Zeta functions over finite fields
an exposition of Dwork’s methods

Martin Ortiz Ramirez

Part B Extended Essay

Hilary Term 2020
1 Introduction

Let \( \mathbb{F}_q \) be the finite field of \( q = p^r \) elements, and \( X \) an affine variety over \( \mathbb{F}_q \), that is,

\[
X = \{(x_1, x_2, \ldots, x_n) \in (\mathbb{F}_q)^n \mid f_i(x_1, \ldots, x_n) = 0 \ \forall \ i = 1, 2, \ldots, m\}
\]

for some \( f_i \in \mathbb{F}_q[x_1, x_2, \ldots, x_n] \). Then, for an extension \( K = \mathbb{F}_{q^s} \) of \( \mathbb{F}_q \) (all finite field extensions are of this form) let \( N_s \) be the number of \( K \)-points of \( X \), i.e. the number of common zeros of the
when they are considered over \(\mathbb{F}_q\). We can encode most of the information about the \(N_s\) in a formal power series:

\[
Z(X/\mathbb{F}_q; T) = \exp \left( \sum_{s=1}^{\infty} N_s \frac{T^s}{s} \right).
\]

This is the zeta function of \(X\), it is defined analogously for projective varieties, but the defining polynomials are homogeneous. For instance, the zeta function of \(\mathbb{A}^n\) is

\[
Z(\mathbb{A}^n/\mathbb{F}_q; T) = \exp \left( \sum_{s=1}^{\infty} q^{ns} \frac{T^s}{s} \right) = \exp(- \log(1 - q^n T)) = \frac{1}{1 - q^n T}.
\]

Zeta functions of varieties over finite fields have been extensively studied in the past century, being an important area of the development of modern number theory and algebraic geometry. The most famous result about them are the Weil conjectures, proposed by Weil in 1949, which have since then been proved. One part of the conjecture, the rationality conjecture, says that the zeta function of any affine or projective variety is a rational function (all the other conjectures require \(X\) to be projective and smooth). This was proved by Dwork in 1960 using \(p\)-adic analytic methods, the approach that we will use here. However, the rationality conjecture, along the rest of the conjectures were later proved via abstract topology such as étale cohomology, developed by Grothendieck, and expanded by Deligne, which earned him the Fields Medal in 1978.

It can be easily proved (see Lemma 3.1) that the rationality conjecture reduces to the case of an affine hypersurface. Because of that we will only consider affine or projective hypersurfaces, which are easier to study. The aim of this essay is to give an exposition of Dwork’s proof of the rationality conjecture, to then introduce a form of \(p\)-adic cohomology due to Dwork, which will be useful to compute zeta functions of non-singular projective hypersurfaces. In particular we will study the projective hypersurface defined by

\[
\sum_{i=1}^{4} x_i^4 - 4\lambda \prod_{i=1}^{4} x_i \in \mathbb{F}_p[x_1, x_2, x_3, x_4].
\]

In the next section we recall a few concepts about \(p\)-adic numbers.

## 2 Background

### 2.1 \(p\)-adic numbers

Let \(p \in \mathbb{Z}\) be a prime number, for a nonzero integer \(n\) let \(\text{ord}_p(n)\) be the largest power of \(p\) that divides \(n\), by convention we define \(\text{ord}_p(0) = \infty\). For a rational number \(x = a/b\) we extend the notion of order by \(\text{ord}_p(x) = \text{ord}_p(a) - \text{ord}_p(b)\). Now we can define a norm in \(\mathbb{Q}\):

\[
|x|_p = \begin{cases} 
0 & \text{if } x = 0 \\
\frac{1}{p^{\text{ord}_p(x)}} & \text{otherwise.}
\end{cases}
\]
It is easy to check that \(|xy|_p = |x|_p|y|_p\) and that \(|\cdot|_p\) satisfies the triangle inequality, so that \(\mathbb{Q}\) becomes a metric space with the \(p\)-adic norm. In fact it is true that \(|x + y|_p \leq \max(|x|_p, |y|_p)\), which means that \(|\cdot|_p\) is a non-Archimedean norm. A useful consequence of this is that every \(p\)-adic 'triangle' is isosceles, that is, if \(|x|_p < |y|_p\) then \(|x + y|_p = |y|_p\). We will refer to this as the isosceles triangle principle.

Note that \(\mathbb{Q}\) is not complete with this metric, the sequence \((\sum_{n=0}^{N} p^n)_{N \geq 0}\) is Cauchy, but it does not converge in \(\mathbb{Q}\). Because of this we define the \(p\)-adic numbers \(\mathbb{Q}_p\) as the completion of \(\mathbb{Q}\) with respect to the \(p\)-adic norm. The elements of \(\mathbb{Q}_p\) are equivalence classes of Cauchy sequences in \(\mathbb{Q}\), if \(a = (a_n)\) is not equivalent to 0, for a given \(\epsilon > 0\) choose \(N\) such that \(|a_n - a_m|_p < \epsilon\) whenever \(n, m \geq N\), and some \(k \geq N\) such that \(|a_k|_p > \epsilon\). Then by the isosceles triangle principle \(|a_k|_p = |a_m|_p\) for all \(m \geq N\), and hence we can define \(|a|_p = \lim_{n \to \infty} |a_n|_p\). It can be shown that this extension is indeed a non-Archimedean norm. Furthermore, \(\mathbb{Q}_p\) is also a field, and by construction, a complete metric space.

More concretely, any \(a \in \mathbb{Q}_p\) has a unique expansion of the form

\[
a = \sum_{n=-N}^{\infty} b_n p^n \quad \text{for } b_n = 0, 1, \ldots, p - 1,
\]

where the convergence takes place in the \(p\)-adic norm. We define \(\mathbb{Z}_p\) to be the valuation ring of \(\mathbb{Q}_p\), i.e. the elements of norm \(\leq 1\). It is easy to see that \(\mathbb{Z}_p\) is a principal ideal domain with every ideal being of the form \((p)^n\), and that \(\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p\). We will use the notation \(a = b \text{ mod } p\) to mean \(|a - b|_p \leq |p|_p = p^{-1}\).

It is also worth introducing the concept of the Teichmüller representative of some \(x \in \mathbb{F}_p\). It is defined to be the unique element \(\alpha\) in \(\mathbb{Z}_p\) such that \(x = \alpha \text{ mod } p\) and that \(\alpha^p = \alpha\). To prove existence, let \(a\) be an integer between 0 and \(p - 1\) that reduces to \(x\) mod \(p\). We can see that the sequence \((a^p)^n\) is Cauchy, thus it converges to some \(\alpha \in \mathbb{Q}_p\). By construction \(\alpha^p = \alpha\) and \(\alpha = x \text{ mod } p\), since \(a^p = a \text{ mod } p\). To prove uniqueness, there are at most \(p\) roots of \(x^p - x\) in \(\mathbb{Q}_p\), but we know that there is at least one for each \(n = 0, 1, \ldots, p - 1\), which are different from each other since their reduction mod \(p\) are different.

### 2.2 Algebraic extensions of \(\mathbb{Q}_p\)

We want to make sense of the norm of an element of \(\mathbb{Q}_p\), by extending the existing norm on \(\mathbb{Q}_p\). Let \(K\) be a finite extension of \(\mathbb{Q}_p\), for \(\alpha \in K\) we define \(N_{K/\mathbb{Q}_p}(\alpha) = \det(E_\alpha)\), where \(E_\alpha\) is the \(\mathbb{Q}_p\)-linear map from \(K\) to itself of multiplication by \(\alpha\). By choosing a basis for \(\mathbb{Q}_p(\alpha)\) and then multiplying it with a \(\mathbb{Q}_p(\alpha)\)-basis for \(K\) we see that \(E_\alpha\)'s matrix has a block form

\[
\begin{pmatrix}
A_\alpha & 0 \\
0 & A_\alpha & \\
& & \ddots & A_\alpha
\end{pmatrix},
\]

3
where $A_\alpha$ is the multiplication map from $\mathbb{Q}_p(\alpha)$ to itself. Therefore

$$N_{K/\mathbb{Q}_p}(\alpha) = N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)[K:\mathbb{Q}_p(\alpha)].$$

By choosing a basis of powers of $\alpha$ for $\mathbb{Q}_p(\alpha)$ we see that $N_{K/\mathbb{Q}_p}(\alpha)$ is in $\mathbb{Q}_p$. Because of that we can set the norm of $\alpha$ to be

$$|\alpha|_p = \left|N_{K/\mathbb{Q}_p}(\alpha)\right|^{1/[K:\mathbb{Q}_p]}_p.$$ 

This definition is independent of the choice of $K$ since

$$[K : \mathbb{Q}_p] = [K : \mathbb{Q}_p(\alpha)][\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$$

implies

$$|\alpha|_p = \left|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|^{1/[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]}_p.$$ 

It is easy to prove that this new norm is multiplicative, agrees with the old one in $\mathbb{Q}_p$ and $|\alpha|_p = 0$ if and only if $\alpha = 0$. The harder part is proving that the norm is non-Archimedean, this can be found in [Kob84, Ch.3, Thm.11]. Once this is proved we can extend the $p$-adic norm to $\overline{\mathbb{Q}}_p$, as our definition agrees in any finite extension of $\mathbb{Q}_p$. We also extend the notion of the order of an element $x \in \mathbb{Q}_p$: 

$$\text{ord}_p(x) = -\log_p |x|_p.$$ 

Now, let $K$ be a finite field extension of $\mathbb{Q}_p$. The integral closure of $\mathbb{Z}_p$ in $K$ consists of all the $\alpha \in K$ that are roots of a monic polynomial over $\mathbb{Z}_p$. This has a nice characterization in terms of the $p$-adic norm.

**Theorem 2.1** (Ch.3, Sec.2 [Kob84]). Let $K$ be a finite extension of $\mathbb{Q}_p$, and let

$$\mathcal{O}_K = \{x \in K : |x|_p \leq 1\}$$

$$\mathfrak{m}_K = \{x \in K : |x|_p < 1\}$$

Then $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}_p$ in $K$, it is also a local ring with maximal ideal $\mathfrak{m}_K$. Furthermore, $k_K = \mathcal{O}_K/\mathfrak{m}_K$, the residue field of $K$, is a finite extension of $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Let $K$ be a finite extension of $\mathbb{Q}_p$ of degree $n$, then the map $\text{ord}_p : K^* \to \frac{1}{n}\mathbb{Z}$ is a group homomorphism. Its image is an additive subgroup of $\frac{1}{n}\mathbb{Z}$, so it must be of the form $\frac{1}{e}\mathbb{Z}$. We define $e$ to be the ramification index of $K$. Let $\pi \in K$ such that $\text{ord}_p(\pi) = 1/e$, then each $x \in K$ has a unique representation as $x = \pi^m x'$, where $|x'|_p = 1$, hence $\mathfrak{m}_K = \pi \mathcal{O}_K$. An extension is unramified when $e = 1$, in this case we can take $\pi = p$. The next lemma relates the ramification index and the degree of the residue field.

**Lemma 2.2.** Let $K$ be a finite extension of $\mathbb{Q}_p$ of degree $n$. Let $e$ be the ramification index, and $f$ the degree of the residue field over $\mathbb{F}_p$. Then $ef = n$. In particular, $K$ is unramified if $f = n$.

**Proof.** Recall that $\mathbb{Q}_p$ has characteristic 0, so $K/\mathbb{Q}_p$ is separable, and that $\mathbb{Z}_p$ is a principal ideal domain, with field of fractions $\mathbb{Q}_p$. In this setting we can use a general theorem that tells us that $\mathcal{O}_K$ is a free module over $\mathbb{Z}_p$ of rank $n = [K : \mathbb{Q}_p]$ [Neu99, Prop 2.10].
Now, let $\pi \in K$ such that $\text{ord}_p(\pi) = 1/e$, so that $m_K = \pi O_K$. Since $\pi^e$ and $p$ have the same order, $(p) = (\pi^e)$ as ideals in $O_K$. Each quotient $\pi^nO_K/\pi^{n+1}O_K$ is isomorphic to $k_K = O_K/\pi O_K$ as abelian groups, thus they have cardinality $p^f$. This means that $O_K/(p) = O_K/(\pi)^e$ has cardinality $p^f$. But as $\mathbb{Z}_p$-modules $O_K/pO_K \cong \mathbb{Z}_p^n/p\mathbb{Z}_p^n$, so that comparing cardinalities gives $ef = n$. \qed

Now we extend the notion of the Teichmüller representative to elements of $\mathbb{F}_q$. We will see that they lie in an unramified extension of $\mathbb{Q}_p$ of degree $r$.

**Theorem 2.3.** Let $q = p^r$. There is a unique unramified extension of $\mathbb{Q}_p$ of degree $r$, where the Teichmüller representatives of $\mathbb{F}_q$ lie. The extension is generated by a primitive $(q - 1)$-th root of unity.

**Proof.** The multiplicative group of a finite field is cyclic, so let $\overline{\alpha}$ be a generator of $\mathbb{F}_q^*$, and let $\overline{p}(x)$ be its minimal polynomial over $\mathbb{F}_p$. Since $\overline{\alpha}$ generates $\mathbb{F}_q$ it must be of degree $r$. Now let $p(x) \in \mathbb{Z}_p[x]$ be a polynomial reducing to $\overline{p}(x) \mod p$, by Gauss’s lemma it is irreducible over $\mathbb{Q}_p$. Let $\alpha \in \mathbb{Q}_p$, be a root of $p(x)$ and define $K = \mathbb{Q}_p(\alpha)$, so that $[K : \mathbb{Q}_p] = r$. Being a root of a monic polynomial in $\mathbb{Z}_p$, $\alpha$ lies in $O_K$. We know that the degree of $k_K$ over $\mathbb{F}_p$ is less or equal than $r$, and that $\alpha + m_K$ is a root of the degree $r$ irreducible polynomial $\overline{p}(x)$. Therefore $k_K \cong \mathbb{F}_q$. By Lemma 2.2 we know that $K$ is unramified, so that $m_K = pO_K$.

Now for some $x \in \mathbb{F}_q$, choose some $a \in O_K$ such that $x = a + m_K$. Since the $\alpha^i + m_K$ freely generate $k_K \cong \mathbb{F}_q$, we can choose $a$ such that

$$a = \sum_{i=0}^{r-1} \lambda_i \alpha^i \quad \text{for } \lambda_i \in \mathbb{Z}_p.$$  

We want to show that the sequence $(a^n)_{n \geq 0}$ converges in $K$. By Lagrange's theorem $a^{q-1} = 1 \mod m_K$, so that the coefficients of $\alpha^i$ in the expansion (2.1) of $a^{q-1} - 1$ must be in $m_K \cap \mathbb{Z}_p = p\mathbb{Z}_p$. By induction it is easy to see that $a^{q^n(q-1)} \in 1 + p^{n+1}\mathbb{Z}_p[\alpha]$, that is, $a^{q^n+1} - a^{q^n} \in p^{n+1}\mathbb{Z}_p[\alpha]$. Telescoping this sum gives that $a^{q^n} - a^{q^m} \in p^{m+1}\mathbb{Z}_p[\alpha]$ for $n > m$. This means that the coefficients in the expansion (2.1) of $a^{q^n}$ are Cauchy, hence they converge in $\mathbb{Z}_p$. Therefore $a^{q^n}$ converges to some $\beta \in K$. We have seen that $a^q = a = a^q \mod m_K$, so that $\beta = a \mod m_K$. Also, by construction $\beta^q = \beta$. This is the Teichmüller representative of $x \in \mathbb{F}_q$, notice that each Teichmüller representative is different from each other, because their reduction mod $m_K$ are different. Thus $K$ contains all $q$ roots of $x^q - x$. Let $\beta$ be a primitive $(q - 1)$-th root of unity, then $L = \mathbb{Q}_p(\beta) \subseteq K$. The inclusion induces the embedding

$$L/O_L \to K/O_K \quad a + O_L \longmapsto a + O_K,$$

which is in fact surjective, since $\{\beta^n : 1 \leq n \leq q - 1\}$ contains all the nonzero Teichmüller representatives of $K$. Therefore $k_L \cong k_K \cong \mathbb{F}_q$, which means that $[L : \mathbb{Q}_p] \geq r$, and this implies that $K = L$.

