) \geq r\}$

Remark 2.66. The condition 2.64 is weaker than the condition of a Tate algebra.

Remark 2.67. If G_1, G_2 satisfies the condition 2.64, then $G_1 + G_2, G_1 G_2$, and $G_1(X^h)$ satisfy the condition 2.64 for $h \geq 0$ an integer.

Proposition 2.68. Let G satisfies the condition 2.64, for $s \geq 1$, we set $\text{Tr}(\Psi^s) = \sum_{u \geq 0} (\Psi_{q,G})^s(u, u)$ the trace of matrix $\Psi_{q,G}$. Then $\text{Tr}(\Psi^s)$ is convergent. Moreover, we have

$$(q^s - 1) \text{Tr}(\Psi^s) = \sum_{x^{q^s}=1} G(x) G(x^q) \cdots G(x^{q^{s-1}})$$

where $x = (x_1, \dots, x_n) \in \mathbb{C}_p^n$, and $x^{q^s} = 1$ means that $x_i^{q^s} = 1$ for $i = 1, \dots, n$.

Proof. We can replace q by q^s , and $G(X)$ by $G(X)G(X^q) \cdots G(X^{q^{s-1}})$ by applying the two formulas of proposition 2.63. We can suppose that $s=1$. We have then $\text{Tr}(\Psi) = \sum_{u \geq 0} g_{(q-1)u}$ is convergent since G satisfies the condition 2.64 and this is a strict sub series.

On the other hand we know that

$$\sum_{x^{q-1}=1} x^v = \begin{cases} (q-1)^n & \text{if } (q-1) \mid v \\ 0 & \text{if } (q-1) \nmid v \end{cases}.$$

Thus we have

$$\sum_{x^{q-1}=1} G(x) = (q-1)^n \sum_{u \geq 0} g_{(q-1)u}.$$

$\square$

Definition 2.69. Let G satisfies the condition 2.64. We define the determinant for the matrix $1 - t\Psi$, where t is a variable by

$$\det(1 - t\Psi) := \sum_{k=0}^{\infty} \gamma_k t^k$$

where $\gamma_k := (-1)^k \sum_{u, \sigma} \varepsilon(u, v) \Psi(u_1, v_1) \cdots \Psi(u_k, v_k)$, with $u_1 < \cdots < u_k$ distinct, $v_1, \dots, v_k$ is a permutation of u , say that $\sigma(u) = v$ for a permutation σ and $\varepsilon(u, v) := \varepsilon(\sigma)$. γ_k is the determinant of all matrices of size $k \times k$.

Proposition 2.70. γ_k is convergent.

Proof. We calculate for $\Psi(U)$, a general term of γ_k , we have by the condition 2.64 $v_p(\Psi(U)) \geq M(q-1) \sum_{i=1}^k \deg(u_i)$. Thus we have $v_p(\Psi(U)) \rightarrow \infty$ when $u_k \rightarrow \infty$. $\square$

Proposition 2.71. *Let G satisfies the condition 2.64,*

- (i) $\det(1 - t\Psi) = \exp(-\sum_{s=1}^{\infty} \text{Tr}(\Psi^s) \frac{t^s}{s})$.
- (ii) *The power series $\det(1 - t\Psi)$ is convergent on the whole plane $\mathbb{C}_p$.*

Proof. (i) We know that $1 - X = \exp(\log(1 - X)) = \exp(-\sum_{s=1}^{\infty} \text{Tr}(X^s) \frac{t^s}{s})$, and $\det(\exp(X)) = \exp(\text{Tr}(X))$, this gives us $\det(1 - t\Psi) = \exp(-\sum_{s=1}^{\infty} \text{Tr}(\Psi^s) \frac{t^s}{s})$ for finite matrices.

Let Ψ_r denote the truncated $r \times r$ matrix, we have then $\det(1 - t\Psi_r)$ tend to $\det(1 - t\Psi)$ when $r \rightarrow \infty$ for the simple convergence of coefficients.

