On a Theorem of Dwork

Benjamin Michael Dickman

April 14, 2008

Advisor: Professor Robert Benedetto

Submitted to the
Department of Mathematics and Computer Science
of Amherst College
in partial fulfillment of the requirements
for the degree of
Bachelor of Arts with Distinction

Abstract

This thesis concerns the number of zeros of a multivariable polynomial f over a finite field. More specifically, the zeta-function of f is defined in terms of a certain power series with coefficients determined by the number of zeros of f over various finite fields. Our main result is Dwork's Theorem, stating that the zeta-function of f is in fact a rational function, i.e., a quotient of two polynomials, each with rational coefficients.

Acknowledgements

I would like to thank my parents, grandparents, siblings, and dog, for their constant words (and barks) of encouragement. I would also like to thank the Amherst College math department, who took me in as a lowly Math 11 student and convinced me to continue my mathematical education with Math 12, 13, 15, 21, 26, 28, 31, 34, 37, 42, 44, 77, and 78. Of course, I would especially like to thank Professor Benedetto, who introduced me to p-adic numbers and mathematical research during a summer REU, gave me the opportunity to be a teaching assistant for an introductory Calculus class, was extremely involved in the thesis writing process from start to finish, and taught me that the plural of the word "genus" is "genera."

Index of Notation

Contents

Chapter 1

Background

1.1 Algebraic Geometry

Throughout this section, let K be a field and let n be a positive integer.

Definition 1.1. We define *n-dimensional affine space over K*, denoted $\mathbb{A}^n_K$, to be the set of ordered n-tuples $(x_1, \ldots, x_n)$ where each $x_i \in K$.

The notation $\mathbb{A}^n_K$ is used instead of K^n to emphasize that we are thinking of the set as a set merely of points, not as a vector space.

Definition 1.2. Let $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ be a non-zero polynomial in n variables. Then the *affine hypersurface* defined by f in $\mathbb{A}^n_K$ is defined to be

$$H_f = \{(x_1, \ldots, x_n) \in \mathbb{A}^n_K \mid f(x_1, \ldots, x_n) = 0\}.$$

We define the *dimension* of H_f to be the number $n - 1$.

Although our main theorem will be concerned only with affine space, we also have the following definition.

Definition 1.3. We define *n-dimensional projective space over K*, denoted $\mathbb{P}^n_K$, to be the set of equivalence classes of $\mathbb{A}^{n+1}_K - \{(0, \ldots, 0)\}$, where we declare $(x_0, x_1, \ldots, x_n)$ to be equivalent to $(y_0, y_1, \ldots, y_n)$ if and only if there is a $\lambda \in K - \{0\}$ such that $y_i = \lambda x_i$ for all $i = 0, 1, \ldots, n$.

Projective n-space can be viewed as containing affine n-space, as follows. Consider the map $\mathbb{A}_K^n \hookrightarrow \mathbb{P}_K^n$ defined by

$$(x_1, \ldots, x_n) \mapsto \text{ equivalence class of } (x_1, \ldots, x_n, 1).$$

Thus the image of $\mathbb{A}_K^n$ consists of all of $\mathbb{P}_K^n$ except for the equivalence classes of $(n+1)$-tuples of the form $(x_1, \ldots, x_n, 0)$. Meanwhile, that hyperplane is isomorphic to $\mathbb{P}_K^{n-1}$ under the one-to-one correspondence sending

$$\text{equivalence class of } (x_1, \ldots, x_n, 0) \mapsto \text{ equivalence class of } (x_1, \ldots, x_n).$$

Continuing in this fashion, and abusing notation slightly, we can write $\mathbb{P}_K^n$ as the disjoint union

$$\mathbb{P}_K^n = \mathbb{A}_K^{n-1} \cup \mathbb{A}_K^{n-2} \ldots \cup \mathbb{A}_K^1 \cup \{\text{point}\}.$$

Definition 1.4. Given a monomial $x_1^{d_1} \cdots x_n^{d_n}$, the *total degree* d is defined to be $d = d_1 + \cdots + d_n$. We say a polynomial $\tilde{f}(X_0, \ldots, X_n) \in K[X_0, \ldots, X_n]$ is *homogeneous* of degree d if it is a linear combination of monomials, each of which has the same total degree d.

Note that if $\tilde{f}(X_0, \ldots, X_n) \in K[X_0, \ldots, X_n]$ is homogeneous and $\tilde{f}(x_0, \ldots, x_n) = 0$, then $\tilde{f}(\lambda x_0, \ldots, \lambda x_n) = 0$ for all $\lambda \in K - \{0\}$. Thus, the following definition should make sense.

Definition 1.5. Let $\tilde{f}(X_0, \ldots, X_n) \in K[X_0, \ldots, X_n]$ be a polynomial in $n+1$ variables. Then the *projective hypersurface* defined by $\tilde{f}$ in $\mathbb{P}_K^n$ is defined to be

$$\tilde{H}_{\tilde{f}} = \{(x_0, x_1, \ldots, x_n) \in \mathbb{P}_K^n \mid \tilde{f}(x_0, x_1, \ldots, x_n) = 0\}.$$

We conclude our first section with the following lemma.