Finally let $K'$ be other unramified extension of degree $r$, so that $k_{K'} \cong \mathbb{F}_q$ for $q = p^r$ by Lemma 2.2. By taking $\overline{\alpha}$ to be a generator of $k_{K'}$, we can repeat the same argument to show that $K'$ is generated by a primitive $(q - 1)$-th root of unity, hence $K = K'$. \qed
We will denote the Teichmüller representative of \( x \in \mathbb{F}_q \) as \( \text{Teich}(x) \). As a corollary of the above we obtain that for \( x, y \in \mathbb{F}_q \), \( \text{Teich}(xy) = \text{Teich}(x)\text{Teich}(y) \), since both sides are equal mod \( m_K \) and they are roots of \( x^q - x \).

**Corollary 2.4.** Let \( K = \mathbb{Q}_p(\beta) \) be the unramified extension of \( \mathbb{Q}_p \) of degree \( r \), where \( \beta \) is a primitive \( (q-1) \)-th root of unity. Then the map \( \tau : K \to K \) defined by \( \tau|_{\mathbb{Q}_p} = \text{id}_{\mathbb{Q}_p} \), \( \tau(\beta) = \beta^p \) generates \( \text{Gal}(K/\mathbb{Q}_p) \).

**Proof.** To prove that \( \tau \in \text{Gal}(K/\mathbb{Q}_p) \) we show that \( m(x) \in \mathbb{Z}_p[x] \), the minimal polynomial of \( \beta \) over \( \mathbb{Q}_p \), is \( \prod_{i=0}^{r-1}(x - \beta^p^i) \). We have that \( m(x)^p = m(x^p) + pf(x) \) for some \( f(x) \in \mathbb{Z}_p[x] \), so that \( m(\beta^p) = -pf(\beta) \). Since \( m(x) | x^{q-1} - 1 \),

\[
m(x) = \prod_{i=1}^{r}(x - \beta^{n_i}) \text{ for some different } n_i \in \{0, 1, \ldots, q-1\}.
\]

By Theorem 2.3 \( \{\beta^i + m_K \text{ for } i = 0, 1, \ldots, q-1\} = k_K \). Thus \( |m(\beta^p)|_p = |pf(\beta)|_p < 1 \) implies \( m(\beta^p) = 0 \). Repeating the argument shows that \( m(\beta^p) = 0 \) for all \( i \), so that \( m(x) = \prod_{i=0}^{r-1}(x - \beta^p^i) \). Note that \( r = [K : \mathbb{Q}_p] = |\text{Gal}(K/\mathbb{Q}_p)| \) and the \( \tau^i, i = 0, 1, \ldots, r-1 \) are pairwise different, so \( \tau \) generates \( \text{Gal}(K/\mathbb{Q}_p) \). \( \square \)

### 2.3 Power series

It can be seen that \( \overline{\mathbb{Q}}_p \) is not complete, we define \( \Omega \) to be the completion of \( \overline{\mathbb{Q}}_p \), and we extend the \( p \)-adic norm in the same way we did for \( \mathbb{Q}_p \). It turns out that \( \Omega \) is algebraically closed. As a consequence of the isosceles triangle principle, a sum \( \sum a_n \) in \( \Omega \) converges if and only if \( |a_n|_p \) tends to 0. Using this fact we see that the radius of convergence of \( \sum_{n=0}^{\infty} a_n x^n \in \Omega[[x]] \) is given by \( R^{-1} = \limsup |a_n|_p^{1/n} \). A power series with infinite radius of convergence is said to be *entire*. We will use of standard properties of well-known power series, such as \( \exp \), \( \log \), or the binomial expansion [Kob84, Ch.4].

Now we introduce the concept of the Newton polygon of a power series \( 1 + \sum_{n=1}^{\infty} a_n x^n \). Plot the points \( (n, \text{ord}_p(a_n)) \) in the plane. The Newton polygon is defined as the convex hull of these points, and it consists of segments joining vertices \( (n, \text{ord}_p(a_n)) \), although the last segment may be infinite. Let \( K \) be a complete extension of \( \mathbb{Q}_p \), and \( D(p^\lambda) = \{ x \in \Omega : |x|_p \leq p^\lambda \} \). The main result about Newton polygons is the following [Kob84, Ch.4, Thm.14].

**Theorem 2.5 (\( p \)-adic Weirstrass Preparation Theorem).** Let \( f(x) \in 1 + x K[[x]] \) converge in \( D(p^\lambda) \). Let \( N \) the total horizontal length of the segments of the Newton polygon having slope \( \leq \lambda \), if this length is finite. Otherwise take \( N \) to be largest integer such that \( (N, \text{ord}_p(a_N)) \) lies on the last segment, of slope \( \lambda \) (which exists because \( f(x) \) converges on \( D(p^\lambda) \)). Then there exists a polynomial \( h(x) \in 1 + K[x] \) of degree \( N \) and a power series \( g(x) \in 1 + x K[[x]] \) which is nonzero and converges in \( D(p^\lambda), \) such that

\[
h(x) = f(x)g(x).
\]

Furthermore, all the roots of \( h(x) \) lie on \( D(p^\lambda) \).
For some $f(x) \in 1 + \Omega[[x]]$ define $\lambda(f)$ as the slope of the first segment of its Newton polygon.

**Corollary 2.6.** Let $f(x) \in 1 + xK[[x]]$ be entire, where $K$ is a complete extension of $\mathbb{Q}_p$. Then it has a unique factorization of the type

$$f(x) = \prod_{i=1}^{\infty} p_i(x)^{n_i},$$

where the product ranges over distinct irreducible polynomials in $K[x]$ with constant term 1, and $\lambda(p_i) \to \infty$.

**Proof.** For each $\lambda$, let $h_\lambda(x) = f(x)g_\lambda(x)$ as in Theorem 2.5. We claim that $h_\lambda(x) \to f(x)$ as $\lambda$ tends to infinity. Let $h_\lambda(x) = \sum c_{n,\lambda}x^n$, $f(x) = \sum a_n x^n$, and $g_\lambda(x) = \sum b_{n,\lambda}x^n$. By [Kob84, Ch. 4, Lemma 7], for $n > 0$ we have $\text{ord}_p(b_{n,\lambda}) \geq n\lambda/2$, since $g_\lambda(x)$ has no $\Omega$-roots in $D(p^{\lambda/2})$. Now,

$$c_{n,\lambda} = a_n + \sum_{i=1}^{n} b_{i,\lambda}a_{n-i},$$

so that $|c_{n,\lambda} - a_n|_p \leq Mp^{-\lambda/2}$, where $M = \max_i |a_i|_p$. Thus $h_\lambda(x) \to f(x)$. The multiplicity of the roots of $h_\lambda(x)$ can be read by formally differentiating $f(x)$, so that for $\lambda' > \lambda$, $h_\lambda$ divides $h_{\lambda'}$ in $\Omega[x]$, which implies that one divides the other in $K[x]$. In fact, the multiplicity of the roots of $h_\lambda(x)$ and $h_{\lambda'}(x)$ in $D(p^n)$ is the same. Decomposing $h_n(x)$ into irreducible factors gives us the desired factorization, since the irreducible factors of $h_{n+1}(x)/h_n(x)$ cannot have roots with norm less than $p^n$, so that Koblitz’s lemma ensures that $\lambda(p_i) \to \infty$.

Uniqueness follows from the fact that different irreducible polynomials in $K[x]$ cannot share a root in $\Omega$, so that if $\alpha_i$ is a root of $p_i$, $n_i$ counts the multiplicity of the root in $f$. But using the $p$-adic preparation theorem, the multiplicity of a root of $f$ in $D(p^\lambda)$ is the same as its multiplicity in $h_\lambda(x)$.

Such a factorization will be called a ”Weirstrass factorization”. We will use it in Section 4 to prove Theorem 4.11.

### 3 The set-up

#### 3.1 Dwork’s character

**Lemma 3.1.** To prove Weil’s rationality conjecture it suffices to consider affine hypersurfaces.

**Proof.** Let $X = \{ x \in (\mathbb{F}_q)^n \mid f_i(x) = 0 \ \forall \ i = 1, 2 \ldots m \}$ be an affine variety. Assuming that the rationality conjecture holds for hypersurfaces we prove that $Z(X/\mathbb{F}_q; T) = Z(T)$ is rational, we...
proceed by induction on $m$. Let $X_i = \{ x \in (\mathbb{F}_q)^n \mid f_i(x) = 0 \}$. It follows from the inclusion-exclusion formula that

$$\bigg| \bigcup_i X_i \bigg| = \sum_i |X_i| - \sum_{i,j} |X_i \cap X_j| + \ldots + (-1)^n \bigg| \bigcap_i X_i \bigg| .$$

Note that

$$\bigcup_i X_i = \{ x \in (\mathbb{F}_q)^n \mid \prod_{i=1}^m f_i(x) = 0 \}$$

so that all the terms in the alternating sum are varieties defined by less than $m$ polynomials, except $\cap X_i = X$. This shows that $Z(T)$ is the product of zeta functions (or their inverses) of varieties defined by less than $m$ polynomials, thus we are done by the induction hypothesis.

Now let $X = \{ x \in \mathbb{P} \mathbb{F}_q^n \mid f(x) = 0 \}$ be a projective hypersurface, for some $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_{n+1}]$ homogeneous. We prove that $Z(T)$ is rational by induction on $n$. For $n = 0$, $X$ is just a point or the empty set, so that $Z(T) = \frac{1}{1 - T}$ or $Z(T) = 1$. Now suppose that the statement is true up to some $n-1 \geq 0$, we have the decomposition $\mathbb{P} \mathbb{F}_q^n = A_n \sqcup \mathbb{P} \mathbb{F}_q^{n-1}$, so that $N_s = N'_s + N''_s$, where $N'_s$ corresponds to an affine hypersurface, and $N''_s$ to a projective hypersurface in $\mathbb{P} \mathbb{F}_q^{n-1}$. Therefore $Z(T) = Z'(T)Z''(T)$, both of which are rational by hypothesis. The fact that projective varieties also satisfy the rationality conjecture can be proven in the same as the affine case.

We now introduce Dwork’s exponential function, which will play a key role in the theory. Let $\mathfrak{J}(x) = \exp(\pi(x - x^p))$, where $\pi \in \Omega$ such that $\pi^{p-1} = -p$. Denote its expansion by

$$\mathfrak{J}(x) = \sum_{n=0}^{\infty} c_n(\pi x)^n = \sum_{n=0}^{\infty} \lambda_n x^n. $$

**Lemma 3.2.** We have

$$\text{ord}_p(\lambda_n) \geq \frac{p-1}{p^2} n,$$

in particular $\mathfrak{J}(x)$ converges on a disk $|x|_p \leq 1 + \epsilon$, for some $\epsilon > 0$.

**Proof.** Let $\mu$ be the Möbius function, we have the following formal identity

$$\exp(x) = \prod_{k=1}^{\infty} (1 - x^k)^{-\mu(k)/k},$$

since the right hand side has logarithmic derivative

$$\sum_{k=1}^{\infty} \frac{\mu(k)x^{k-1}}{1 - x^k} = \sum_{k=1}^{\infty} \mu(k)x^{k-1} \sum_{m=0}^{\infty} x^{mk} = \sum_{n=1}^{\infty} x^{n-1} \sum_{d|n} \mu(d) = 1.$$  

We can rewrite it as

$$\exp(x) = \prod_{(k,p)=1} (1 - x^k)^{-\mu(k)/k}(1 - x^{kp})^{\mu(k)/kp},$$

8
therefore
\[ \mathcal{J}(X) = \exp(\pi(x - x^p)) = \exp(\pi x + (\pi x)^p / p) = \prod_{(k,p)=1} (1 - \pi^k x^k)^{-\mu(k)/k} (1 - \pi^k p^2 x^{kp^2})^{\mu(k)/kp^2}. \]

By the binomial expansion
\[ (1 - \pi^k x^k)^{-\mu(k)/k} = \sum_{i=0}^{\infty} (-1)^i \pi^{ki} \binom{-\mu(k)/k}{i} x^{ki} = \sum_{i=0}^{\infty} a_i(k) x^{ki}. \]

Since \((k, p) = 1\), \(1/k\) is in \(\mathbb{Z}_p\), so that \((-\mu(k)/k) \in \mathbb{Z}_p\). Thus
\[ \text{ord}_p(a_i(k)) \geq \frac{ki}{p-1} > \frac{p-1}{p^2} ik. \] (3.1)

Similarly, for the second factor
\[ (1 - \pi^{kp^2} x^{kp^2})^{\mu(k)/kp^2} = \sum_{i=0}^{\infty} (-1)^i \binom{\mu(k)/kp^2}{i} (\pi x)^{ikp^2} = \sum_{i=0}^{\infty} b_i(k) x^{ikp^2}. \]

Using that \(\text{ord}_p(i!) < i/(p-1)\),
\[ \text{ord}_p(b_i(k)) > \frac{ikp^2}{p-1} - 2i - \frac{i}{p-1} \geq \frac{p-1}{p^2} ikp^2. \] (3.2)

Putting (3.1) and (3.2) together we conclude that
\[ \text{ord}_p(\lambda_i) \geq \frac{p-1}{p^2} i, \] (3.3)
which means that \(\mathcal{J}(x)\) converges on a disk of radius bigger than 1.

We define Dwork’s character \(\Theta_p : \mathbb{F}_p \to \Omega^*\) as
\[ \Theta_p(x) = \mathcal{J}(\text{Teich}(x)). \]

Note that \(\exp\) converges in the disk \(\{|x|_p < |\pi|_p\}\), so that for \(|a|_p \leq 1\), \(\mathcal{J}(x)^p = \exp(p\pi(x - x^p))\) takes the value of \(\exp(p\pi(a - a^p))\) at \(a\). Therefore, for \(x \in \mathbb{F}_p\)
\[ \Theta_p(x)^p = \mathcal{J}(\text{Teich}(x))^p = \exp(p\pi(\text{Teich}(x) - \text{Teich}(x)^p)) = 1. \]

This means that \(\Theta_p(x)\) is a \(p\)-th root of unity.

**Lemma 3.3.**
\[ \mathcal{J}(x) = 1 + \pi x \mod \pi^2 x^2 \]
\textit{Proof.} We consider the Artin-Hasse exponential [Kob84, p.93]

\[ E(x) = \prod_{(k,p) = 1} \left( 1 - x^k \right)^{-\mu(k)/k} = \exp \left( x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \ldots \right), \]

which has coefficients in \( \mathbb{Z}_p \) because each factor has. Also, the coefficients of \( E(\pi x) \) up to \( x^{p^2-1} \) are precisely \( \lambda_i \). Hence, for \( 1 \leq i \leq p^2 - 1 \)

\[ \text{ord}_p(\lambda_i) \geq \frac{i}{p-1}. \]

For \( i \geq p^2 \) we can use the previous bound (3.3) to obtain \( |\lambda_i|_p \leq |\pi^2|_p \) for \( i \geq 2 \), as desired. \( \square \)

In particular \( \Theta_p(1) = 1 + \pi \mod \pi^2 \) and \( \Theta_p(x) = 1 + \text{Teich}(x)\pi \mod \pi^2 \). Hence

\[ \Theta_p(x) = \Theta_p(1)^{\text{Teich}(x)}, \]

since \( \Theta_p(x) \) is a \( p \)-th root of unity. By definition \( \text{Teich}(x + y) = \text{Teich}(x) + \text{Teich}(y) + pZ \) for some \( Z \in \mathbb{Z}_p \), so that \( \Theta_p(x + y) = \Theta_p(x)\Theta_p(y) \).