(ii) $\Leftrightarrow (-\liminf \frac{v_p(\gamma_k)}{k} = -\infty)$. Since we have $v_p(\Psi(U)) \geq M(q-1) \sum_{i=1}^k \deg(u_i)$, we have thus $v_p(\gamma_k) \geq M(q-1) \inf(\sum_{i=1}^k \deg(u_i))$. Here the infimum is taken over $u_1, \dots, u_n$ positive and distinct. So we want to show that $\frac{d_k}{k} \rightarrow +\infty$ after setting $d_k = \inf(\sum_{i=1}^k \deg(u_i))$. We can reorder $u_1, \dots, u_n$ such that $\deg(u_i) \leq \deg(u_{i+1})$, then $d_k = \sum_{i=1}^k \deg(u_i)$. Since $\deg(u_i)$ tend to infinity, in fact we know that $|\{u \in \mathbb{Z}_{\geq 0}^n, \deg(u) < k\}| =: F(n, k) < +\infty$ is a combinatorial function, so the same for its mean value. Hence we have $\frac{d_k}{k} \rightarrow +\infty$, when $k \rightarrow \infty$. $\square$

2.6. End of the proof. Now we have all the tools needed to do the explicit calculation on the torus as we said before.

We know by the characterisation of finite field that for $q = p^t$, $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ for P a irreducible polynomial of degree t , hence all finite field are affine varieties so we can suppose $q = p$ and $K = \mathbb{F}_p$.

Now, set $K \subset K_s$ the unique field extension of degree s .

Proof. (proof of theorem 2.48) We denote $N_s = |X(K_s)|$, the number of K_s points of X . Choose $t \in K_s$, we apply theorem 2.49 and denote $\theta_s(t)$ the p -th root of the unit defined by

$$\theta_s(t) = \varepsilon^{\text{Tr}(t)} = \Theta([t])\Theta([t]^p) \cdots \Theta([t]^{p^{s-1}}).$$

Since θ_s is a non trivial character of K_s , we have:

$$\sum_{x_0 \in K_s} \theta_s(x_0 u) = \begin{cases} p^s & \text{if } u = 0 \\ 0 & \text{if } u \neq 0 \end{cases}.$$

For $u = f(x)$, we take the sum and get

$$p^s N_s = (p^s - 1)^n + \sum_{\substack{x \in \mathbb{T}_{K_s}^n \\ x_0 \in K_s^\times}} \theta_s(x_0 f(x)).$$

We write $X_0 f(X_1, \dots, X_n)$ as sum of monomials $\sum_{i=1}^P a_i X^{w_i}$, where $X = (X_0, \dots, X_n)$, $a_i \in \mathbb{F}_p$. We have thus

$$p^s N_s = (p^s - 1)^n + \sum_{X^{p^s-1}=1} \prod_{i=1}^P \theta_s(a_i X^{w_i}).$$

since θ_s is a character. We pass to Teichmüller representative and apply theorem 2.49 and get

$$p^s N_s = (p^s - 1)^n + \sum_{X^{p^s-1}=1} \prod_{i=1}^P \prod_{j=0}^{s-1} \Theta([a_i X^{w_i}]^{p^j}).$$

We set $G(X) = \prod_{i=1}^P \Theta([a_i X^{w_i}])$, and the equation is written as

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

We've seen in corollary 2.57 that $v_p(\beta_k) \geq \frac{k}{p-1}$, hence $\Theta([a_i X^{w_i}])$ satisfy the condition 2.64, we have the same for G as product.

We then apply the proposition 2.68 with $q = p$ and get

$$p^s N_s = (p^s - 1)^n + (p^s - 1)^{n+1} \text{Tr}(\Psi^s).$$

We do the Newton binomial and obtain

$$p^s N_s = \sum_{i=0}^n (-1)^i \binom{n}{i} p^{s(n-i)} + \sum_{i=0}^{n+1} \binom{n+1}{i} p^{s(n+1-i)} \text{Tr}(\Psi^s).$$

We now set $\Delta(t) = \det(1 - t\Psi) = \exp(-\sum_{s=1}^{\infty} \text{Tr}(\Psi^s) \frac{t^s}{s})$ as in proposition 2.71.