Lemma 1.6. *Let Ω be an algebraically closed field. Then for any positive integers n and a, we have*

$$\sum_{\substack{\zeta \in \Omega \\ \zeta^n = 1}} \zeta^a = \begin{cases} n & \textit{if } n | a \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. If n divides a, then

$$\sum_{\substack{\zeta\in\Omega\\ \zeta^n=1}} \zeta^a = \sum_{\substack{\zeta\in\Omega\\ \zeta^n=1}} (\zeta^n)^k = \sum_{\substack{\zeta\in\Omega\\ \zeta^n=1}} 1 = n.$$

If n does not divide a, let $S = \sum_{\substack{\zeta\in\Omega\\ \zeta^n=1}} \zeta^a$, and let $\zeta_n \in \Omega$ be a primitive n^{th} root of unity; note that ζ_n exists because Ω is algebraically closed. Then $\zeta_n^a \cdot S = S$. But $\zeta_n^a \neq 1$; so $S = 0$. □

1.2 Inclusion/Exclusion Principle

The following principle from Discrete Mathematics will be useful to us both in proving our main theorem, and in proving some of its corollaries.

Proposition 1.7 (Inclusion/Exclusion Principle)**.** *Suppose $A_1, \dots, A_n$ are finite sets. Then*

$$\left|\bigcup_{i=1}^n A_i\right| = \sum_{i=1}^n |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i\cap A_j\cap A_k| - \cdots + (-1)^{n+1}|A_1\cap\cdots\cap A_n|.$$

Proof. We proceed by induction on n. The case $n = 1$ is trivial. Suppose the statement holds for n sets. For $n + 1$ sets, we have

$$\begin{aligned}\left|\bigcup_{i=1}^{n+1} A_i\right| = \left|\Big(\bigcup_{i=1}^{n} A_i\Big)\cup A_{n+1}\right| &= \left|\bigcup_{i=1}^{n} A_i\right| + \left|A_{n+1}\right| - \left|\Big(\bigcup_{i=1}^{n} A_i\Big)\cap A_{n+1}\right| \\ &= \left|\bigcup_{i=1}^{n} A_i\right| + \left|A_{n+1}\right| - \left|\bigcup_{i=1}^{n} \Big(A_i\cap A_{n+1}\Big)\right|.\end{aligned}$$

Note $A_i \cap A_{n+1}$ is a finite set for all i, and hence we can now use our inductive hypothesis for the unions above. This gives us

$$\begin{aligned}&\left|\bigcup_{i=1}^{n+1} A_i\right| = \sum_{i=1}^n \left|A_i\right| - \sum_{1\le i<j\le n}\left|A_i\cap A_j\right| + \sum_{1\le i<j<k\le n}\left|A_i\cap A_j\cap A_k\right| - \cdots + (-1)^{n+1}\left|A_1\cap\cdots\cap A_n\right| + \left|A_{n+1}\right| \\ &-\Big(\sum_{i=1}^n\left|A_i\cap A_{n+1}\right| - \sum_{1\le i<j\le n}\left|A_i\cap A_j\cap A_{n+1}\right| + \sum_{1\le i<j<k\le n}\left|A_i\cap A_j\cap A_k\cap A_{n+1}\right| - \cdots + (-1)^{n+1}\left|A_1\cap\cdots\cap A_{n+1}\right|\Big) \\ &= \sum_{i=1}^{n+1}\left|A_i\right| - \sum_{1\le i<j\le n+1}\left|A_i\cap A_j\right| + \sum_{1\le i<j<k\le n+1}\left|A_i\cap A_j\cap A_k\right| - \cdots + (-1)^{n+2}\left|A_1\cap\cdots\cap A_{n+1}\right|.\end{aligned}$$

Thus the Inclusion/Exclusion principle holds for all integers $n \ge 1$. □

1.3 Statement of Dwork's Theorem

We end our introductory chapter by stating our main theorem and outlining the remainder of the thesis.

Definition 1.8. Let K be a field, and let n be a positive integer. Let $f(X_1, \ldots, X_n) \in K[X_1, \ldots X_n]$ be a non-zero polynomial. For a field M containing K, we then define

$$H_f(M) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n_M \mid f(x_1, \ldots, x_n) = 0\}.$$

Given $f \in \mathbb{F}_q[X_1, \ldots, X_n]$, we then form the following sequence of natural numbers:

$$N_s = \#(H_f(\mathbb{F}_{q^s})).$$

Let $1 + T\mathbb{Q}[T]$ denote the set of power series in T with rational coefficients and constant term 1. We are now ready to define the zeta-function we will be considering in this thesis, after which we can formally state Dwork's Theorem.

Definition 1.9. Let n be a positive integer. Then the *zeta-function* of H_f over the field $\mathbb{F}_q$ is defined to be the power series

$$Z(H_f/\mathbb{F}_q; T) = \exp\Big(\sum_{s=1}^{\infty} N_s T^s/s\Big) \in 1 + T\mathbb{Q}[[T]].$$

Here, $\exp(T) = \sum_{n=0}^{\infty} T^n/n! \in \mathbb{Q}[[T]]$ is considered as a formal power series, and the composition is simply composition of formal power series.

At first glance it is not at all clear what sort of properties such an infinite power series might have. It is thus all the more surprising that the following result holds.