For \( q = p^r \) we can define \( \Theta_q : \mathbb{F}_q \to \Omega^* \) by \( \Theta_q(x) = \Theta_p(\text{tr}(x)) \), where

\[ \text{tr}(x) = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = \sum_{n=0}^{r-1} x^{p^n} \in \mathbb{F}_p. \]

It is well-known that \( \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \) is a surjective additive map onto \( \mathbb{F}_p \), so that there exists \( \alpha \in \mathbb{F}_q \) such that \( \Theta_q(\alpha) = \Theta_p(1) \neq 1 \), by Lemma 3.3. Recall that from our discussion in the previous section

\[ \text{Teich}(x + y) = \text{Teich}(x) + \text{Teich}(y) + pZ \text{ for some } |Z|_p \leq 1, \]

then

\[ \text{Teich}(\text{tr}(x)) = pZ' + \sum_{n=0}^{r-1} \text{Teich}(x)^p^n \text{ for some } |Z'|_p \leq 1. \]

Also, \( \text{Teich}(x) \) lies in the unramified extension \( K \) of \( \mathbb{Q}_p \) with \( k_K \cong \mathbb{F}_q \), and by Corollary 2.4

\[ \sum_{n=0}^{r-1} \text{Teich}(x)^p^n = \text{Tr}_{K/\mathbb{Q}_p}(\text{Teich}(x)) \in \mathbb{Q}_p \cap \mathcal{O}_K = \mathbb{Z}_p. \]

Thus \( Z' \in \mathbb{Z}_p \) and we can write

\[ \Theta_q(x) = \Theta_p(1)^{\sum_{n=0}^{r-1} \text{Teich}(x)^p^n}. \quad (3.4) \]

By a similar argument

\[ \text{Teich}(\text{tr}(x + y)) = \text{Teich}(\text{tr}(x) + \text{tr}(y)) = \text{Teich}(\text{tr}(x)) + \text{Teich}(\text{tr}(y)) + pZ = \sum_{n=0}^{r-1} (\text{Teich}(x)^p^n + \text{Teich}(y)^p^n) + pZ' \text{ for some } Z' \in \mathbb{Z}_p. \]
Therefore
\[ \Theta_q(x + y) = \Theta_q(x) \Theta_q(y). \]

We say that \( \Theta_q \) is Dwork’s multiplicative character. Let
\[
\mathfrak{J}_r(x) := \prod_{i=0}^{r-1} \mathfrak{J}(x^{p^i}) = \prod_{i=0}^{r-1} \exp(\pi(x^{p^i} - x^{p^{i+1}})) = \exp(\pi(x - x^q)).
\] (3.5)

**Lemma 3.4.** For \( x \in \mathbb{F}_q \), \( \Theta_q(x) = \mathfrak{J}_r(\text{Teich}(x)). \)

**Proof.** We know that \( \Theta_q(x) \) is a \( p \)-th root of unity and that \( \Theta_q(x) = 1 + (\sum_{n=0}^{r-1} \text{Teich}(x)^{p^n}) \pi \mod \pi^2 \), by Lemma 3.3 and (3.4). We also know that
\[
\mathfrak{J}_r(\text{Teich}(x)) = \prod_{i=0}^{r-1} (1 + \text{Teich}(x)^{p^i}) = 1 + \left( \sum_{n=0}^{r-1} \text{Teich}(x)^{p^n} \right) \pi \mod \pi^2.
\]

Therefore it is enough to prove that \( \mathfrak{J}_r(\text{Teich}(x)) \) is a \( p \)-th root of unity. We have that
\[
\mathfrak{J}_r(\text{Teich}(x))^p = \exp(p\pi(x - x^q))
\]
so that for \( |x|_p = 1 \), the inside of the exponential lies within its radius of convergence, meaning that
\[
\mathfrak{J}_r(\text{Teich}(x))^p = \exp(p\pi(\text{Teich}(x) - \text{Teich}(x)^q)) = 1
\]
as desired. \( \Box \)

Now, let \( X \) be the affine hypersurface defined by \( P(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n] \), and let \( N^*_s \) be the number of \( x \in \mathbb{F}_q^n \) with no component zero that satisfy \( P(x) = 0 \).

**Lemma 3.5.**
\[ (q^s - 1)^n + \sum_{(y,x) \in (\mathbb{F}_q^*)^n} \Theta_q(yP(x)) = q^s N^*_s. \] (3.6)

**Proof.** We first prove that
\[ \sum_{x \in \mathbb{F}_q} \Theta_q(x) = 0, \]
which follows from the fact that \( \Theta_q \) is a character and that there exists \( \alpha \in \mathbb{F}_q \) such that \( \Theta_q(\alpha) \neq 1 \):
\[
\sum_{x \in \mathbb{F}_q} \Theta(x) = \sum_{x \in \mathbb{F}_q} \Theta(x + \alpha) = \Theta_q(\alpha) \sum_{x \in \mathbb{F}_q} \Theta(x).
\]

Then
\[
\sum_{y \in \mathbb{F}_q} \Theta_q(yP(x)) = \begin{cases} 
q, & \text{if } P(x) = 0 \\
0, & \text{otherwise}
\end{cases}
\]
and
\[ \sum_{y \in \mathbb{F}_q} \Theta_q(yP(x)) = \begin{cases} q - 1, & \text{if } P(x) = 0 \\ -1, & \text{otherwise} \end{cases} \]
so that
\[ \sum_{(y,x) \in (\mathbb{F}_q^2)^{n+1}} \Theta_{q^x}(yP(x)) = (q^s - 1)N_s^* - ((q^s - 1)^n - N_s^*) = q^sN_s^* - (q^s - 1)^n. \]

We want to rewrite this lemma, which only uses the fact that \( \Theta_q \) is a character, in terms of \( p \)-adic power series. It is convenient to set \( y = x_0 \) and write \( W(x) = x_0 P(x_1, x_2, \ldots, x_n) \). For a multi-index monomial we write \( x^v = \prod_{i=0}^n x_i^{v_i} \). Let \( \Delta \) be the set by which the monomials of \( W(x) \) are indexed. We write \( W(x) = \sum_{v \in \Delta} w(x^v) \), and let
\[ W(X) = \sum_{v \in \Delta} \text{Teich}(w(x))X^v = \sum_{v \in \Delta} W_vX^v \]
be the \( p \)-adic lift of \( W(x) \). We define the following series:
\[ \mathcal{C}(X) = \exp(\pi(W(X) - W(X^q))). \]
This converges in a polydisk of the form \(|X_i|_p \leq 1 + \epsilon\) since
\[ \mathcal{C}(X) = \prod_{v \in \Delta} \exp(\pi(W_vX^v - W_vX^q)) = \prod_{v \in \Delta} \mathcal{J}_r(W_vX^v), \]
and \( \mathcal{J}_r(x) \) converges on a disk of radius bigger than 1 by (3.5). In particular they are both continuous functions at the Teichmüller representatives. By expanding the product we obtain the following identity:
\[ \mathcal{C}_s(X) := \prod_{n=1}^{s-1} \mathcal{C}(X^q^n) = \exp(\pi(W(X) - W(X^q))). \]
Using Lemma 3.4 we obtain that for \( x \in (\mathbb{F}_q^s)^{n+1} \)
\[ \Theta_{q^x}(W(x)) = \prod_{v \in \Delta} \Theta_{q^x}(w(x)^v) = \prod_{v \in \Delta} \mathcal{J}_{rs}(W_v\text{Teich}(x)^v) = \lim_{x \to \text{Teich}(x)} \prod_{v \in \Delta} \mathcal{J}_{rs}(W_vX^v) \]
\[ = \lim_{x \to \text{Teich}(x)} \prod_{v \in \Delta} \exp(\pi(W_vX^v - (W_vX^v)^qv)) = \lim_{x \to \text{Teich}(x)} \exp(\pi(W(X) - W(X^q))) \]
\[ = \lim_{x \to \text{Teich}(x)} \prod_{n=1}^{s-1} \mathcal{C}(X^q^n) = \prod_{n=1}^{s-1} \mathcal{C}(\text{Teich}(x)^q^n) = \mathcal{C}_s(\text{Teich}(x)), \]
where \( \text{Teich}(x) \) denotes the tuple \( (\text{Teich}(x_0), \ldots, \text{Teich}(x_n)) \). With this in mind we can rewrite (3.6) as
\[ q^sN_s^* = (q^s - 1)^n + \sum_{(x_i)^{q^s-1}=1} \mathcal{C}(x)\mathcal{C}(x^q)\ldots\mathcal{C}(x^{q^s-1}) = (q^s - 1)^n + \sum_{(x_i)^{q^s-1}=1} \mathcal{C}_s(x), \]
where the sum runs over all the Teichmüller representatives of \( \mathbb{F}_q^s \).
3.2 Operators on the ring of power series

Define \( \mathcal{H} \) as the \( \Omega \)-algebra of power series \( \Phi(X) = \sum_{v \in \mathbb{N}^{n+1}} \Phi_v X^v \) such that \( |\Phi_v|_p \to 0 \) as \( \deg(v) \) tends to \( \infty \). This is in some way the minimal set of restrictions we can impose on \( \mathcal{H} \), since we want to evaluate power series at the Teichmüller representatives. From Lemma 3.2 we know that every coefficient \( \lambda_i \) in \( J(x) \) (and hence in \( J_r(x) \)) satisfies \( \text{ord}_p(\lambda_i) \geq M \) for some \( M > 0 \). It follows that \( \mathcal{C}(X), \mathcal{C}_s(X), \) and \( \Psi_q \mathcal{C}(X) \) are in \( \mathcal{H} \), which is sufficient for our purposes. Elements \( \Phi(X) \in \mathcal{H} \) are also operators that act by multiplication. We define the linear operator \( \Psi_q \)

\[
\Psi_q(X^v) = \begin{cases} 
X^{v/q}, & \text{if } q \mid v \\
0, & \text{otherwise}
\end{cases}
\]

which extends to a map from \( \mathcal{H} \) to itself:

\[
\Psi_q \Phi(X) = \sum_v \Phi_{qv} X^v.
\]

The following identity is straightforward to prove

\[
\Psi_q \Phi(X) \Phi(X^q) \ldots \Phi(X^{q^{r-1}}) = (\Psi_q \Phi(X))^s. \tag{3.9}
\]

We will also make use of the infinite matrix of the operator \( \Psi_q \Phi(X) \) with respect to the basis \( \{X^v\} \), whose entries are \( (\Phi_{qu-v})_{u \geq v} \) (and 0 for \( u < v \)), since

\[
\Psi_q \Phi(X) X^v = \sum_{u \geq v} \Phi_{qu-v} X^u,
\]

where \( \Phi_w = 0 \) if \( w \notin \mathbb{N}^{n+1} \), and \( u \geq v \) means that every coordinate in \( u \) is greater or equal than the corresponding one in \( v \). For \( \Phi(X) \in \mathcal{H} \) we will consider the trace of the matrix of \( \Psi_q \Phi(X) \):

\[
\text{Tr}(\Psi_q \Phi(X)) = \sum_v \Phi_{(q-1)v}.
\]

It is well-defined because \( |\Phi_{(q-1)v}|_p \to 0 \) as \( \deg(v) \to \infty \). Next, we relate the sum in (3.8) to the trace of \( \Psi_q \mathcal{C}(X) \).

**Lemma 3.6.** Let \( \Phi(X) \in \mathcal{H} \). Then

\[
\sum_{(x_i)^{q-1}=1} \Phi(x) = (q - 1)^{n+1} \text{Tr}(\Psi_q \Phi(X))
\]

**Proof.** We use the result

\[
\sum_{x^{q-1}=1} x^v = \begin{cases} 
q - 1, & \text{if } q - 1 \text{ divides } v \\
0, & \text{otherwise}
\end{cases}
\]
This can be proven using that \( S = \{ x^v \mid x^q - 1 = 1 \} \) is a subgroup of the cyclic group of \((q - 1)\)-th roots of unity, and each root appears the same number of times in the sum. Then \( S \) is cyclic, i.e. it consists the roots of \( x^m - 1 \) for some \( m \), which sum to 0 unless \( m = 1 \). Hence,

\[
\sum_{(x,v)^{q-1}=1} x^v = \begin{cases} (q - 1)^{n+1}, & \text{if } q - 1 \text{ divides } v \\ 0, & \text{otherwise} \end{cases}
\]

Therefore,

\[
\sum_{(x,v)^{q-1}=1} \Phi(x) = (q - 1)^{n+1} \sum_v \Phi_{(q-1)v} = (q - 1)^{n+1} \text{Tr}(\Psi_q \Phi(X)).
\]

We want to apply the previous lemma to the power series \( \mathcal{C}_s(X) = \mathcal{C}(X) \mathcal{C}(x^q) \ldots \mathcal{C}(x^{q^{s-1}}) \). Using (3.9) we obtain

\[
\sum_{(x,v)^{q-1}=1} \mathcal{C}(x) \mathcal{C}(x^q) \ldots \mathcal{C}(x^{q^{s-1}}) = (q^s - 1)^{n+1} \text{Tr} \left( \Psi_q \mathcal{C}(x) \mathcal{C}(x^q) \ldots \mathcal{C}(x^{q^{s-1}}) \right)
\]

\[
= (q^s - 1)^{n+1} \text{Tr} \left( (\Psi_q \mathcal{C}^s) \right). \tag{3.10}
\]

We can write

\[
\mathbf{U} = \Psi_q \mathcal{C} = e^{-\pi W(X)} \Psi_q e^{\pi W(X)},
\]

this will be the key operator in Dwork’s theory. However, neither \( e^{\pm \pi W(X)} \) is in \( H \), so this decomposition is purely formal. Putting (3.8) and (3.10) together

\[
N_s^* = (q^s - 1)^n + (q^s - 1)^{n+1} \frac{1}{q^s} \text{Tr}(\mathbf{U}^s). \tag{3.11}
\]

We will use this formula to study a series closely related to the zeta function:

\[
Z^*(T) = \exp \left( \sum_{s=1}^{\infty} N_s^* \frac{T^s}{s} \right).
\]

For an infinite matrix \( A \) we define the determinant of \( I - AT \) as

\[
\det(I - AT) = \sum_{n=0}^{\infty} b_n T^n,
\]

where

\[
b_n = (-1)^n \sum_{1 \leq u_1 < \ldots < u_n} \text{sgn}(\sigma) a_{u_1 \sigma(u_1)} a_{u_2 \sigma(u_2)} \ldots a_{u_n \sigma(u_n)}.
\]

**Lemma 3.7.** Let \( \Phi(X) \in H \), and let \( A \) be the matrix of \( \Psi_q \Phi(X) \) with respect to the basis \( \{ X^v \} \). Then \( \det(I - AT) \) is well-defined and it is an entire power series. In particular \( \det(I - \mathbf{U}T) \) is entire.
We will prove it in Section 4 (see Theorem 4.7).

Lemma 3.8. For $A$ as in the previous discussion, we have

$$\exp \left( - \sum_{s=1}^{\infty} \text{Tr}(A^s) \frac{T^s}{s} \right) = \det(I - AT)$$

This will again be proven with the tools of Section 4 (see the comment below Theorem 4.12).

Therefore, by expanding the powers of $q^s$ in (3.11), and using the previous lemma, we get

$$Z^*(T) = \prod_{j=0}^{n} (1 - q^{-1}T)^{(-1)(n-j+1)} \prod_{k=0}^{n+1} \det(1 - q^{k-1}T)^{(-1)(n-k)} \frac{(n+1)^{k}}{k}, \quad (3.12)$$

and each determinant is an entire function in $\Omega[[T]]$. Being the quotient of two entire power series we say that $Z^*(T)$ is $p$-adic meromorphic. To end this section we relate $Z(T)$ and $Z^*(T)$.

Lemma 3.9. $Z(T)$ is also $p$-adic meromorphic.

Proof. We prove it by induction on the dimension $n$ of the ambient space. For $n = 0$ it’s easy since $X$ is empty or a point. Now suppose the hypothesis holds true for $0, 1, \ldots, n-1$. Note that

$$Z(T)/Z^*(T) = \exp \left( \sum_{s=1}^{\infty} (N_s - N^*_s) \frac{T^s}{s} \right)$$

is the zeta function of $\bigcup_{i=1}^{n} X_i$, where $X_i = X \cap \{x_i = 0\}$, which is a lower dimensional hypersurface. In Lemma 3.1 we showed how the zeta function of a union is the product of zeta functions (or their inverses) of all the possible intersections, which are also lower dimensional varieties. By hypothesis these zeta functions are meromorphic, and we have proved that $Z^*(T)$ is meromorphic. Thus $Z(T)$ is also meromorphic.

This concludes the hardest part of the proof of the rationality conjecture. Dwork [Dwo60] finished the proof using the $p$-adic Weirstrass preparation theorem together with some estimates on the norm of the coefficients of $Z(T)$, the argument can also be found in [Kob84, Ch.5, Sec.5]. We will instead prove the rationality conjecture for non-singular hypersurfaces, along with a much stronger result in Section 6.

4 p-adic Banach spaces

In the rest of the essay we will develop tools that allow us to compute zeta functions of non-singular hypersurfaces in practice, something that we will do in Section 7. In Section 5 we introduce a particular form of homology that we will use to prove an expression similar to (3.12) but where the determinants are finite-dimensional, which makes them amenable to computations. In Section
6 we prove some facts about the homology of non-singular hypersurfaces, incidentally proving the rationality conjecture for these hypersurfaces. Before we do that we need some theory about \( p \)-adic Banach spaces. Every result left unproven in this section can be found in [Mon70, Ch.6].