We multiply the formula by $\frac{t^s}{s}$

$$p^s N_s \frac{t^s}{s} = \sum_{i=0}^n (-1)^i \binom{n}{i} p^{s(n-i)} \frac{t^s}{s} + \sum_{i=0}^{n+1} \binom{n+1}{i} p^{s(n+1-i)} \text{Tr}(\Psi^s) \frac{t^s}{s}.$$

Then we take sum over s , then apply the exponential, at the left hand side we get $Z(X, pt)$. We have precisely

$$Z(X, pt) = \prod_{i=0}^n (1 - p^{n-i}t)^{(-1)^{i+1} \binom{n}{i}} \prod_{i=0}^{n+1} \Delta(p^{n+1-i}t)^{(-1)^{i+1} \binom{n+1}{i}}.$$

Since Δ is convergent on the whole plane $\mathbb{C}_p$, see proposition 2.71, we have that $Z(X, t)$ is meromorphic on the entire plane $\mathbb{C}_p$, then we've completed our proof. $\square$

Remark 2.72. *With a slight modification, Dwork's proof of rationality is also valid for the exponential sums discussed in the introduction.*

Acknowledgements. I'd like to give sincere gratitude to my supervisor Jean-François Dat for his careful guidance and insightful and enlightening remarks with a very modern view point from which I've benefited a lot. It also occurs to me to thank Sorbonne Université for such a marvelous opportunity. Nonetheless, I've also like to thank gratefully all my professors of this year Hélène Eynard-Bontemps, Alexis Boutier, Farrell Brumley, Jean-François Dat, Antoine Ducros, Elisha Falbel, Mathieu Florence, Quentin Gazda, Lourenço Joao, Loïc Merel, Matteo Tamiozzo, Jean-Baptiste Teyssier, who had given inspiring courses in various topics in mathematics that had really broaden my horizon, and especially to Javier Fresan to whom I owe the introduction.

REFERENCES

- [Bor84] Émile Borel. Sur une application d'un théorème de M. Hadamard. *Bulletin des Sciences Mathématiques. Deuxième Série*, 22-25 (1894).
- [Col1] Pierre Colmez. Les nombres p -adiques, notes du cours de M2.
- [Col2] Pierre Colmez. Distributions et fonctions analytiques, notes du cours de M2.
- [DW58] Bernard Dwork. Norm residue symbol in local number fields. *Abh. Math. Sem. Univ. Hamburg*, t. 22, 1958, p. 180-190.
- [DW60] Bernard Dwork. On the Rationality of the Zeta Function of an Algebraic Variety. *American Journal of Mathematics*, vol. 82, no. 3, 1960, pp. 631-48.
- [FP] Javier Fresán, Peter Jossen. Exponential motives.
- [FK88] Eberhard Freitag, Reinhardt Kiehl. Etale Cohomology and the Weil Conjecture *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics*, (MATHE3, volume 13) 1988.
- [Ked06] Kiran S. Kedlaya. Fourier transforms and p -adic 'Weil II' *Compositio Mathematica*, 2006.
- [Kob74] Neal Koblitz. p -adic Numbers, p -adic Analysis, and Zeta-Functions. *Graduate Texts in Mathematics*, volume 58 1974.
- [KW01] Reinhardt Kiehl, Rainer Weissauer. Weil Conjectures, Perverse Sheaves and ℓ -adic Fourier Transform *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics*, (MATHE3, volume 42) 2001.
- [Lou] João Lourenço. Espace Perfectoïdes, notes du cours de M2.
- [Rob00] Alain M. Robert. A Course in p -adic Analysis. *Graduate Texts in Mathematics*, volume 198, 2000.
- [Ser60] Jean-Pierre Serre. Rationalité des fonctions ζ des variétés algébriques. In *Séminaire Bourbaki*, no. 5 (1960), Exposé no. 198.
- [Tao] Terence Tao. Dwork's proof of rationality of the zeta function over finite fields.