Theorem 1.10 (Dwork)**.** *The zeta function of any affine hypersurface is a ratio of two polynomials with coefficients in* $\mathbb{Q}$*.*

How does one go about proving such a theorem? Before we go any further, we begin with a few examples to illustrate how the zeta-function works.

First, recall from calculus that the Maclaurin series of $-\log(1-T)$ is

$$-\log(1-T) = \sum_{s=1}^{\infty} T^s/s.$$

Example 1.11. The zeta-function $Z(\mathbb{A}^n_{\mathbb{F}_q}/\mathbb{F}_q;T)$ of the space $\mathbb{A}^n_{\mathbb{F}_q}$ is $1/(1-q^nT)$.

Proof. In this case we have $N_s = \#\mathbb{A}^n_{\mathbb{F}_{q^s}} = q^{ns}$, and hence

$$\exp\Big(\sum_{s=1}^{\infty} N_sT^s/s\Big) = \exp\Big(\sum_{s=1}^{\infty}(q^nT)^s/s\Big) = \exp\Big(-\log(1-q^nT)\Big) = 1/(1-q^nT). \qquad \square$$

Example 1.12. The zeta-function $Z(\mathbb{P}^n_{\mathbb{F}_q}/\mathbb{F}_q;T)$ of the space $\mathbb{P}^n_{\mathbb{F}_q}$ is $\displaystyle\prod_{i=0}^{n}\frac{1}{1-q^iT}$.

Proof. Recall that we have the disjoint union

$$\mathbb{P}^n_K = \mathbb{A}^{n-1}_K \cup \mathbb{A}^{n-2}_K \ldots \cup \mathbb{A}^1_K \cup \{\text{point}\}.$$

Thus, $N_s = q^{sn} + q^{s(n-1)} + \cdots + q^s + 1$, so that

$$\exp\Big(\sum_{s=1}^{\infty} N_sT^s/s\Big) = \prod_{i=0}^{n}\exp\Big(\sum_{s=1}^{\infty} q^{si}T^s/s\Big) = \prod_{i=0}^{n}\frac{1}{1-q^iT}. \qquad \square$$

Remark 1.13. Note that strictly speaking, we have only defined the zeta-function for an affine hypersurface. However, we can still consider $\exp\Big(\sum_{s=1}^{\infty} N_sT^s/s\Big)$ using the obvious choice for our $\{N_s\}_{s\geq 1}$, namely the sequence of integers defined by $N_s = \#\mathbb{P}^n_{\mathbb{F}_{q^s}}$ for $s \geq 1$.

Example 1.14. The zeta-function $Z(H_f/\mathbb{F}_q;T)$ for H_f defined by $f = x_1x_4 - x_2x_3 - 1$ is $\frac{1-qT}{1-q^3T}$.

Proof. In order to calculate N_s, we consider two cases:

Case 1. $x_3 = 0$. Then $x_1x_4 - x_2x_3 = 1$ becomes $x_1x_4 = 1$. Since x_2 is out of the equation, it can be any element of $\mathbb{F}_{q^s}$. Thus, there are q^s choices for x_2. Meanwhile, x_1 can be any element of $\mathbb{F}^\times_{q^s}$. Then $x_4 = (x_1)^{-1}$ is already determined. Hence there are $q^s(q^s-1) = q^{2s} - q^s$ points in H_f with $x_3 = 0$.

Case 2. $x_3 \neq 0$. Then x_1 and x_4 can be any elements of $\mathbb{F}_{q^s}$, and x_3 can be any element of $\mathbb{F}^\times_{q^s}$. But this completely determines x_2, so that there are $q^sq^s(q^s-1) = q^{3s} - q^{2s}$ points in H_f with

$x_3 \neq 0$.

Thus $N_s = \#(H_f(\mathbb{F}_{q^s})) = q^{3s} - q^{2s} + q^{2s} - q^s = q^{3s} - q^s$. So $Z(H_f/\mathbb{F}_q; T)$ becomes

$$\frac{\exp\left(\sum_{s=1}^{\infty} q^{3s}T^s/s\right)}{\exp\left(\sum_{s=1}^{\infty} q^{s}T^s/s\right)} = \frac{1-qT}{1-q^3T}. \qquad \square$$

Dwork's Theorem is the first part of a series of conjectures known as the Weil Conjectures, named after André Weil, which provide detailed information about the zeta-function. First proposed in the late 1940's, the Weil Conjectures were proved in their entirety by 1974. However, it was Bernard Dwork's proof in 1959 of the rationality of the zeta-function that was the first significant step towards a full proof. For Dwork's original paper, see [1]. For a partial statement of the Weil Conjectures, we refer the reader to Appendix B.

In order to prove that the rationality of the zeta-function holds in general, there is much work to be done. The following is a brief summary of our remaining chapters. In Chapter 2, we introduce the reader to $\mathbb{Q}_p$ along with a few well-known functions in p-adic analysis that will be useful to us later on. Chapter 3 defines several lesser-known functions, and uses them to prove results that will be necessary for the following chapter. It is there in Chapter 4 that the heart of our proof lies, as we show that the zeta-function is p-adic meromorphic. Chapter 5 serves as a bit of an interlude, in which we consider precisely when a power series can be written as a rational function. The thesis concludes with Chapter 6, in which we restate and then prove Dwork's Theorem along with several corollaries.