**Definition 4.1.** Let \( K \) be a complete extension of \( \mathbb{Q}_p \), and \( V \) a vector space over \( K \). Let \( || \cdot || \) be a norm on \( V \) satisfying

1. \( ||v + w|| \leq \max(||v||, ||w||) \).
2. \( ||\lambda v|| = |\lambda|_p ||v||, \lambda \in K \).
3. \( ||v|| = 0 \) iff \( v = 0 \).

If \( V \) is complete with the usual metric \( d(v, w) = ||v - w|| \) we say that \( V \) is a Banach space over \( K \).

A key example is the following. Let \( I \) be a set and let \( C(I) \) be the space of functions \( f : I \to K \) such that \( f(i) \to 0 \), that is, for all \( r > 0 \) there are only finitely many \( i \in I \) with \( |f(i)|_p \geq r \). Set \( ||f|| = \max_{i \in I} |f(i)|_p \), then \( C(I) \) becomes a Banach space with this norm. For each \( i \in I \) let \( e_i \in C(I) \) be defined by \( e_i(j) = \delta_{i,j} \). The \( e_i \) are said to be an orthonormal basis of \( C(I) \). We will say that a collection of vectors \( \{v_i\} \) in a Banach space \( V \) is an orthonormal basis if there is an isomorphism to some \( C(I) \) sending \( v_i \) to \( e_i \).

From now on let \( V \) be a Banach space admitting a countable orthonormal basis \( \{e_i\} \).

Let \( L(V, V) \) be the space of continuous linear maps \( T : V \to V \), and \( ||T|| = \sup_{v \neq 0} \frac{||T(v)||}{||v||} \). Let \( U \) be a neighbourhood of zero such that \( T(U) \subset \{||v|| \leq 1\} \), then there exists \( M > 0 \) such that \( T(\{||v|| \leq 1\}) \subset MT(U) \subset \{||v|| \leq M\} \). Since \( \frac{||T(v)||}{||v||} = ||T(v')|| \), where \( ||v'|| = 1 \), the norm is always a positive real number. It is easy to check that it is indeed a norm and that \( L(V, V) \) is complete.

We can give a description of \( L(V, V) \) in terms of matrices. Let \( M \) be space of matrices \( M = (a_{ij})_{i,j<\infty} \) with entries in \( K \) such that \( |a_{ij}|_p \) is bounded and its column vectors are in \( C(\mathbb{N}) \). Set \( ||M|| = \sup |a_{ij}|_p \). Then for \( T \in L(V, V) \) define \( M = (a_{ij}) \) by \( T(e_i) = \sum_{j=0} M_{ij} e_j \). The map \( T \mapsto M \) is then a Banach space isomorphism since

\[
||T|| = \sup_{(b_i) \neq 0} \frac{||\sum_{i=0}^\infty b_i T(e_i)||}{\max_i |b_i|_p} = \sup_{(b_i) \neq 0} \frac{\max_j (|b_i|_p \sum_i |a_{ij}|_p)}{\max_i |b_i|_p} \leq \max_i \frac{\sum |a_{ij}|_p}{|b_i|_p} \leq \max \frac{|a_{ij}|_p}{|b_i|_p},
\]

and

\[
\sup_{i>0} \frac{||T(e_i)||}{||e_i||} = \sup_{i>0} \left| \sum_j a_{ji} e_j \right| = \max_{i,j} |a_{ij}|_p,
\]

so that \( ||T|| = ||M|| \). From now on \( M = (a_{ij}) \) will denote the matrix of an operator with respect to an orthonormal basis.

**Definition 4.2.** Let \( C_{\text{fin}}(V, V) \) be the 2-sided ideal of \( L(V, V) \) consisting of maps with a finite dimensional image. Let \( C(V, V) \) be the closure of \( C_{\text{fin}}(V, V) \) in \( L(V, V) \). The operators in \( C(V, V) \) are called completely continuous.
Let $C^*(\mathbb{N})$ be the space of bounded sequences, with norm $\|(a_n)\| = \max |a_n|_p$, there is a convenient matrix description for operators in $C(V, V)$, which can be proven in a similar way to the $L(V, V)$ case.

**Lemma 4.3.** $T \in L(V, V)$ belongs to $C(V, V)$ if and only if its matrix $M$ with respect to the orthonormal basis $\{e_i\}$ has row vectors tending to 0 in the norm of $C^*(\mathbb{N})$.

Now suppose that $H \in C_{\text{fin}}(V, V)$, let $W$ be a finite dimensional subspace containing $\text{Im } H$, and let $H_0 = H|W$. Define $D_H(t) = \det(1 - tH_0) := 1 + \sum_{i>0} c_i(H) t^i$, which is easily seen to be independent of $W$.

**Lemma 4.4.** Suppose that $H, H' \in C_{\text{fin}}(V, V)$ have norm at most 1. Then for all $k$

$$|c_k(H) - c_k(H')| \leq ||H - H'||$$

Using this lemma and the fact that $c_k(\lambda H) = |\lambda|^k c_k(H)$ for $\lambda \in K$ we obtain

**Corollary 4.5.** The functions $c_k : C_{\text{fin}}(V, V) \to K$ are uniformly continuous on bounded subsets, and hence they extend uniquely to functions $c_k : C(V, V) \to K$.

**Definition 4.6.** For $H \in C(V, V)$, let $D_H(t)$ be the power series

$$D_H(t) = 1 + \sum_{k=1}^{\infty} c_k(H) t^k$$

This can be seen as a way to make sense of $\det(I - tH)$. We prove that $D_H(t)$ is an entire power series. Choose an orthonormal basis $\{e_i\}$, and by reordering the basis arrange the norm (in $C^*(\mathbb{N})$) of the row vectors of $M$ in decreasing size. We get a decreasing sequence of positive real numbers $(r_n)$ such that $r_n \to 0$.

**Theorem 4.7.** For $H \in C(V, V)$, $|c_k(H)| \leq r_1 r_2 \ldots r_k$. Thus $D_H(t)$ is entire.

**Proof.** Let $M^*_i$ be the upper left $i \times i$ submatrix of $M$, and let $M_i$ be the matrix obtained from $M$ by replacing every row vector except from the first $i$ ones by 0s; by Lemma 4.3 it converges to $M$. Let $T_i \in C_{\text{fin}}(V, V)$ be its corresponding operator, then $c_k(T_i)$ is the coefficient of $t^k$ in $\det(1 - tM^*_i)$. This coefficient is a sum of products, each of them with values in $k$ different rows of $M$; hence for $k \leq i$, $|c_k(T_i)| \leq r_1 r_2 \ldots r_k$. Clearly $T_i \to H$ in $L(V, V)$, so by definition $c_k(T_i) \to c_k(H)$, and we are done.

Before proceeding further we apply the theory to our case in question. Let $\mathcal{H}$ be as in Section 3.2, it is a $\Omega$-Banach space with orthonormal basis $\{X^v\}$. For some $\Phi(X) = \sum_v \Phi_v X^v \in \mathcal{H}$, let $H = \Psi_q \Phi$, its matrix with respect to the orthonormal basis is

$$M = (\Phi_{qu-v})_{u \geq v}.$$
The \( u \)-th row vector has norm at most
\[
\max_{v \leq u} |\Phi_{uv - v}|_p \to 0 \quad \text{as} \quad \deg(u) \to \infty.
\]

From Lemma 4.3 it follows that \( H \in C(V, V) \), and thus \( D_H(t) \) is entire. Note that the way in which we defined \( \det(1 - AT) \) in Section 3 is equivalent to the definition of \( D_H(t) \), so that Lemma 3.7 follows.

Define the ring \( E \) of entire power series in \( 1 + K[[t]] \), and let \( f \in K[[t]] \) be irreducible. For some \( g(t) \in 1 + tK[[t]] \) define \( \ord_f(g) \) as the maximum \( s \) such that \( f^s \) divides \( g \) in \( E \). This is well-defined, because by Theorem 2.5 \( g \) can only have finitely many roots of norm less than \( n \).

**Lemma 4.8.** [Mon70, Thm. 5.6] Let \( f(t) \in K[t] \) be irreducible, let \( g(t) \in E \) and let \( g = \prod p_i^{n_i} \) be the Weirstrass factorization of \( g \). Then \( \ord_f(g) > 0 \iff f = p_i \) for some \( i \), and in that case \( \ord_{p_i}(g) = n_i \).

If \( f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in K[t] \), define \( f^*(t) = t^n f(t^{-1}) = 1 + a_{n-1}t + \ldots + a_0 t^n \). It is irreducible if and only if \( f \) is irreducible, and its roots are the reciprocal of \( f \). The next theorem relates the roots of \( D_H(t) \) to the generalized eigenspaces of \( V \).

**Theorem 4.9.** Let \( H \in C(V, V) \) and \( f \neq t \) a monic irreducible polynomial over \( K \). Then:

1. \( V = N_f \oplus W_f \), where \( N_f \) and \( W_f \) are \( H \)-invariant subspaces, \( N_f \) is finite dimensional, \( f(H) \) is nilpotent on \( N_f \) and bijective on \( W_f \).
2. For any real \( r \) there are only finitely many \( f \) such that \( N_f \neq 0 \) and \( \lambda(f^*) < r \).
3. \( \dim N_f = \deg(f) \ord_f, D_H \).

Note that any decomposition as in (1) is unique, with \( N_f = \bigcup \ ker f(H)^s \) and \( W_f = \bigcap \ im f(H)^s \).

**Definition 4.10.** Let \( U \) be a vector space over \( K \), a linear map \( H: U \to U \) is said to be nuclear if it satisfies (1) and (2) of Theorem 4.9. If \( H \) is nuclear, define \( \Tr_{\text{nc}}(H) = \sum \Tr(H|N_f) \), where the sum ranges over all monic irreducible \( f \neq t \).

The sum above converges: let \( f = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \), by the structure theorem for finitely generated modules \( N_f \cong \bigoplus_i K[t]/f(t)^n \) as a \( K[t] \)-module. Hence \( N_f \) is the direct sum of \( H \)-cyclic subspaces \( W_i \). For each of them we have \( \Tr(H|W_i) = -a_{n-1} \dim W_i / \deg(f) \), by choosing a basis of the form \( \{ v, Hv, \ldots, H^{n-\deg(f)} v \} \). Summing over all these subspaces we obtain
\[
\Tr(H|N_f) = -\frac{\dim N_f}{\deg(f)} a_{n-1}.
\] (4.1)

Thus \( |\Tr(H|N_f)| \leq |a_{n-1}| \leq p^{-\lambda(f^*)} \), and \( \Tr(H|N_f) \to 0 \). Also, for a finite dimensional \( U \), the structure theorem for finitely generated modules shows that \( U = \bigoplus N_f \), where the sum ranges over the irreducible \( f \). It follows that \( \Tr_{\text{nc}}(H) = \Tr(H) \), since \( \Tr(H|N_i) = 0 \). Next, we relate the notion of trace from Section 3.2 to \( \Tr_{\text{nc}} \).
**Theorem 4.11.** Let \( H \in C(V,V) \), with matrix \( M = (a_{ij}) \) with respect to the basis \( \{e_i\} \). Then \( H \) is nuclear and \( \text{Tr}_{\text{nuc}}(H) = -c_1(H) = \sum_{i=1} a_{ii} = \text{Tr} M \).

**Proof.** By Theorem 4.9 and Lemma 4.8 \( H \) is nuclear and \( D_H(t) \) has Weirstrass factorization \( \prod (f^{*})^{\dim N_f} \frac{\text{deg}(f)}{\deg(f)} f^{*} \). Thus the coefficient \( c_1(H) \) of \( t \) in \( D_H(t) \) is \( \sum_{i=1} \text{dim} N_f \deg(f) c_1(f^{*}) \), where \( c_1(f^{*}) \) is the coefficient of \( t \) in \( f^{*} \), and the sum ranges over the irreducibles not equal to \( t \). It follows from (4.1) that this is \( -\text{Tr}_{\text{nuc}}(H) \). Finally, we can prove \( -c_1(H) = \sum a_{ii} \) by approximating \( H \) by a sequence in \( C_{\text{fin}}(V,V) \), as in Theorem 4.7. \( \square \)

We finish the section with a theorem that proves Lemma 3.8.

**Theorem 4.12.** Let \( H \in C(V,V) \), then

\[
f(t) := \exp \left( -\sum_{s=1}^{\infty} \text{Tr}_{\text{nuc}}(H^s) \frac{t^s}{s} \right) = D_H(t).
\]

**Proof.** Let \( M_n^s \) be the upper left \( n \times n \) submatrix of \( M = (a_{ij}) \) and let \( M_n \in C_{\text{fin}}(V,V) \) be the matrix obtained from \( M \) by replacing all row vectors except the first \( n \) by 0s. Define

\[
f_n(t) = \exp \left( -\sum_{s=1}^{\infty} \text{Tr}(M_n^s) \frac{t^s}{s} \right) = \exp \left( -\sum_{s=1}^{\infty} \text{Tr}((M_n^s)^s) \frac{t^s}{s} \right),
\]

we claim that \( f_n(t) \to f(t) \). Let \( \lambda_n = \max_{i>n} |a_{ij}|_p \), then \( |\text{Tr}(M^s) - \text{Tr}(M_n^s)|_p \leq \lambda_n^s \), and \( \lambda_n \to 0 \). Let

\[
g_n(t) = \frac{f_n(t)}{f(t)} = \exp \left( -\sum_{s=1}^{\infty} \left( \text{Tr}(M_n^s) - \text{Tr}(M^s) \right) \frac{t^s}{s} \right) = \sum_{s=0}^{\infty} b_s t^s,
\]

for sufficiently big \( r > 0 \) we have

\[
|b_s|_p \leq \frac{\lambda_n^s}{|s|!}_p \leq (r\lambda_n)^s.
\]

Let \( f(t) = \sum a_s t^s \), and \( f_n(t) = \sum c_{n,s} t^s \). Then for some fixed \( s \)

\[
|c_{n,s} - a_s|_p = \sum_{i=1}^{s} b_i a_{s-i} \leq \max_{1 \leq i \leq s} (r\lambda_n)^i |a_{s-i}|_p \to 0 \text{ as } n \to \infty
\]
as desired. Since \( \det(1 - M_n t) \to D_H(t) \) by definition, it is enough to prove the statement when the matrices are finite dimensional, which is a standard result [Kob84, p.121]. \( \square \)

This, together with the fact that for \( \Phi(X) \in \mathcal{H} \), \( H = \Psi q \Phi \) is a completely continuous operator on \( \mathcal{H} \) proves Lemma 3.8.
5 An analytical approach to homology

We now construct Dwork’s cohomology theory for projective hypersurfaces [Dwo62] following Monsky’s approach [Mon70]. We will present the theory in terms of homology, but this is just an isomorphic dual to the more commonly used cohomology. Let $F/\mathbb{Q}_p$ be the unramified extension of degree $r$, and let $\pi$ be a root of $x^{p-1} + p = 0$, which is irreducible over $F$ since every root has order $1/(p-1)$. Let $K = F(\pi)$, then $[K : \mathbb{Q}_p] = (p-1)r$. We claim that the index of ramification of $K$ is $p-1$. Given $\alpha = \sum_{i=0}^{p-2} f_i \pi^i \in K$, for $0 \leq i < j \leq p-2$,

$$\text{ord}_p(f_i \pi^i) \in \frac{i}{p-1} + \mathbb{Z} \implies \text{ord}_p(f_i \pi^i) \neq \text{ord}_p(f_j \pi^j),$$

so that

$$\text{ord}_p(\alpha) = \min_{0 \leq i \leq p-2} \text{ord}_p(f_i \pi^i) \in \frac{1}{p-1}\mathbb{Z}.$$ 

Thus, by Lemma 2.2 the residue field of $K$ is $\mathbb{F}_q$. We will also use that $K$, and in fact every finite extension of $\mathbb{Q}_p$ is complete [Neu99, Ch.2, Prop 4.9]. Let $f(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ be a homogeneous polynomial of degree $d$, defining the hypersurface $X = \{x \in \mathbb{P}^{n-1}_q : f(x) = 0\}$. Let $W(x) = x_0 f(x)$, as before $W(X) \in K[x_0, x_1, \ldots, x_n]$ denotes the Teichmüller lifting of $W(x)$.