Chapter 2

$\mathbb{Q}_p$ and p-adic Analysis

2.1 Metrics and Absolute Values

Definition 2.1. Given a nonempty set X, a *metric* on X is a function $d : X \times X \to [0, \infty)$ such that for all $x, y, z \in X$:

(1) $d(x, y) = 0$ if and only if $x = y$.

(2) $d(x, y) = d(y, x)$.

(3) $d(x, y) \leq d(x, z) + d(z, y)$.

Definition 2.2. Given a field K, an *absolute value* is a function $\| \cdot \| : K \to [0, \infty)$ such that for $x, y \in K$:

(1) $\|x\| = 0$ if and only if $x = 0$.

(2) $\|x \cdot y\| = \|x\| \cdot \|y\|$.

(3) $\|x + y\| \leq \|x\| + \|y\|$.

The two definitions above may appear to be rather similar. In fact, they are intimately related, as can be seen in the following proposition.

Proposition 2.3. *Let K be a field and let $\| \cdot \|$ be an absolute value on K. Then $d(x, y) = \|x - y\|$ is a metric.*

Proof. Let $x, y, z \in K$.

(1) $d(x, y) = 0 \iff \|x - y\| = 0 \iff x - y = 0 \iff x = y$, where the first equivalence

is by definition of d, and the second is a property of $\|\cdot\|$.

(2) Note that $\|1\| = \|1 \cdot 1\| = \|1\| \cdot \|1\|$. Since $1 \neq 0$, we have $\|1\| \neq 0$. Thus $\|1\| = 1$. Hence $1 = \|1\| = \|(-1)(-1)\| = \|-1\| \cdot \|-1\|$. Since $\|-1\| \geq 0$ by the definition of an absolute value, we have $\|-1\| = 1$. Hence,

$$d(x,y) = \|x-y\| = \|(-1)(y-x)\| = \|-1\| \cdot \|y-x\| = \|y-x\| = d(y,x).$$

(3) $d(x,y) = \|x-y\| = \|(x-z)+(z-y)\| \leq \|x-z\| + \|z-y\| = d(x,z) + d(z,y)$. □

Thus with the above proposition in mind, we have the following definition.

Definition 2.4. We say a metric d on a field K is *induced* by an absolute value $\|\cdot\|$ if d is defined by $d(x,y) = \|x-y\|$.

Example 2.5. Let $K = \mathbb{Q}$. Then the absolute value $|x|$ induces a metric $d(x,y) = |x-y|$ which is the usual concept of distance on the real number line. We will denote this absolute value by $|\cdot|_\infty = |\cdot|$ solely for notational convenience.

One might wonder if there are other, less familiar absolute values on $\mathbb{Q}$.

Definition 2.6. Let p be any prime number. For any nonzero integer a, let $\operatorname{ord}_p a$ be the highest power of p which divides a, i.e., the greatest m such that $a \equiv 0 \mod p^m$. If $a = 0$, we write $\operatorname{ord}_p a = \infty$. For a rational number $x = a/b$, we define $\operatorname{ord}_p x$ to be $\operatorname{ord}_p a - \operatorname{ord}_p b$.

Remark 2.7. Note that the definition of ord_p is well-defined for elements of $\mathbb{Q}$: If $a/b = c/d$, then $\operatorname{ord}_p a - \operatorname{ord}_p b = \operatorname{ord}_p c - \operatorname{ord}_p d$. Note also that $\operatorname{ord}_p(xy) = \operatorname{ord}_p x + \operatorname{ord}_p y$ for all $x, y \in \mathbb{Q}$.

Example 2.8. Let $x = 40 = 2^3 \cdot 5$. Then $\operatorname{ord}_2 x = \operatorname{ord}_2 40 = 3$.
Let $y = 5/81 = 5/3^4$. Then $\operatorname{ord}_3 y = \operatorname{ord}_3(5/81) = \operatorname{ord}_3 5 - \operatorname{ord}_3 81 = 0 - 4 = -4$.
Let $z = -31/7$. Then $\operatorname{ord}_5 z = \operatorname{ord}_5(-31) - \operatorname{ord}_5 7 = 0 - 0 = 0$.

Proposition 2.9. *Consider the map $|\cdot|_p : \mathbb{Q} \to [0,\infty)$ defined by:*

$$|x|_p = \begin{cases} p^{-\operatorname{ord}_p x}, & \text{if } x \neq 0; \\ 0, & \text{if } x = 0. \end{cases}$$

Then $|\cdot|_p$ is an absolute value on $\mathbb{Q}$.