We now introduce a similar space to $\mathcal{H}$ (see Section 3.2), it will have stricter convergence constraints, which will result in a better behaved homology. For a positive integer $\gamma$, let $L(\gamma)$ be the $K$-Banach space with orthonormal basis $\pi^{[\gamma v_0]} X^v$, where the indices $v$ satisfy $d v_0 = \sum_{i=1}^{n} v_i$; this is because monomials in $U$ are of this form. Elements $\Phi \in L(\gamma)$ are of the form

$$\Phi(X) = \sum_{v} a_v \pi^{[\gamma v_0]} X^v, \quad a_v \to 0. \quad (5.1)$$

**Lemma 5.1.** $\mathcal{C}(X) \in L(\gamma)$ for $\gamma < \frac{(p-1)^2}{pq}$.

**Proof.** Recall (3.7)

$$\mathcal{C}(X) = \prod_{v \in \Delta} \mathcal{J}_r(W_v X^v), \quad (5.2)$$

and

$$\mathcal{J}_r(x) = \prod_{i=0}^{r-1} \mathcal{J}(x^{p^i}),$$

where $\mathcal{J}(x) = \sum_{i=0}^{\infty} \lambda_i x^i$. We know by Lemma 3.2 that

$$\text{ord}_p(\lambda_i) \geq \frac{p-1}{p^2 i},$$

so that if $\mathcal{J}(x^{p^i}) = \sum_{i=0}^{\infty} \lambda'_i x^i$,

$$\text{ord}_p(\lambda'_i) \geq \frac{p-1}{p^{2+i}}.$$
This means that the coefficients $b_i$ of $\mathfrak{J}_r(x)$ satisfy
\[ \text{ord}_p(b_i) \geq \frac{p-1}{pq} i. \]

Then
\[ \mathfrak{J}_r(W_v X^\gamma) = \sum_{n=0}^{\infty} b_n W_v^n X^{n\gamma} = \sum_{n=0}^{\infty} c_v X^\gamma, \]
with
\[ \text{ord}_p(c_v) \geq \frac{p-1}{pq} \quad v_0 = \text{ord}_p\left(\frac{(p-1)^2}{pq} v_0\right), \]
due to the way $W(x)$ was defined. From (5.2), we deduce that the coefficients of $\mathfrak{C}(X)$ satisfy the same inequality, and the lemma follows.

**Theorem 5.2.** For $0 < \gamma < \frac{(p-1)^2}{p}$, $L(\gamma)$ is stable under $\mathfrak{U}$, and $\mathfrak{U} \in C(L(\gamma), L(\gamma))$. If $M$ is the matrix of $\mathfrak{U}$ with respect to the basis $\{X^s\}$, then for all $s$
\[ \text{Tr}_{\text{nuc}}(\mathfrak{U}^s|L(\gamma)) = \text{Tr} M^s. \]

**Proof.** By Lemma 5.1, $\mathfrak{C} \in L(\gamma/q)$. Now, $L(\gamma/q)$ is closed under multiplication, and $\Psi_q$ maps $L(\gamma/q)$ into $L(\gamma)$. Therefore we have
\[ L(\gamma) \hookrightarrow L(\gamma/q) \xrightarrow{\psi_q} L(\gamma/q) \xrightarrow{\phi_q} L(\gamma), \]
so that $L(\gamma)$ is stable under $\mathfrak{U}$. The inclusion $L(\gamma) \hookrightarrow L(\gamma/q)$ is represented by a diagonal matrix with entries tending to 0, so it is the limit of continuous maps with finite dimensional images. Since $\mathfrak{C}$ and $\Psi_q$ are also continuous it follows that $\mathfrak{U}$ is completely continuous. Now, let $M = (\Phi_\mathfrak{U},v)$, so that $\mathfrak{U}(X^\gamma) = \sum_u \Phi_\mathfrak{U},v X^u$. It is easy to see that $\Phi_\mathfrak{U},v \neq 0$ only if $dv_0 = \sum v_i$. Let $(a_\mathfrak{U},v)$ be the matrix of $\mathfrak{U}$ with respect to the orthogonal basis $\{Y^\gamma = \pi^{[\gamma v_0]} X^\gamma\}$, then $a_\mathfrak{U},v = \pi^{[\gamma v_0] - [\gamma q_0]} \Phi_\mathfrak{U},v$. In particular $a_\mathfrak{U},v = \Phi_\mathfrak{U},v$. Hence, by Theorem 4.11, $\text{Tr}_{\text{nuc}}(H|L(\gamma)) = \sum a_\mathfrak{U},v = \sum \Phi_\mathfrak{U},v = \text{Tr} M$.

Replacing $\mathfrak{C}$ by $\mathfrak{C}_s$ we can prove the analogue of Lemma 5.1 for $\mathfrak{C}_s(X)$. Using the fact that $\mathfrak{U}^s = \Psi_q^s \mathfrak{C}_s(X)$ completes the proof.

Crucially, for $p \neq 2, 1 < \frac{(p-1)^2}{p}$ so that we can work in $L = L(1)$, and by Theorem 4.9 $\mathfrak{U}$ is nuclear on $L$. From now on we assume that $p \neq 2$. Combining this theorem and (3.11) we get that if $X^\gamma$ is the affine variety defined by $f(x_1, x_2, \ldots, x_m) = 0$ and $\prod x_i \neq 0$, then
\[ q^s N_s(X^\gamma) = (q^s - 1)^n + (q^s - 1)^{n+1} \text{Tr}_{\text{nuc}}(\mathfrak{U}^s|L). \quad (5.3) \]

We will decompose $X$ into affine ”patches”, and use them to transform (5.3) into a formula for $N_s = N_s(X)$. For this we will make use of some special subspaces of $L$.
Definition 5.3. If \( v \) is a \((n+1)\)-tuple with \( dv_0 = \sum_{i=1}^{n} v_i \), let \( Y^v = \pi^v X^v \). For \( A \subseteq \{1,2,\ldots,n\} \), let \( L_A \) be the closed subspace of \( L \) having as orthonormal basis the \( Y^v \) such that \( v_i > 0 \) for all \( i \in A \). Similarly, \( L_A^* \) has as orthonormal basis the \( Y^v \) such that \( v_i > 0 \) for some \( i \in A \). Let \( \mathcal{A} = \{1,2,\ldots,n\} \setminus A \), \( a = |A| \), and \( \pi = |\mathcal{A}| \).

For \( A \subseteq \{1,2,\ldots,n\} \) let \( X_A^* \) the affine variety defined by \( f(x_1,x_2,\ldots,x_n) = 0 \), \( x_i = 0 \) for \( i \in A \) and \( x_i \neq 0 \) for \( i \in \mathcal{A} \).

Lemma 5.4.

\[
q^s N_s(X_A^*) = (q^s - 1)^{\pi} + (q^s - 1)^{\pi+1} \text{Tr}_{\text{nuc}}(\mathfrak{U}|L/L^A).
\]

Proof. Let \( f_A(x) \) be the polynomial obtained from \( f \) by replacing \( x_i \) by 0 whenever \( i \in A \). Then \( X_A^* \) can be thought as the affine variety defined by \( f_A(x) = 0 \) and \( \prod_{i \in \mathcal{A}} X_i \neq 0 \). We want to apply Theorem 5.2 with \( f \) replaced by \( f_A \), and \( n \) replaced by \( \pi \). Define \( W(A) \), \( \mathfrak{C}(A) \), \( \mathfrak{U}(A) \) and \( L(A) \) using \( f_A \) in the same way they were defined for \( f \). Then \( \mathfrak{U}(A) \) is obtained from \( \mathfrak{U} \) by replacing the \( X_i \), \( i \in A \) with 0, and \( L(A) \) is spanned by the \( Y^v \) with \( v_i = 0 \) \( \forall i \in A \), i.e. \( L(A) \cong L/L^A \). With this identification \( \mathfrak{U} \) induces \( \mathfrak{U}(A) \) on \( L(A) \), and Theorem 5.2 gives the desired result. For \( A = \{1,2,\ldots,n\} \) this argument fails, but in this case the lemma reduces to \( q^s = 1 + (q^s - 1) \).

The (disjoint) union of the \( X_A^* \) is the affine hypersurface \( \{f(x) = 0\} \). Therefore \( (q^s - 1)N_s(X) = -1 + \sum_A N_s(X_A^*) \). Using the identity [Mon70, Lemma 7.2]

\[
\text{Tr}_{\text{nuc}}(\mathfrak{U}|L/L^B) = \sum_{A \subseteq B} (-1)^{|A|} \text{Tr}_{\text{nuc}}(\mathfrak{U}|L_A)
\]

along with the previous lemma, we obtain

\[
N_s = \frac{q^{s(n-1)} - 1}{q^s - 1} + \frac{(-1)^n}{q^s} \sum_{A} (-1)^{|A|} q^{s\pi} \text{Tr}_{\text{nuc}}(\mathfrak{U}|L_A).
\]

We now start constructing our homology, which is very much analytical in nature. Let \( K^n \) have basis \( \{\xi_1,\xi_2,\ldots,\xi_n\} \), then \( B = L \otimes_K \wedge K^n \) has the structure of a graded Banach space over \( K \): \( B = \bigoplus_{k=0}^{n} B_k \), where

\[
B_k = \left\{ \sum \Phi_\beta(X) \otimes_K \xi_{\beta_1} \wedge \cdots \wedge \xi_{\beta_k} : \Phi_\beta \in L \right\}.
\]

Its elements are called \( k \)-forms, from now on we omit the \( \otimes_K \) and \( \wedge \) symbols. Then \( \mathfrak{U} \) is an operator on \( B \) via its action on \( L \). Let \( \mathfrak{L} \) be the closed subspace of \( B \)

\[
\sum L_{\{\beta_1,\ldots,\beta_s\}} \xi_{\beta_1} \cdots \xi_{\beta_s},
\]

where the sum extends over subsets \( \{\beta_1,\ldots,\beta_s\} \) of \( \{1,2,\ldots,n\} \). The graded subspaces \( \mathfrak{L}_k \) of \( B_k \) are defined as expected. Since each \( L_A \) is stable under \( \mathfrak{U} \), so is \( \mathfrak{L} \). Define a map of graded Banach spaces \( \alpha : \mathfrak{L} \rightarrow \mathfrak{L} \) by \( \alpha_i = q^i \mathfrak{U} \). Note that \( \mathfrak{L}_i \cong \bigoplus_{n=1}^{i} L_A \) as \( K \)-vector spaces, so that using (5.4) we obtain
Theorem 5.5. \( \alpha_i \) is nuclear on \( \mathfrak{L}_i \) and

\[
N_s = q^{(n-1)s} - 1 + \frac{(-1)^n}{q^s} \sum_{j=0}^{n} (-1)^j \text{Tr}_{\text{nuc}}(\alpha_j^s).
\]

This justifies the slightly odd indexing of \( \mathfrak{L} \). We now define a differential operator that will make \( \mathfrak{L} \) into a chain complex.

Definition 5.6. For \( 1 \leq i \leq n \), \( \mathfrak{D}_i \) is the operator \( e^{-\pi W(X)} D_i e^{\pi W(X)} \) on \( K[[X_0, X_1, \ldots, X_n]] \), where \( D_i = X_i \frac{\partial}{\partial X_i} \).

The \( \mathfrak{D}_i \) commute with each other because the partial derivatives of \( D_i \) do. For \( \Phi \in K[[X_0, \ldots, X_n]] \), \( \mathfrak{D}_i(\Phi) = D_i \Phi + \pi(D_i W(X)) \Phi \), so that \( L \) is stable under \( \mathfrak{D}_i \). We also have the relation

\[
\mathcal{M} \mathfrak{D}_i = q \mathcal{D}_i \mathcal{M}.
\] (5.5)

After using that \( \mathcal{M} = e^{-\pi W(X)} \Psi q e^{\pi W(X)} \) it reduces to \( \Psi D_i = q D_i \Psi q \), which is easily proven on the basis elements \( Y^v \). Define \( \mathfrak{D} : B_k \to B_{k-1} \) as

\[
\mathfrak{D} \Phi(X) \xi_{\beta_1} \xi_{\beta_2} \ldots \xi_{\beta_k} = \sum_{j=1}^{k} (-1)^{j+1} \mathfrak{D}_j(\Phi(X)) \xi_{\beta_1} \ldots \hat{\xi}_{\beta_j} \ldots \xi_{\beta_k},
\]

where \( \hat{\xi}_{\beta_j} \) means that the symbol is omitted. We recall the concept of chain homology: let \( U_i, i = 0, 1, \ldots, n \) be \( K \)-vector spaces and let \( \partial_i : U_i \to U_{i-1} \) be linear maps

\[
0 \to \partial_{n+1} U_n \to \partial_n U_{n-1} \to \partial_{n-1} U_{n-2} \to \ldots \to \partial_1 U_0 \to \partial_0 U_0 \to 0.
\]

Such a chain is called a chain complex \( (U_\bullet) \) if \( \partial_i \circ \partial_{i+1} = 0 \) for \( i = 0, 1, \ldots, n-1 \). Then we can form the homology groups \( (K \)-vector spaces\) \( H_i(U) = \ker \partial_i / \text{Im} \partial_{i+1} \), for \( i = 0, 1, \ldots, n \). A chain map \( f : (U_\bullet) \to (V_\bullet) \) consists of maps \( f_i : U_i \to V_i \) such that the following diagram commutes

\[
0 \to \partial_{n+1} U_n \to \partial_n U_{n-1} \to \partial_{n-1} U_{n-2} \to \ldots \to \partial_1 U_0 \to \partial_0 U_0 \to 0
\]

\[
0 \to \partial'_{n+1} V_n \to \partial'_{n-1} V_{n-1} \to \partial'_{n-2} V_{n-2} \to \ldots \to \partial'_1 V_0 \to \partial'_0 V_0 \to 0
\]

A chain map induces a map in homology

\[
(f_i)_* : H_i(U) \to H_i(V)
\]

\[
u_i + \text{Im} \partial_{i+1} \longleftrightarrow f_i(u_i) + \text{Im} \partial'_{i+1}.
\]

Using the fact that the \( D_i \) commute we see that \( \mathfrak{D}^2 = 0 \), so we have made \( B \) into a chain complex. From (5.5) it follows that \( \alpha : B \to B \) is a chain map, which is a vital feature for any useful homology in this setting. Since \( \mathfrak{D}_i(\Phi) = D_i \Phi + \pi(D_i W(X)) \Phi \) we find that \( \mathfrak{D}_i \) maps \( L_{\mathfrak{D}_i[1]} \) to \( L_{\mathfrak{D}_i} \), so that \( \mathfrak{L}_\bullet \) is a subcomplex of \( B \), and \( \alpha \) is a chain map \( \mathfrak{L}_\bullet \to \mathfrak{L}_\bullet \). We now prove a lemma that will allow us to obtain the equivalent of Theorem 5.5 in homology.
Lemma 5.7. Let $U_n \to U_{n-1} \to \ldots \to U_0$ be a chain complex of $K$-vector spaces, and $f : U_\bullet \to U_\bullet$ be a chain map such that each $f_i$ is nuclear. Then each $(f_i)_*$ is nuclear and

$$\sum_{j=0}^{n} (-1)^j \text{Tr}_{\text{nuc}}(f_j) = \sum_{j=0}^{n} (-1)^j \text{Tr}_{\text{nuc}}(f_j)_*.$$ 

Proof. Let $p \neq t$ irreducible in $K[t]$. For each $i$, $U_i = N_p(U_i) \oplus W_p(U_i)$. Now, $\partial_i$ maps $N_p(U_i)$ to $N_p(U_{i-1})$, for if $u_i \in N_p(U_i)$, then $p^n u_i = 0$ for all $n$. Then $\partial_i p(f_i)^n u_i = (f_i)^n \partial_i u_i = 0$, using that $f$ is a chain map. Similarly $\partial_i$ maps $W_p(U_i)$ to $W_p(U_{i-1})$. Therefore

$$H_i(U) = \ker \partial_i / \text{Im} \partial_{i+1} \cong H_i(N_p(U_i)) \oplus H_i(W_p(U_i)),$$

and both summands are $(f_i)_*$ invariant, since $N_p(U_i)$ and $W_p(U_i)$ are $f_i$ invariant. Similarly $p(f_i)_*$ is nilpotent in $H_i(N_p(U_i))$, and surjective on $H_i(W_p(U_i))$. It is also injective, since for $v \in W_p(U_i)$ such that $p(f_i)v \in \text{Im} \partial_{i+1}W_p(U_{i+1})$, one has

$$p(f_i)v = \partial_{i+1}p(f_i+1)^n u = p(f_i)\partial_{i+1}(p(f_i+1)^n u),$$

where we can assume that $v \in W_p(U_{i+1})$, as any contribution from $N_p(U_{i+1})$ is killed by $p(f_i+1)^n$. Since $p(f_i)$ is bijective on $W_p(U_i)$

$$v = \partial_{i+1}(p(f_i+1)^n u) \in \partial_{i+1}W_p(U_{i+1}).$$

The dimension of $H_i(N_p(U_i))$ is at most the dimension of $N_p(U_i)$ so that the former is finite and condition (2) in the definition of nuclearity is clearly satisfied. Thus the $(f_i)_*$ are nuclear. Using (4.1), proving

$$\sum_{j=0}^{n} (-1)^j \text{Tr}((f_j)_*|H_j(N_p(U_j))) = \sum_{j=0}^{n} (-1)^j \text{Tr}(f_j|N_p(U_j))$$