Proof. It is clear that $|\cdot|_p$ satisfies properties (1) and (2) of absolute values. For property (3), note that for any $r, s \in \mathbb{Z}$ we have $\operatorname{ord}_p(r+s) \geq \min\{\operatorname{ord}_p r, \operatorname{ord}_p s\}$. After all, if $p^m|r$ and $p^m|s$, then $p^m|(r+s)$. With this in mind, given $x, y \in \mathbb{Q}$, we write $x = a/b$ and $y = c/d$ in lowest terms, so that $x + y = (ad+bc)/bd$. Now $\operatorname{ord}_p(x+y) = \operatorname{ord}_p(ad+bc) - \operatorname{ord}_p b - \operatorname{ord}_p d$. Hence,

$$\begin{aligned}\operatorname{ord}_p(x+y) &\geq \min\{\operatorname{ord}_p(ad), \operatorname{ord}_p(bc)\} - \operatorname{ord}_p b - \operatorname{ord}_p d \\ &= \min\{\operatorname{ord}_p a + \operatorname{ord}_p d, \operatorname{ord}_p b + \operatorname{ord}_p c\} - \operatorname{ord}_p b - \operatorname{ord}_p d \\ &= \min\{\operatorname{ord}_p a - \operatorname{ord}_p b, \operatorname{ord}_p c - \operatorname{ord}_p d\} \\ &= \min\{\operatorname{ord}_p x, \operatorname{ord}_p y\}.\end{aligned}$$

Thus $|x+y|_p = p^{-\operatorname{ord}_p(x+y)} \leq \max\{p^{-\operatorname{ord}_p x}, p^{-\operatorname{ord}_p y}\} = \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$. □

Note that we actually proved a stronger inequality above than property (3). This leads us to the following definition.

Definition 2.10. Let K be a field. An absolute value $\|\cdot\|$ on K is *non-Archimedean* if

$$\|x+y\| \leq \max\{\|x\|, \|y\|\} \text{ for all } x, y \in K.$$

A metric d on X is *non-Archimedean* if

$$d(x,y) \leq \max\{d(x,z), d(z,y)\} \text{ for all } x, y, z \in X.$$

Thus $|\cdot|_p$ is a non-Archimedean absolute value on $\mathbb{Q}$. Note also that a non-Archimedean absolute value always induces a non-Archimedean metric, since then:

$$d(x,y) = \|x-y\| = \|(x-z)+(z-y)\| \leq \max\{\|x-y\|, \|z-y\|\} = \max\{d(x,z), d(y,z)\}.$$

Now that we have established that $|\cdot|_p$ is an absolute value on $\mathbb{Q}$, a natural question to ask is: Why bother studying this particular absolute value? Before answering this, we provide the following two definitions.

Definition 2.11. Two metrics d_1 and d_2 on a nonempty set X are said to be *equivalent* if there exist $c_1, c_2, \in (0, \infty)$ such that for all $x, y \in X$ we have: $d_1(x,y) \leq c_1 d_2(x,y)$ and $d_2(x,y) \leq c_2 d_1(x,y)$. We say two absolute values are equivalent if they induce equivalent metrics.

Definition 2.12. The *trivial* absolute value on a field K is given by $\|0\| = 0$ and $\|x\| = 1$ for all $x \in K - \{0\}$. (Note that this does in fact give an absolute value.) Any other absolute value is thus said to be *nontrivial.*

The following characterization of absolute values on the rational numbers is due to Alexander Ostrowski.

Theorem 2.13 (Ostrowski)**.** *Every nontrivial absolute value $\|\cdot\|$ on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some prime p or for $p = \infty$.*

Proof. The proof of this is elementary but not particularly pertinent, and thus is omitted. See [2, pp. 3 – 5]. □

Working with an absolute value such as $|\cdot|_p$ can have strange consequences. Consider a "triangle" with vertices $0, x, y \in K$, and hence sides of length $\|x\|, \|y\|$, and $\|x - y\|$, where $\|\cdot\|$ is a non-Archimedean absolute value on K. The following proposition says that (at least) two of these lengths are equal. Thus every "triangle" in K is isosceles.

Proposition 2.14 (Isosceles Triangle Principle)**.** *Let K be a field with non-Archimedean absolute value $\|\cdot\|$, and let $x, y \in K$ with $\|x\| \neq \|y\|$. Then $\|x \pm y\| = \max\{\|x\|, \|y\|\}$.*

Proof. Without loss of generality, suppose $\|x\| < \|y\|$. Then

$$\|x - y\| \leq \max(\|x\|, \|y\|) = \|y\| = \|x - (x - y)\| \leq \max(\|x\|, \|x - y\|) = \|x - y\|,$$

where the final equality follows since $\|y\| \not\leq \|x\|$. Therefore, we have $\|y\| = \|x - y\|$. For $\|x + y\|$, we have $\|x + y\| = \|x - (-y)\| = \max\{\|x\|, \|-y\|\} = \max\{\|x\|, \|y\|\}$. □

As another example of a surprising property of non-Archimedean absolute values, consider the following definitions.

Definition 2.15. Let K be a field. Let $\|\cdot\|$ be a non-Archimedean absolute value on K. Let $r \in \mathbb{R}^+$, and let $a \in K$. Then we define the open disc of radius r with center a to be

$$D_a(r^-) = \{x \in K \mid \|x - a\| < r\}.$$

Similarly, we define the closed disc of radius r with center a to be

$$D_a(r) = \{x \in K \mid \|x - a\| \leq r\}.$$

Finally, we let $D(r) = D_0(r)$ and $D(r^-) = D_0(r^-)$.

With this definition in mind, it will turn out that any point in a disc can serve as the center. We make this idea precise with the following proposition.

Proposition 2.16. *Let K be a field and let $\| \cdot \|$ be a non-Archimedean absolute value on K. Let $a, b \in K$, with $b \in D_a(r)$. Then*

$$D_a(r) = D_b(r).$$

Proof. Consider $x \in D_a(r)$. Then $\|x - a\| \leq r$ by definition of a closed disc. Thus,

$$\|x - b\| = \|(x - a) + (a - b)\| \leq \max\{\|x - a\|, \|a - b\|\} \leq r,$$

so that $x \in D_b(r)$. Similarly, we have that $x \in D_b(r)$ implies $x \in D_a(r)$. Hence $D_a(r) = D_b(r)$. □

Remark 2.17. Note that the same proof shows the above proposition for open discs, where we simply replace $\leq$ with $<$.

Propositions 2.14 and 2.16 serve as an introduction to how how strange the non-Archimedean world can be. Bearing them in mind, we are now ready to move on and use one specific non-Archimedean absolute value, $| \cdot |_p$, to construct the field of p-adic numbers known as $\mathbb{Q}_p$.

2.2 $\mathbb{Q}_p$, Ω, and $\mathbb{Z}_p$

The reader familiar with a construction of $\mathbb{R}$ from $\mathbb{Q}$ using Cauchy sequences of rational numbers should see a strong resemblance in the constructions of the following section.

Definition 2.18. Let K be a field and let $\|\cdot\|$ be an absolute value on K. A sequence $\{a_1, a_2, a_3, \ldots\}$ is *Cauchy* (with respect to $\| \cdot \|$) if for every real number $\varepsilon > 0$ there is a positive integer N such that for all natural numbers $m, n > N$, we have $\|a_m - a_n\| < \varepsilon$. We say that K is *complete* (with respect to $\| \cdot \|$) if every Cauchy sequence of points in K has a limit that is also in K.

Definition 2.19. Consider the set of sequences of rational numbers that are Cauchy with respect to $|\cdot|_p$. We say two such Cauchy sequences $\{a_i\}$ and $\{b_i\}$ are *equivalent* if $|a_i - b_i|_p \to 0$ as $i \to \infty$. Then $\mathbb{Q}_p$ is defined to be the set of equivalence classes of Cauchy sequences. Elements of $\mathbb{Q}_p$ are called *p-adic rational numbers.*

Given equivalence classes a and b of Cauchy sequences as in Definition 2.19, choose any representatives $\{a_i\} \in a$ and $\{b_i\} \in b$. We then define $a \cdot b$ to be the equivalence class represented by the Cauchy sequence $\{a_i b_i\}$. Similarly, we define $a + b$ to be $\{a_i + b_i\}$ and $a - b$ to be $\{a_i - b_i\}$. For multiplicative inverses, given a Cauchy sequence a, we can pick $\{a_i\} \in a$ with no zero terms; we then use the sequence $\{1/a_i\}$, which will be Cauchy unless $\{a_i\}$ is equivalent to $\{0\}$. It is easy to check that these operations are well-defined.

The set $\mathbb{Q}_p$ of equivalence classes of Cauchy sequences forms a field with addition, multiplication, and inverses defined as above. We can also view $\mathbb{Q} \subset \mathbb{Q}_p$ by identifying an element $x \in \mathbb{Q}$ with the equivalence class of the constant sequence $\{x, x, \ldots\}$ in $\mathbb{Q}_p$.

To see that $+$ and $\cdot$ on $\mathbb{Q}_p$ obey the distributive law, consider $a, b, c \in \mathbb{Q}_p$. Choose sequences $\{a_i\}, \{b_i\}, \{c_i\}$ to be their respective representatives. Then $a(b + c)$ is the equivalence class of $\{a_i(b_i + c_i)\} = \{a_i b_i + a_i c_i\}$, which also lies in the equivalence class of $ab + ac$. The other field axioms hold similarly.

Given a Cauchy sequence $\{a_i\}$ that does not tend to 0, we can find a real number $c > 0$ and an integer N_1 so that whenever $n \geq N_1$, we have $|a_n|_p \geq c > 0$. Since the sequence is Cauchy, we can also find an integer N_2 such that whenever $m, n \geq N_2$ we have $|a_n - a_m|_p < c$. Let $N = \max\{N_1, N_2\}$. Then

$$n, m \geq N \quad \Longrightarrow \quad |a_n - a_m|_p < \max\{|a_n|_p, |a_m|_p\}.$$

By the Isosceles Triangle Principle, we thus have $|a_n|_p = |a_m|_p$ for all $n, m > N$. We can now extend $|\cdot|_p$ to $\mathbb{Q}_p$ in the following natural way.

Definition 2.20. Let $a \in \mathbb{Q}_p$ be represented by the Cauchy sequence $\{a_i\}$. Then we define

$$|a|_p = \lim_{n \to \infty} |a_n|_p.$$

Thus $\mathbb{Q}_p$ is complete with respect to $|\cdot|_p$; i.e., every $|\cdot|_p$-Cauchy sequence in $\mathbb{Q}_p$ converges.