(and hence the rest of the lemma) reduces to proving

$$\sum_{j=0}^{n} (-1)^j \dim N_p(U_j) = \sum_{j=0}^{n} (-1)^j \dim H_j(N_p(U_j)).$$

But

$$\dim H_j(N_p(U_j)) = \dim \ker \partial_j|N_p(U_j) - \dim \text{Im} \partial_{j+1}N_p(U_{j+1}) = \dim \ker \partial_j|N_p(U_j) - \dim N_p(U_{j+1}) - \dim \ker \partial_{j+1}|N_p(U_j),$$

and the lemma follows. \qed

Combining this lemma with Theorem 5.5 yields

Theorem 5.8. $\alpha : \mathfrak{L}_\bullet \to \mathfrak{L}_\bullet$ is a chain map and

$$N_s(X) = \frac{q^{(n-1)s} - 1}{q^s - 1} + \frac{(-1)^n}{q^s} \sum_{j=0}^{n} (-1)^j \text{Tr}_{\text{nuc}}(\alpha_j)_*.$$
Plugging this expression into $Z(T)$, and using Lemma 3.8 in the finite-dimensional case gives

**Corollary 5.9.** Suppose that each of the $H_i(\mathfrak{L}_*)$ is finite dimensional. Then

$$Z(T) = \prod_{j=0}^{n-2} \frac{1}{1 - q^j T} \prod_{j=0}^{n} \det \left( 1 - \frac{(\alpha_j)_* T}{q} \right)^{(-1)^{n+j+1}}.$$ 

One might think of applying Theorem 4.12 to the formula of Theorem 5.8, relaxing the assumption of finite dimensionality, but there is no a priori orthonormal basis for $H_i(\mathfrak{L}_*)$. Also note that we would have an analogous expression replacing $L$ by the weaker $\mathcal{H}$. The reason for this refinement is that for a non-singular hypersurface, $H_i(\mathfrak{L}_*) = 0$ for $i > 0$, and $H_0(\mathfrak{L}_*)$ is finite dimensional. We prove this in the next section.

### 6 Non-singular hypersurfaces. A link between analytical and algebraic homology

We introduce the concept of a Koszul complex, appropriately simplified for our purposes.

**Definition 6.1.** Let $R$ be a ring and $N$ a $R$-module. Let $\phi_i : R \to R$, $i = 1, 2, \ldots, n$ be commuting endomorphisms of $R$. We can form a complex denoted $K_\bullet(N; \phi_1, \ldots, \phi_n)$ having $B = N \otimes_R \wedge R^n$ as the base graded space, and defining

$$\partial_i : B_i \to B_{i-1}$$

$$a\xi_{\beta_1} \cdots \xi_{\beta_i} \mapsto \sum_{j=1}^{i} (-1)^{j+1} \phi_j(a) \xi_{\beta_1} \cdots \hat{\xi}_{\beta_j} \cdots \xi_{\beta_i},$$

where $\hat{\xi}_i$ means that the symbol is omitted. The homology groups are denoted $H_i(N; \phi_1, \ldots, \phi_n)$.

We see that $\mathfrak{L}_*$ is a subcomplex of $K_\bullet(L; \mathfrak{D}_1, \ldots, \mathfrak{D}_n)$. Now, we say that a sequence $\phi_1, \phi_2, \ldots, \phi_n$ of commuting endomorphisms of $R$ is regular if

$$\phi_s : R/\sum_{1}^{s-1} \phi_i(R) \to R/\sum_{1}^{s-1} \phi_i(R)$$

is injective for $s = 1, 2, \ldots, n$. For $r_1, r_2, \ldots, r_n$ in a commutative $R$, we say that the sequence is regular if the associated endomorphisms via acting by multiplication are regular. We will use a well-known theorem about Koszul complexes [Pro, Lemma 15.29.2].

**Theorem 6.2.** If $\phi_1, \phi_2, \ldots, \phi_n$ is a regular sequence on $R$, then $H_i(R; \phi_1, \ldots, \phi_n) = 0$ for $i \geq 1$. 

25
We now build an algebraic version of the complex defined in the previous section. When the number of variables is clear we write $k[x_1, \ldots, x_n] = k[X]$. For $f \in k[x_1, \ldots, x_n]$ homogeneous of degree $d$, let

$$
\Delta_i : k[X] \to k[X]
$$

$$
\varphi \mapsto \varphi_i + f \varphi,
$$

where $\varphi_i = \frac{\partial \varphi}{\partial x_i}$. Again, the $\Delta_i$ commute, so we can form $K_\bullet(k[X]; \Delta_1, \ldots, \Delta_n) := K_\bullet(k[X])$. Let $k[X]^{(j)}$ be the subspace of $k[X]$ spanned by monomials $x^v$ with $\deg(v) = j \mod d$. Then $\Delta_i$ maps $k[X]^{(j)}$ to $k[X]^{(j-1)}$. Thus we can write

$$
K_\bullet(k[X]) = \bigoplus_{i=1}^d K_i,
$$

where

$$
K_i = \sum_{0 \leq s \leq n} k[X]^{(s-n+i)} \xi_{\beta_1} \cdots \xi_{\beta_s}.
$$

Define $\mathfrak{L}(f)$ as $K_0$, which is a subcomplex of $K_\bullet(k[X])$. Let $H_i(f)$ denote its homology groups, and $\partial_i$ the boundary maps.

We can use this complex to give an alternative description of $\mathfrak{L}_\bullet$. Let $K$ as in the beginning of Section 5. Let $F \in \mathcal{O}_K[X_1, X_2, \ldots, X_n]$ be the lift of $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, a homogeneous polynomial of degree $d$. We can construct $K[X]$, $K[X]^{(j)}$, and $\mathfrak{L}_i(F)$ as before. They all have structure of normed space over $K$ with

$$
\| \sum c_v X^v \| = \max |c_v|_p.
$$

Let $M$, $M^{(j)}$, and $\widehat{\mathfrak{L}}_i(F)$ be the completions of the previous spaces. $M$ can be embedded in $K[[X_1, \ldots, X_n]]$, in fact its not hard to see that

$$
M = \left\{ \sum a_v X^v : a_v \to 0 \text{ as } \deg(v) \to \infty \right\}.
$$

Now, the maps $\Delta_i : K[X] \to K[X]$ are continuous and extend to linear operators on $M$, similarly the boundary maps extend to $\widehat{\mathfrak{L}}_i(F)$, so that it becomes a complex of Banach spaces. Let $\widehat{\partial}_i$, $\widehat{H}_i(F)$ be its $i$th boundary map and homology group respectively. It is easy to see that $\widehat{\partial}_i$ is a contraction, that is, $\|\widehat{\partial}_i \omega\| \leq \|\omega\|$.

**Lemma 6.3.** $\mathfrak{L}_\bullet \cong \widehat{\mathfrak{L}}(F)$ as complex Banach spaces.

**Proof.** From the characterization of $M$ (6.2), it follows that for $A = \{\beta_1, \ldots, \beta_s\} \subseteq \{1, 2, \ldots, n\}$, there are Banach space isomorphisms $M^{(s-n)} \cong L_{\mathcal{A}}$ given by

$$
X^v \mapsto (\pi X_0)^j \left( \prod_{i \in \mathcal{A}} X_i \right) X^v,
$$

where
where \( j = \frac{\deg(v) + n - s}{d} \). They extend to maps \( f_i : \mathfrak{L}_i \to \tilde{\mathfrak{L}}_i(F) \). We can easily check that

\[
\begin{array}{ccc}
M^{(s-n)} & \xrightarrow{\cong} & L_{\{\beta_1, \ldots, \beta_s\}} \\
\downarrow \Delta_{s} & & \downarrow \Delta_{s} \\
M^{(s-1-n)} & \xrightarrow{\cong} & L_{\{\beta_1, \ldots, \beta_{s-1}\}}
\end{array}
\]

commutes, thus the \( f_i \) form a chain map.

This lemma is one of the motivations for the use of the ring \( L \) in the definition of \( \mathfrak{L} \), as we can check that the factor of \( \pi^j \) cannot be removed from the isomorphisms, and Theorem 6.6 will show that \( \tilde{\mathfrak{L}}(F) \) is the right complex to consider. We say that a homogeneous \( f \in k[x_1, \ldots, x_n] \) is non-singular if the only common zero of the partial derivatives \( f_i \) and \( f \) is the origin. For the rest of the section we work with \( f \) non-singular. We need some algebraic results to proceed.

**Lemma 6.4.** For \( f \in k[x_1, \ldots, x_n] \) homogeneous of degree \( d > 0 \), and non-singular; \( f_1, f_2, \ldots, f_n \) is a regular sequence on \( k[x_1, \ldots, x_n] \).

The proof can be found in [Mon70, Lemma 8.3], together with a property of Cohen-Macaulay rings [Mat86, Thm 17.4].

**Theorem 6.5.** With \( f \) as in Lemma 6.4,

1. \( H_1(k[X]; \Delta_1, \ldots, \Delta_s) = 0 \) for \( 1 \leq s \leq n \).
2. \( H_i(f) = 0 \) for \( i > 0 \).

**Proof.** For (1) we need to show that for \( \phi_i \in k[X] \) satisfying \( \sum_{i=1}^s \Delta_i(\phi_i) = 0 \), there is a skew-symmetric matrix \( (a_{ij})_{1 \leq i,j \leq s} \) such that

\[
\phi_i = \sum_{j=1}^s \Delta_j(a_{ij}).
\]

We prove it by induction on \( n = \max \deg(\phi_i) \). Let \( p_i \) be the \( n \)-th degree component of \( \phi_i \). Then \( \sum_{i=1}^s f_i p_i = 0 \). By Lemma 6.4 and Theorem 6.2, \( H_1(k[X]; f_1, \ldots, f_s) = 0 \), so that there exists a skew-symmetric matrix \( (b_{ij}) \) such that

\[
p_i = \sum_{j=1}^s f_j b_{ij},
\]

and we can choose \( b_{ij} \) to be homogeneous of degree \( n - d + 1 \). Now,

\[
\sum_{i=1}^s \Delta_i \left( \phi_i - \sum_{j=1}^s \Delta_j(b_{ij}) \right) = 0,
\]
and each \( \phi_i - \sum_{j=1}^s \Delta_j(b_{ij}) \) has degree less than \( n \), so that we are done by induction hypothesis. A moment of thought reveals that (1) implies that \( \Delta_1, \ldots, \Delta_n \) is a regular sequence, so that \( H_i(k[X]; \Delta_1, \ldots, \Delta_n) = 0 \) for \( i > 0 \). Since \( H_i(f) \) is a direct summand of this space by (6.1), we are done.

Now we relate the algebraic and analytic homology. Let \( C \) be the subcomplex of \( \tilde{\mathcal{L}}(F) \) built from \( \mathcal{O}_K[X] \) instead of \( K[X] \), that is, the unit ball in \( \tilde{\mathcal{L}}(F) \). We have seen that the coefficients in \( \tilde{\mathcal{L}} \) are power series \( \sum a_v X^v \) with \( a_v \to 0 \). If we consider the reduction mod \( \pi, C = \mathcal{O}_K/\pi \mathcal{O}_K \), all but finitely many coefficients vanish, and we are left with the complex \( \mathcal{L}(f) \) over \( k = \mathcal{O}_K/\pi \mathcal{O}_K \cong F_q \), since \( F \) reduces to \( f \) mod \( \pi \) and both are constructed using the operators \( \Delta_i \).

**Theorem 6.6.**

1. For any \( i \), \( H_i(C) = 0 \) implies \( H_i(C) = 0 \).

2. If \( H_0(C) \) has dimension \( l < \infty \) over \( \mathcal{O}_K/\pi \mathcal{O}_K \cong F_q \), then \( H_0(C) \) is a free \( \mathcal{O}_K \)-module of rank \( l \).

*Proof.* The map \( \pi: C \to C \) is injective, so that we have the exact sequence of complexes

\[
0 \to C \xrightarrow{\pi} C \to \overline{C} \to 0,
\]

which induces an exact sequence in homology, meaning that

\[
H_i(\overline{C}) \cong H_i(C)/\pi H_i(C).
\] (6.3)

If \( H_i(\overline{C}) = 0 \), then \( H_i(C) = \pi H_i(C) \). This means that every monomial \( X^v \) vanishes in homology, since \( \partial_{i+1} \) is a contraction. We can sum all these monomials in homology, which implies that \( H_i(C) = 0 \). To prove (2), we claim that \( H_0(C) \) is finitely generated over \( \mathcal{O}_K \). Since \( H_0(\overline{C}) \) is finitely generated as a \( \mathcal{O}_K \)-module, let \( H_0(C)/\pi H_0(C) = \langle \Phi_1, \ldots, \Phi_n \rangle_{\mathcal{O}_K} \). We can write any \( \Phi \in H_0(C) \) as

\[
\Phi = \sum_{i=1}^n a_i \Phi_i + \pi \Phi' = \sum_{i=1}^n (a_i + \pi b_i) \Phi_i + \pi^2 \Phi'' = \sum_{i=1}^n \left( \sum_{m=0}^{\infty} a_{i,m} \pi^m \right) \Phi_i \in \langle \Phi_1, \ldots, \Phi_n \rangle_{\mathcal{O}_K},
\]

since \( \mathcal{O}_K \) is complete. Note that \( H_0(C) \) has no \( \mathcal{O}_K \)-torsion, because \( \pi: H_0(C) \to H_0(C) \) is injective, and every nonzero \( a \in \mathcal{O}_K \) can be expressed as \( a = u \pi^n \), where \( u \) is a unit. Thus, since \( \mathcal{O}_K \) is a principal ideal domain, \( H_0(C) \) and \( \pi H_0(C) \) are free \( \mathcal{O}_K \)-modules, and the rank formula follows from (6.3). □

From Theorem 6.5 it follows that \( H_i(\overline{C}) = 0 \) for \( i > 0 \). We deduce that \( H_i(\mathcal{L}_\bullet) \cong \hat{H}_i(F) = 0 \) for \( i > 0 \). Finally, we deal with the dimension of \( H_0(f) \). For a graded \( k[X] \)-module \( N \), the Hilbert power series is defined as \( P_N(t) = \sum_{i=0}^\infty (\dim_k N_i) t^i \), where \( N_i \) is the homogeneous part of \( N \) of degree \( i \).
Lemma 6.7 ([Mon70], Lemma 8.4). For $f$ as in Lemma 6.4, $M = k[X]/(f_1, f_2, \ldots, f_n)$ is finite dimensional over $k$. If $P_M(t) = \sum c_j t^j$, then

$$\sum_{j=\frac{-(n \mod d)}{d}} c_j t^j = \frac{1}{d}((d - 1)^n + (-1)^n(d - 1)).$$

Theorem 6.8. Let $f \in k[X]$ be homogeneous of degree $d > 0$, and non-singular. Then

$$\dim H_0(f) = d^{-1}((d - 1)^n + (-1)^n(d - 1)).$$

Proof. By the previous lemma

$$\dim_k \left( k[X]^{(-n)}/\sum f_i k[X]^{(1-n)} \right) = d^{-1}((d - 1)^n + (-1)^n(d - 1)).$$