We now wish to extend $|\cdot|_p$ not only to $\mathbb{Q}_p$, but any field K that is a finite extension of $\mathbb{Q}_p$. Given such a finite extension $\mathbb{Q}_p \subset K$, view K as a finite-dimensional vector space over $\mathbb{Q}_p$. Thus, given $\alpha \in K$, we have a linear map $K \to K$ defined by multiplication by α. Since the map is linear, it has an associated matrix, A_α, for any given $\mathbb{Q}_p$ basis of K.

Definition 2.21. Let K be a finite field extension of $\mathbb{Q}_p$. Given $\alpha \in K$, let A_α be the matrix corresponding to multiplication by α. Then we define the *norm function* $N_{K/\mathbb{Q}_p} : K \to \mathbb{Q}_p$ by $N_{K/\mathbb{Q}_p}(\alpha) = \det(A_\alpha)$.

Theorem 2.22. *Let $\mathbb{Q}_p \subset K$ be a finite extension of degree n. Then the function $|\cdot|_p : K \to [0, \infty)$ defined by*

$$|x|_p = |N_{K/\mathbb{Q}_p}(x)|_p^{1/n}$$

is a non-Archimedean absolute value on K extending the p-adic absolute value on $\mathbb{Q}_p$.

Proof. (Sketch.) Let $\alpha, \beta \in K$. We have $|\alpha|_p = 0$ if and only if $|N_{K/\mathbb{Q}_p}(\alpha)|_p = 0$; since $N_{K/\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p$, this happens if and only if $N_{K/\mathbb{Q}_p}(\alpha) = 0$. But this, in turn, occurs only when multiplication by α is not invertible. Since K is a field, this happens only when $\alpha = 0$. For the second property, by properties of determinants, we have $N_{K/\mathbb{Q}_p}(\alpha \cdot \beta) = N_{K/\mathbb{Q}_p}(\alpha) \cdot N_{K/\mathbb{Q}_p}(\beta)$. Then take n^{th} roots of each side.

In order to show our new absolute value is the same as our old one when restricted to $\mathbb{Q}_p$, let $\alpha \in \mathbb{Q}_p$. It is then clear from our determinant definition that $N_{K/\mathbb{Q}_p}(\alpha) = \alpha^n$. Thus, $|\alpha| = (|\alpha|_p^n)^{1/n} = |\alpha|_p$.

We omit the proof that our new absolute value is non-Archimedean, as it is tedious and takes us too far afield. For a full proof of this, see [2, p. 62] or [3, p. 151] □

Given an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, the absolute value extends to $\bar{\mathbb{Q}}_p$ as follows. For any $\alpha \in \bar{\mathbb{Q}}_p$, let $K \subset \bar{\mathbb{Q}}_p$ be any finite extension of $\mathbb{Q}_p$ containing α, and define $|\alpha|_p$ as in Theorem 2.22. Such a field K always exists (e.g., $K = \mathbb{Q}_p(\alpha)$), and it is easy to check that this definition of $|\alpha|_p$

is independent of the choice of K. It follows easily that $|\cdot|_p$ is an absolute value on $\bar{\mathbb{Q}}_p$ that agrees with the definition in Theorem 2.22 on any finite subextension $\mathbb{Q}_p \subset K$.

Unfortunately, $\bar{\mathbb{Q}}_p$, unlike $\mathbb{Q}_p$ and its finite extensions, is no longer complete. By the same process we used to construct $\mathbb{Q}_p$, we can define a field Ω, consisting of equivalence classes of Cauchy sequences on $\bar{\mathbb{Q}}_p$. Then $\bar{\mathbb{Q}}_p$ embeds (via constant sequences) into Ω, and the absolute value $|\cdot|_p$ extends to Ω. It is here in Ω that we will be carrying out our p-adic analysis, as motivated by the following theorem.

Theorem 2.23. *The field Ω is closed and complete with respect to $|\cdot|_p$.*

Proof. Omitted. See [2, pp. 71 – 73]. □

Having successfully built $\mathbb{Q}_p$ up to Ω, we now take a step in the reverse direction and consider a set contained within $\mathbb{Q}_p$.

Definition 2.24. We define the *p-adic integers* to be the set $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$. An element of $\mathbb{Z}_p$ is a called a *p-adic integer.*

Note that $\mathbb{Z} \subset \mathbb{Z}_p$: Given $n \in \mathbb{Z}$, can write $n = p^\ell \cdot r$, where $\ell \geq 0$ and p does not divide r. Then $|n|_p = p^{-\ell} \leq 1$.

Proposition 2.25. *$\mathbb{Z}_p$ is a* subring *of $\mathbb{Q}_p$, i.e., $\mathbb{Z}_p \subset \mathbb{Q}_p$ is closed under sum, difference, and product.*

Proof. Let $a, b \in \mathbb{Z}_p$, i.e., $|a|_p \leq 1$ and $|b|_p \leq 1$. Then $|a+b| \leq \max\{|a|_p, |b|_p\} \leq 1$. Thus $|a+b|_p \leq 1$, so that $a+b \in \mathbb{Z}_p$. The proof for $a-b$ is similar. For $a \cdot b$, we have $|ab|_p = |a|_p|b|_p \leq 1 \cdot 1 = 1$. Hence $ab \in \mathbb{Z}_p$. □

Definition 2.26. If $a, b \in \mathbb{Q}_p$, we write $a \equiv b \pmod{p^n}$ if $|a-b|_p \leq p^{-n}$.