Let $U$ be a homogeneous subspace of $k[X]$ such that

$$U \oplus \sum f_i k[X]^{(1-n)} = k[X]^{(-n)}, \quad (6.4)$$

it will suffice to prove that the projection

$$\varphi: U \to k[X]^{(-n)}/\sum \Delta_i k[X]^{(1-n)} = H_0(f)$$

is bijective. Let $u \in U$ such that $u = \sum \Delta_i \phi_i$ for $\phi_i \in k[X]^{(1-n)}$, we will show by induction on $n = \max \deg(\phi_i)$ that $u = 0$. Let $p_i$ be the $n$-th degree component of $\phi_i$. Then $\sum f_i p_i$ is the $(n - 1 + d)$-th degree component of $u$, so it must be 0, since it lies inside

$$U \cap \sum f_i k[X]^{(1-n)} = 0.$$

Now we are in the same setting as in the proof of Theorem 6.5, which shows that $p_i = \sum f_i b_{ij}$ for $(b_{ij})$ homogeneous of degree $n + 1 - d$ and skew-symmetric. Thus

$$u = \sum \Delta_i (\phi_i - \sum \Delta_j(b_{ij})),
\text{where each } \phi_i - \sum \Delta_j(b_{ij}) \text{ has degree less than } n,$$

and we are done by induction hypothesis. To prove surjectivity, by (6.4) it is enough to show that for each $\phi \in \sum_{i=1}^n f_i k[X]^{(1-n)}$, there exists $\varphi \in \sum_{i=1}^n \Delta_i k[X]^{(1-n)}$ such that $\phi + \varphi \in U$. Let $\phi = \sum_{i=1}^n f_i g_i$, then

$$\phi - \sum_{i=1}^n \Delta_i g_i = \sum_{i=1}^n \frac{\partial g_i}{\partial x_i}$$

is a polynomial of degree less than $\phi$ (without loss of generality), and thus we are done by induction on the degree of $\phi$. \qed

Using Theorem 6.6 we find that $H_0(C)$ is a free $O_K$-module of rank $\dim H_0(f)$. Then any free generating set for $H_0(C)$ is a basis for $\hat{H}_0(F)$: they are clearly independent since $K$ is the field of fractions of $O_K$, and there cannot be a larger set of $K$-independent elements, for after appropriate rescaling they would form a $O_K$-free set in $H_0(C)$. Therefore, by Lemma 6.3,

$$\dim H_0(C) = d^{-1}((d - 1)^n + (-1)^n(d - 1)).$$

Putting this together with Corollary 5.9 yields

29
Corollary 6.9. For \( f \in \mathbb{F}_q[x_1, \ldots, x_n] \) homogeneous of degree \( d > 0 \) and non-singular, let \( Z(T) \) be the zeta function of \( \{ x \in \mathbb{F}^{n-1} : f(x) = 0 \} \). Then \( Z(T) \in \mathbb{Q}(T) \) and

\[
Z(T) = \frac{P(T)^{(-1)^{n+1}}}{(1 - T)(1 - qT) \ldots (1 - q^{n-2}T)},
\]

where

\[
P(T) = \det_{H_0(\mathfrak{L}_*)} \left( 1 - \frac{(\mathfrak{U})_i T}{q} \right).
\]

Proof. Suppose \( n \) is odd. Since the determinant is finitely dimensional we have

\[
Z(T) \prod_{j=0}^{n-2} (1 - q^jT) = \det_{H_0(\mathfrak{L}_*)} \left( 1 - \frac{(\mathfrak{U})_i T}{q} \right) \in \mathbb{Q}[T] \cap \mathcal{O}_K[T] = \mathbb{Q}[T].
\]

The proof for \( n \) even is similar. \( \square \)

7 Deformation theory and Dwork’s family for \( d = 4 \)

7.1 Diagonal forms

Let \( f(x) = \sum_{i=1}^{n} a_i x_i^d \in \mathbb{F}_q[x_1, x_2, \ldots, x_n] \) for \( p > 2 \) and \( p \nmid d \) (so that the hypersurface is non-singular), and let \( A_i = \text{Teich}(a_i) \). We proceed to find a basis for \( H_0(\mathfrak{L}_*) \), \( H_0 \) for short. For \( \Phi(X) \in L_{\{i\}} \), \( \mathcal{D}_i \Phi(X) = 0 \) in \( H_0 \). That is, in \( H_0 \)

\[
-\pi D_i W(X) \Phi = -d A_i \pi X_0 X_i^d \Phi = D_i \Phi.
\]

Therefore, given \( Y^v \in L_{\{1,2,\ldots,n\}} \) (recall Definition 5.3),

\[
Y^v = \lambda Y^u, \text{ where } u_i \in \{1, 2, \ldots, d\} \text{ and } |\lambda|_p \leq 1.
\]

Out of the possible combinations for \( Y^u \), the ones having some \( u_i = d \) vanish in \( H_0 \), using (7.1). We claim that

\[
S = \{ Y^v : 0 < v_i < d \}
\]

is a basis for \( H_0 \). A combinatorial argument shows that \( |S| = d^{-1}((d-1)^n + (-1)^n(d-1)) \), so it is enough to prove that it generates \( L_{\{1,2,\ldots,n\}} \). For an arbitrary power series \( \Phi \in L_{\{1,2,\ldots,n\}} \), each term \( Y^v \) satisfies

\[
Y^v = \lambda_{u,v} Y^u + \mathfrak{D} \left( \sum_{i=1}^{n} \phi_{v,i} \xi_i \right),
\]

where \( \phi_{v,i} \in \mathcal{O}_K[X], \lambda_{u,v} \in \mathcal{O}_K, \) and \( Y^u \in S \). This allows us to sum all the terms of \( \Phi \) in homology

\[
\Phi = \sum_{u \in S} \left( \sum_{v} b_v \lambda_{u,v} \right) Y^u + \mathfrak{D} \left( \sum_{i=1}^{n} \left( \sum_{v} b_v \phi_{v,i} \right) \xi_i \right),
\]

30
and hence $S$ is a basis for $H_0$. We will sometimes write $(v_1, v_2, \ldots, v_n)$ for $Y^V$. To illustrate the computation of $\mathfrak{U}$ for a diagonal form let

$$f(x) = a_1 x_1^3 + a_2 x_2^3 + a_3 x_2^3 \in \mathbb{F}_q[x_1, x_2, x_3]$$

with $q = 2 \mod 3$.

$$\mathfrak{U} = \Psi_q \exp(\pi(W(X) - W(X^q))) = \Psi_q \left( \mathfrak{J}_r(A_1 X_0 X_1^3) \mathfrak{J}_r(A_2 X_0 X_2^3) \mathfrak{J}_r(A_3 X_0 X_3^3) \right).$$

If $\mathfrak{J}_r(x) = \sum c_i \pi^{n_i} x^{n_i}$, then

$$\mathfrak{U}(1,1,1) = \Psi_q \sum_{n_i} \left( \prod_{i=1}^{3} c_{n_i} \right) \pi^{1 + \sum n_i} X_0^{1 + \sum n_i} \prod_{i=1}^{3} A_i^{n_i} X_i^{3n_i+1}.$$  

The terms that survive $\Psi_q$ satisfy $3n_i + 1 = 0 \mod q$, that is, $n_i = a + k_i q$, where $a = \frac{2q-1}{3}$. Also, $\pi^n = (-p)^{\frac{q-1}{3}} \pi := (-p)^N \pi$. Then

$$\mathfrak{U}(1,1,1) = p^{2N} \sum_{i=1}^{3} \left( \prod_{k_i=0}^{\infty} c_{a+k_i q} (-p)^{Nk_i} (A_i \pi X_0 X_i^3)^{k_i} \right) (2,2,2),$$

similarly

$$\mathfrak{U}(2,2,2) = (-p)^N \prod_{i=1}^{3} \left( \sum_{k_i=0}^{\infty} c_{b+k_i q} (-p)^{Nk_i} (A_i \pi X_0 X_i^3)^{k_i} \right) (1,1,1),$$

where $b = \frac{q-2}{3}$. Now, for $\Phi(X) \in L_{(1,2,3)}$ we have the following identity in $H_0$:

$$(-A_i \pi X_0 X_i^3)^n \Phi = \frac{D_i}{3} (-A_i \pi X_0 X_i^3)^{n-1} \Phi = (-A_i \pi X_0 X_i^3)^{n-1} \left( \frac{D_i}{3} + (n-1) \right) \Phi = \left( \frac{D_i}{3} \right)_n \Phi,$$

where $(k)_n = k(k+1) \ldots (k+n-1)$ is the Pochhammer symbol. In fact,

$$(-A_i \pi X_0 X_i^3)^n \Phi = \left( \frac{D_i}{3} \right)_n \Phi + \mathfrak{D}(\Phi \xi_i).$$

(7.4)

We prove that each of

$$\sum_{k_i=0}^{\infty} c_{a+k_i q} (-p)^{Nk_i} (A_i \pi X_0 X_i^3)^{k_i}$$

is in $L$, which will allow us to substitute the previous identity into (7.3). We know that $\mathfrak{J}_r(x) = \mathfrak{J}(x) \mathfrak{J}(x^p) \ldots \mathfrak{J}(x^{p^{r-1}})$, so that by Lemma 3.2 $\text{ord}_p(c_n) \geq \left( \frac{q-1}{p^r} - \frac{1}{p-1} \right) n$. Thus

$$\text{ord}_p(c_{a+k_i q} (-p)^{Nk_i}) \geq \frac{qp^2 - 2qp + q - p}{p^2(p-1)} k_i + a',$$

for some constant $a'$. This tends to infinity for $p > 2$. Therefore, using (7.4),

$$\sum_{k_i=0}^{\infty} c_{a+k_i q} (-p)^{Nk_i} (A_i \pi X_0 X_i^3)^{k_i} \Phi = \sum_{k_i=0}^{\infty} c_{a+k_i q} \left( \frac{D_i}{3} \right)^{k_i} \Phi,$$

31
where \( \Phi \in L_{\{1,2,3\}} \). We can apply this identity (from left to right) to (7.3) to obtain

\[
\Omega(1,1,1) = p^{2N} \prod_{i=1}^{3} \left( \sum_{k_i=0}^{\infty} \sum_{k} c_{a+kq}(-p)^{Nk}(-1)^k \left( \frac{D_i}{3} \right)^k \right) (2,2,2) = \\
p^{2N} \left( \sum_{k=0}^{\infty} c_{a+kq}(-p)^{Nk}(-1)^k \left( \frac{2}{3} \right)^k \right)^3 (2,2,2),
\]

and

\[
\Omega(2,2,2) = (-p)^{N} \left( \sum_{k=0}^{\infty} c_{b+kq}(-p)^{Nk}(-1)^k \left( \frac{1}{3} \right)^k \right)^3 (1,1,1). \tag{7.5}
\]

We deduce that

\[
Z(T) = \frac{1 + \alpha T^2}{(1 - T)(1 - qT)},
\]

for some \( \alpha \in \mathbb{Q} \). It is not hard to see how this generalizes to arbitrary diagonal forms \( (p \nmid d \text{ and } p > 2) \), where we will have relations analogous to (7.5), with appropriate changes to the values \( a \) and \( b \). We will freely use these expressions in the rest of the section.

### 7.2 Adding non-diagonal terms

We have seen that our method handles diagonal forms particularly well. We now wish to study the one parameter family \( f(x) = \sum_{i=1}^{n} x_i^d + \lambda h(x) \in \mathbb{F}_p[x_1, \ldots, x_n] \), where \( h(x) \) has no diagonal terms. We will focus on the example

\[
f(x) = x_1^4 + x_2^4 + x_3^4 + x_4^4 - 4\lambda x_1 x_2 x_3 x_4
\]

over \( \mathbb{F}_p \), for \( p = 1 \mod 4 \). This is a particular case of the Dwork family, defined by

\[
f(x) = \sum_{i=1}^{d} x_i^d - d\lambda \prod_{i=1}^{d} x_i,
\]

which has been extensively studied, first by Dwork [Dwo69] and Katz [Kat72] among others, and more recently Candelas et al [CdR00] [Cd07] studied the case \( d = 5 \), which made the subject widely known to the string theory community. The rest of the essay is an exposition of the \( d = 4 \) case using the methods developed here, which are nonetheless similar to Dwork’s. The general theory from this subsection can be found in [Lau04a] and [Lau04b]. Let \( \pi W(X) = \pi X_0 F(X) = \sum_{i=1}^{4} \pi X_0 X_i^4 + \lambda Q \), where \( Q = -4\pi X_0 X_1 X_2 X_3 X_4 \). To make the dependence on \( \lambda \) explicit, write

\[
\Omega_i(\lambda) = e^{-\pi W} D_i e^{\pi W} = e^{-\lambda Q} \Omega_i(0) e^{\lambda Q},
\]

and

\[
\Omega(\lambda) = e^{-\pi W} \Psi e^{\pi W} = e^{-\lambda Q} \Omega(0) e^{\lambda Q}. \tag{7.6}
\]
Here we have used $\lambda$ to denote $\text{Teich}(\lambda)$, so that $\lambda^p = \lambda$. The problem is that then the $e^{\pm \lambda Q}$ are not in $L$, so we cannot naively assume that $\det(I - \mathfrak{U}(\lambda)T/p) = \det(I - \mathfrak{U}(0)T/p)$. The idea is to consider $\lambda$ as a free variable, and work with carefully defined subspaces [Lau04a, Def.22] $L_\lambda$ of $K[[X, \lambda]]$, where elements

$$\sum_{j=0}^{\infty} a_j(X)\lambda^j$$

satisfy convergence conditions on the $a_j(X)$ that allow for a small enough $\alpha$ to be substituted for $\lambda$. From now on to avoid confusion we will use $\lambda$ for the free variable, $\Gamma \in \mathbb{F}_p$ for the parameter in $f(x)$ and $\mu = \text{Teich}(\Gamma)$. Then $L_\lambda$ becomes a module over the power series in $K[[\lambda]]$ that converge in a disk around the origin, and we can consider the quotient module

$$H_{0,\lambda} = L_\lambda^0 / \sum_{i=1}^{n} \mathfrak{D}_i(\lambda)L_\lambda^i,$$

where $L_\lambda^0$ means that all monomials in each $a_j(X)$ are divisible by $X_0 \ldots X_n$, and in $L_\lambda^i$ all of them are divisible by $X_0 \ldots X_{i-1}X_{i+1} \ldots X_n$. This is constructed in the same way as $H_0(\mathfrak{L}_*)$, so one would expect to recover useful information about the latter. Lauder [Lau04a, Prop.24] proved that the same $S$ as before (7.2) is a free generating set for the quotient module $H_{0,\lambda}$. He also proves [Lau04a, Lemma 29] that if $C(\lambda)$ is the matrix of

$$e^{\lambda Q} : H_{0,\lambda} \to H_0$$

$$\Phi(X, \lambda) + \mathfrak{D}(\lambda)\Psi(X, \lambda) \mapsto e^{\lambda Q}\Phi + \mathfrak{D}(0)e^{\lambda Q}\Psi$$

with respect to $S$, then the the matrix of $\mathfrak{U}(\lambda)$ with respect to the same basis is

$$\mathfrak{U}(\lambda) = C(\lambda^p)^{-1}\mathfrak{U}(0)C(\lambda).$$

The intuition behind this fact is that the following diagram commutes, owing to (7.6).

$$\begin{array}{ccc}
H_{0,\lambda} & \xrightarrow{\mathfrak{U}(\lambda)} & H_{0,p} \\
\downarrow e^{\lambda Q} & & \downarrow e^{\lambda Q} \\
H_0 & \xrightarrow{\mathfrak{U}(0)} & H_0
\end{array}$$

The entries of $\mathfrak{U}(\lambda)$ are power series in $\lambda$ which may not converge at the Teichmüller representatives. However, Lauder shows how these power series can be "analytically continued" in the form

$$\Phi(\lambda) + \sum_{n=1}^{\infty} \frac{\Phi_n(\lambda)}{f(\lambda)^n},$$

where $f(x) \in \mathcal{O}_K[x]$, the $\Phi_n$ are polynomials where each coefficient has order greater than $rn$ for some $r > 0$, and $\Phi(\lambda)$ converges on a disk of radius greater than 1. This way we can substitute for values of norm one $\alpha$ such that $|f(\alpha)|_p = 1$. He then goes on to show that substituting $\mu = \text{Teich}(\Gamma)$ for sufficiently general $\Gamma$ on $\mathfrak{U}(\lambda)$ gives the original matrix $\mathfrak{U}$ constructed from $f(x)$. 

33
The matrix $C(\lambda)$ has size $4^{-1}(3^4 + 3) = 21$, so we will break it into smaller blocks. For $Y^\nu \in S$, 
\[
e^{\lambda Q}Y^\nu = \sum_{n=0}^{\infty} \frac{\lambda^n Q^n}{n!}Y^\nu = \sum_{j=0}^{3} \sum_{n=0}^{\infty} \frac{\lambda^{4n+j}Q^{4n+j}}{(4n+j)!}Y^\nu,
\]
and by (7.4) 
\[
Q^{4n}\Phi = \prod_{i=1}^{4} (-4\pi X_0 X_i^4)^n \Phi = \prod_{i=1}^{4} 4^n \left( \frac{D_i}{4} \right)^n \Phi.
\]
Hence $e^{\lambda Q}Y^\nu$ lies in the span of $\{Q^jY^\nu : j = 0, 1, 2, 3\}$. Recall that if $v_i = 4$ for some $i$, then $Y^\nu = 0$ in $H_0$. Therefore we can divide $H_{0,\lambda}$ into the following $C(\lambda)$-invariant subspaces:

1. $S_1 = \langle (1, 1, 1, 1), (2, 2, 2, 2), (3, 3, 3, 3) \rangle$
2. $S_2 = \langle (1, 1, 3, 3), (3, 3, 1, 1) \rangle$
3. $S_3 = \langle (1, 3, 3, 1), (3, 1, 3, 1) \rangle$
4. $S_4 = \langle (1, 3, 1, 3), (3, 1, 3, 1) \rangle$

The other basis elements are permutations of $(1, 2, 3, 3)$, and all of them are eigenvectors of $C(\lambda)$. Let $S_5$ be generated by these permutations, and let $C_i(\lambda), U_i(\lambda)$ be the matrices of $C(\lambda)|S_i$, $\U(\lambda)|S_i$ respectively.

We now give the matrix of $\U(0)$, which is computed as in the previous subsection. In our case $\U(0)$ is diagonal, and 
\[
\U(0)Y^\nu = (-p)^{v_0} \prod_{i=1}^{4} \left( \sum_{k=0}^{\infty} c_{a_i + kp}p^k \left( \frac{v_i}{4} \right)_k \right) Y^\nu,
\]
where $a_i = \frac{p-1}{4}v_i$, and $\mathfrak{J}(x) = \exp(\pi(x - x^p)) = \sum c_n x^nx^n$. The following identity is due to Roberts [Rob01, Thm.2] 
\[
\Gamma_p(pz - a) = \sum_{k=0}^{\infty} c_{a+kp}p^k(z)_k \quad \text{for } 0 \leq a \leq p - 1 \text{ and } z \in \mathbb{Z}_p,
\]
where $\Gamma_p$ is the $p$-adic gamma function. Then 
\[
\U(0)Y^\nu = (-p)^{v_0} \prod_{i=1}^{4} \Gamma_p \left( \frac{v_i}{4} - a_i \right) Y^\nu = (-p)^{v_0} \prod_{i=1}^{4} \Gamma_p \left( \frac{v_i}{4} \right) Y^\nu.
\]
We will use the following identities (for $p = 1 \mod 4$) in what follows [Rob00, p.369-374].

1. $\Gamma_p(1/2)^2 = -1$.
2. $\Gamma_p(1/4)^2 \Gamma_p(3/4)^2 = 1$.
3. $\Gamma_p(1/4) \Gamma_p(3/4) \Gamma_p(1/2)^2 = (-1)^{\frac{p-1}{2}}$.

34
7.3 The deformation matrix

We now introduce a more systematic way to study how the zeta function changes along $\Gamma$. Let $B(\lambda)$ be the matrix with entries $b_{u,v}$, where $Y^v, Y^u \in S$ such that

$$QY^v = \sum_{u \in S} b_{u,v} Y^u \text{ in } H_{0,\lambda}.$$ 

It is known [Lau04b, Section A.3] that $C(\lambda)$ is in fact the unique solution around the origin to the Picard-Fuchs differential equation

$$\frac{\partial C}{\partial \lambda} = C(\lambda)B(\lambda), \quad C(\lambda) \equiv I \mod \lambda.$$ 

Using that $D_i(\lambda) = D_i + 4\pi x^i - \lambda Q$ we will see that $B(\lambda)$ has the same block form as $C(\lambda)$:

$$\begin{align*}
(1 - \lambda^4)Q(1, 2, 2, 3) &= 2\lambda^3(1, 2, 2, 3) + D_1(\lambda) \left( \frac{\lambda^2}{4}(0, 1, 1, 2) - \lambda^3(1, 2, 2, 3) \right) \\
+ D_2(-\lambda(3, 0, 4, 1)) + D_3(\lambda)(\lambda^2(4, 1, 1, 2)) - D_4(\lambda)(2, 3, 3, 0),
\end{align*}$$

and there are similar identities for the other permutations of $(1, 2, 2, 3)$, thus there is a $12 \times 12$ block $C_5 = c(\lambda)I$, where

$$\frac{\partial c}{\partial \lambda} = 2\lambda^3 \frac{1}{1 - \lambda^4} c(\lambda), \quad c(0) = 1.$$ 

This gives $c(\lambda) = (1 - \lambda^4)^{-1/2}$, recall that this is the formal power series

$$\quad(1 - \lambda^4)^{-1/2} = \sum_{n=0}^{\infty} (-\lambda^4)^n \left( \frac{-1/2}{n} \right),$$

which does not converge for $|\alpha|_p = 1$. It follows that $U(\lambda)$ has a $12 \times 12$ block

$$\begin{align*}
U_5(\lambda) &= p^2h(\lambda^4) \frac{1 - \lambda^{4p}}{1 - \lambda^4} \Gamma_p(1/4) \Gamma_p(1/2)^2 \Gamma_p(3/4) I = (-1)^{p-1} p^2 h(\lambda^4) \frac{1 - \lambda^{4p}}{1 - \lambda^4} I,
\end{align*}$$

where

$$h(x) = \left( \frac{1 - x}{1 - x^p} \right)^{1/2}.$$ 

Let

$$v(x) = \frac{(1 - x)^p}{1 - x^p} = 1 + pw(x) \in 1 + p\mathbb{Z}_p[x, 1/1 - x^p],$$

we can write

$$h(x) = \left( \frac{1}{1 - x} \right) \frac{v(x)^{p-1}}{x^{1/2}},$$

where $v(x)^{1/2}$ is defined by the binomial expansion. Then $v(x)^{1/2} = \sum b_n x^{n-1} / (1 - x)^n$, where $b_n$ is a a polynomial with $\text{ord}_p(b_n) \geq n$. This means that $v(x)^{1/2}$ has an analytic continuation, and that we can evaluate $v(x)^{1/2}$ at $\mu = \text{Teich}(\Gamma)$ satisfying $\Gamma^{4p} = \Gamma^4 \neq 1$, since this implies that $|1 - \mu^{4p}| = 1.$

35
For this choice of $\Gamma$, $h(\mu^4) = \frac{1 - \mu^4}{1 - \mu^4} = 1$, so that $h(\mu^4) = \pm 1$. The sign is determined by $(1 - \mu^4)^{\frac{p - 1}{2}}$, since $v(\mu^4)^{1/2} = 1 \mod p$. We can express this in terms of Legendre’s symbol for quadratic residues:

$$h(\mu^4) = \left(\frac{1 - \Gamma^4}{p}\right).$$

It follows that

$$U_5(\mu) = (-1)^{\frac{p - 1}{4}}\left(\frac{1 - \Gamma^4}{p}\right)p^2I.$$  

This gives a factor of $(1 \pm pT)^{12}$ in $P(T)$.

For the three $2 \times 2$ blocks we obtain

$$(1 - \lambda^3)Q(1, 1, 3, 3) = \lambda^3(1, 1, 3, 3) + \lambda(3, 3, 1, 1) - O_1(\lambda)(\lambda^3(1, 1, 3, 3))$$

$$- O_2(\lambda)(\lambda^2(4, 0, 2, 2)) - O_3(\lambda)(\lambda(3, 3, 1, 1)) - O_4(\lambda)(2, 2, 4, 0),$$

so that for $i = 2, 3, 4$, $C_i$ satisfies

$$\frac{\partial C_i}{\partial \lambda} = \frac{1}{1 - \lambda^3}C_i(\lambda)\begin{pmatrix} \lambda^3 & \lambda \\ \lambda & \lambda^3 \end{pmatrix}.$$  

This can be solved algebraically to obtain

$$C_i(\lambda) = \frac{1}{2}(1 - \lambda^2)^{-\frac{3}{2}}I + \frac{1}{2}(1 + \lambda^2)^{-\frac{3}{2}}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$  

Its inverse is

$$C_i(\lambda)^{-1} = \frac{(1 - \lambda^4)^{1/2}}{2}\begin{pmatrix} (1 - \lambda^2)^{-1/2} + (1 + \lambda^2)^{-1/2} & -(1 - \lambda^2)^{-1/2} + (1 + \lambda^2)^{-1/2} \\ -(1 - \lambda^2)^{-1/2} + (1 + \lambda^2)^{-1/2} & (1 - \lambda^2)^{-1/2} + (1 + \lambda^2)^{-1/2} \end{pmatrix},$$

so that

$$C_i(\lambda)^{-1}C_i(\lambda) = \frac{1}{2}\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{11} \end{pmatrix},$$

where

$$a_{11} = \frac{1 + \lambda^{2p}}{1 + \lambda^2}h(-\lambda^2) + \frac{1 - \lambda^{2p}}{1 - \lambda^2}h(\lambda^2),$$

and

$$a_{12} = -\frac{1 + \lambda^{2p}}{1 + \lambda^2}h(-\lambda^2) + \frac{1 - \lambda^{2p}}{1 - \lambda^2}h(\lambda^2).$$

Using that $\Gamma_p(1/4)^2\Gamma_p(3/4)^2 = 1$, it follows that for $\Gamma^4 \neq 1$

$$U_i(\mu) = \frac{p^2}{2}\begin{pmatrix} h(\mu^2) + h(-\mu^2) & h(\mu^2) - h(-\mu^2) \\ h(\mu^2) - h(-\mu^2) & h(\mu^2) + h(-\mu^2) \end{pmatrix}.$$  

Since $h(\pm \mu^2) = \left(\frac{1 \pm \Gamma^2}{p}\right) = \pm 1$ we can check that the corresponding factor in $P(T)$ is $(1 - pT)^2$, $(1 + pT)^2$, or $(1 - pT)(1 + pT)$. Hence the first 18 reciprocal roots of $P(T)$ are all $\pm p$, and their
exact value can be made explicit in terms of Legendre’s symbols depending on $\Gamma$. Furthermore, using the functional equation arising from the other Weil conjectures [Kob84, p.114] we see that if $\omega$ is a reciprocal root of $P(T)$ so is $p^2/\omega$, so that one of the remaining 3 reciprocal roots is also $\pm p$.

For $S_1$

$$(1 - \lambda^4)Q(3, 3, 3, 3) = \frac{\lambda}{16}(1, 1, 1, 1) - \frac{7}{4}\lambda^2(2, 2, 2, 2) + 6\lambda^3(3, 3, 3, 3) + \sum_{i=1}^{4} D_i(\lambda)(A_i),$$

where

$$A_1 = -\frac{\lambda}{64}(1, 1, 1, 1) + \frac{3\lambda^2}{16}(2, 2, 2, 2) - \frac{\lambda^3}{4}(3, 3, 3, 3) + \frac{\lambda}{16}(1, 5, 1, 1) - \frac{\lambda}{4}(1, 5, 5, 1) - \frac{1}{4}(0, 4, 4, 4) - \frac{\lambda^2}{4}(2, 6, 2, 2),$$

and the expressions for $A_2, A_3, A_4$ are similar. Thus $C_1$ satisfies

$$\frac{\partial C_1}{\partial \lambda} = C_1 \begin{pmatrix} 0 & 0 & \frac{\lambda}{16}(1 - \lambda^4) \\ -4 & 0 & -7\lambda^2/4(1 - \lambda^4) \\ 0 & -4 & 6\lambda^3/(1 - \lambda^4) \end{pmatrix}.$$ 

Let $(f_1, f_2, f_3)$ be a row of $C_1$, then $f_1$ satisfies the differential equation

$$(1 - \lambda^4)\frac{d^3 f_1}{d\lambda^3} = \lambda f_1 + 7\lambda^2 \frac{df_1}{d\lambda} + 6\lambda^3 \frac{d^2 f_1}{d\lambda^2},$$

and the determinant of $C_1$ is (up to a factor) a Wronskian, so it can be computed to be

$$\det C_1(\lambda) = \frac{-1}{4^3(1 - \lambda^4)^{3/2}}.$$ 

Thus

$$\det \frac{1}{p} U_1(\lambda) = p^3 \left( \frac{1 - \lambda^{4p}}{1 - \lambda^4} h(\lambda^4) \right)^3 \Gamma_p(1/4)^4 \Gamma_p(1/2)^4 \Gamma_p(3/4)^4,$$

and for $\Gamma^4 \neq 1$

$$\det \frac{1}{p} U_1(\mu) = p^3 \left( \frac{1 - \Gamma^4}{p} \right).$$

This means that the 19th reciprocal root of $P(T)$ is $\left( \frac{1 - \Gamma^4}{p} \right) p$. The remaining two are harder to obtain (see [Dwo69, p.75-77]), and involve the analytic continuation of the function $F(1/\lambda^4)/F(1/\lambda^{4p})$, where $F$ is the generalized hypergeometric function

$$F(\lambda) = F\left(\frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1, \lambda \right) = \sum_{n=0}^{\infty} \frac{(1/4)_n(1/2)_n(3/4)_n}{n!^{1/3}} \lambda^n.$$

Note that we have assumed throughout that $\Gamma^4 \neq 1$, in which case $f$ is non-singular, since

$$\nabla f = 0 \implies x_1^4 = \Gamma x_1 x_2 x_3 x_4 \implies (x_1 x_2 x_3 x_4)^4 = \Gamma^4(x_1 x_2 x_3 x_4)^4.$$
For $\Gamma^4 = 1$ the point $[1 : \Gamma : \Gamma : \Gamma]$ is singular, so this is the precise condition for $f$ to be non-singular. Finally, we remark that the choice $p = 1 \mod 4$ is only made to simplify the computations. The case $p = 3 \mod 4$ is similar, but the block structure of $U(0)$ is more complicated. The general case over $\mathbb{F}_q$ is not much more difficult either, but we would have needed to factor $U$ by modifying the operator $\Psi_p$ slightly (see [LW06, Def. 21]). In both cases we would also obtain that the first 19th reciprocal roots of $P(T)$ are of the form $\pm q$.

References

[ Cd07 ] Philip Candelas and Xenia de la Ossa. The Zeta-Function of a p-Adic Manifold, Dwork Theory for Physicists. arXiv e-prints, page arXiv:0705.2056, May 2007.

[ CdR00 ] Philip Candelas, Xenia de la Ossa, and Fernando Rodriguez-Villegas. Calabi-Yau Manifolds Over Finite Fields, I. arXiv e-prints, pages hep-th/0012233, Dec 2000.

[ Dwo60 ] Bernard Dwork. On the rationality of the zeta function of an algebraic variety. American Journal of Mathematics, 82(3):631–648, 1960.

[ Dwo62 ] Bernard M. Dwork. On the zeta function of a hypersurface. Publications Mathématiques de l’IHÉS, 12:5–68, 1962.

[ Dwo69 ] Bernard M. Dwork. $p$-adic cycles. Publications Mathématiques de l’IHÉS, 37:27–115, 1969.

[ Kat72 ] Nicholas Katz. Algebraic solutions of differential equations (p-curvature and the hodge filtration). Inventiones mathematicae, 18:1–118, 1972.

[ Kob84 ] Neal Koblitz. $p$-adic numbers, $p$-adic analysis and zeta functions. Springer-Verlag, 1984.

[ Lau04a ] Alan Lauder. Counting solutions to equations in many variables over finite fields. Foundations of Computational Mathematics, 4:221–267, 07 2004.

[ Lau04b ] Alan Lauder. Deformation theory and the computation of zeta functions. Proceedings of The London Mathematical Society - PROC LONDON MATH SOC, 88, 05 2004.

[ LW06 ] Alan G. B. Lauder and Daqing Wan. Counting points on varieties over finite fields of small characteristic. arXiv Mathematics e-prints, page math/0612147, Dec 2006.

[ Mat86 ] Hideyuki Matsumura. Commutative Ring Theory. Cambridge University Press, 1986.

[ Mon70 ] Paul Monsky. $p$-adic analysis and zeta functions. Lectures in mathematics, Kyoto University, 1970.

[ Neu99 ] Jurgen Neukirch. Algebraic Number Theory. Springer-Verlag, 1999.

[ Pro ] Stacks Project. https://stacks.math.columbia.edu/tag/062D. Accessed: 30/01/2020.

[ Rob00 ] Alain M. Robert. A Course in $p$-adic Analysis. Springer Verlag, 2000.
[Rob01] Alain M. Robert. The gross-koblitz formula revisited. *Rendiconti del Seminario Matematico della Università di Padova*, 105:157–170, 2001.