Note that $a \equiv b (\text{mod } p^n)$ if and only if $(a-b)/p^n \in \mathbb{Z}_p$.

Lemma 2.27. *A sequence $\{a_n\}$ is a Cauchy sequence with respect to a non-Archimedean absolute value $\|\cdot\|$ if and only if*

$$\lim_{n\to\infty} \|a_{n+1} - a_n\| = 0.$$

Proof. The forward implication is clear. For the reverse implication, if $m = n + r$, then

$$\begin{aligned} \|a_m - a_n\| &= \|a_{n+r} - a_{n+r-1} + a_{n+r-1} - a_{n+r-2} + \cdots + a_{n+1} - a_n\| \\ &\leq \max\{\|a_{n+r} - a_{n+r-1}\|, \|a_{n+r-} - a_{n+r-2}\|, \dots, \|a_{n+1} - a_n\|\}, \end{aligned}$$

since the absolute value is non-Archimedean. The lemma thus follows. □

Theorem 2.28. *An infinite series* $\sum_{n=0}^{\infty} a_n$ *with* $a_n \in \Omega$ *converges if and only if*

$$\lim_{n\to\infty} a_n = 0.$$

Proof. A series converges if and only if the sequence of its partial sums converges. Note that a_n is the difference between the n^{th} and $(n-1)^{\text{st}}$ partial sum. Thus, if a_n tends to 0, it follows from Lemma 2.27 that the sequence of partial sums is a Cauchy sequence. Therefore, since Ω is complete, this sequence of partial sums converges. □

For an instance in which one might use the above theorem, we first recall that $D(r^-) = D_0(r^-) = \{x \in \Omega \mid |x|_p < r\}$.

Proposition 2.29. *Let* $f(X) \in \mathbb{Z}_p[[X]]$ *be a power series whose coefficients are all* p*-adic integers. Then* $f(X)$ *converges in* $D(1^-)$*, the open disc of radius 1 about the origin in* Ω.

Proof. Let $f(X) = \sum_{n=0}^{\infty} a_n X^n$, with $a_n \in \mathbb{Z}_p$. Let $x \in D(1^-)$. Then $|x|_p < 1$ and $|a_n|_p \leq 1$ for all n. Thus

$$|a_n x^n|_p \leq |x|_p^n \to 0 \text{ as } n \to \infty.$$

Thus, by Theorem 2.28, $f(x)$ converges for all $x \in D(1^-)$. □

2.3 Teichmüller Representatives

Just as we sometimes work not with integers but rather with their representatives mod p, in later chapters we will sometimes want to replace p-adic integers by another special set of representatives. However, in order to prove the existence of these representatives, we must invoke the following lemma named after Kurt Hensel, who was the first to describe p-adic numbers back in 1897.

Theorem 2.30 (Hensel's Lemma). *Let* $F(x) = \sum_{i=0}^{m} c_i x^i$ *be a polynomial with* $c_i \in \mathbb{Z}_p$ *for all* $i = 1, \dots, m$. *Let* $F'(x) = \sum_{i=0}^{n-1} i \cdot c_i x^{i-1}$ *denote the formal derivative of* F. *Let* $a_0 \in \mathbb{Z}_p$ *such that* $F(a_0) \equiv 0 \bmod p$ *and* $F'(a_0) \not\equiv 0 \bmod p$. *Then there exists a unique* $a \in \mathbb{Z}_p$ *such that*

$$F(a) = 0 \text{ and } a \equiv a_0 \bmod p.$$

Proof. We begin with the following claim.

Claim 2.31. *There exists a unique sequence of integers* $\{a_n\}_{n \geq 1}$*, such that for all* $n \geq 1$ *we have:*

(1) $F(a_n) \equiv 0 \bmod p^{n+1}$

(2) $a_{n+1} \equiv a_n \bmod p^n$

(3) $0 \leq a_n < p^{n+1}$.

Proof. We define the sequence (and prove its properties) inductively.

For $n = 1$, let $\tilde{a}_0$ be the unique integer in $\{0, 1, \dots, p-1\}$ such that $\tilde{a}_0 \equiv a_0 (\text{mod } p)$. Then (2) and (3) will hold if and only if $a_1 = \tilde{a}_0 + b_1 p$, for some $0 \leq b_1 \leq p - 1$. Expanding $F(\tilde{a}_0 + b_1 p)$, we have

$$\begin{aligned} F(a_1) = F(\tilde{a}_0 + b_1 p) &= \sum c_i (\tilde{a}_0 + b_1 p)^i \\ &\equiv \sum \left(c_i \tilde{a}_0^i + i c_i \tilde{a}_0^{i-1} b_1 p\right) \quad (\text{mod } p^2) \\ &\equiv F(\tilde{a}_0) + F'(\tilde{a}_0) b_1 p \quad (\text{mod } p^2). \end{aligned}$$

Since $F'(a_0) \not\equiv 0$, there is a unique integer $b_1 \in \{0, 1, \dots, p-1\}$ such that $F(\tilde{a}_0) + F'(\tilde{a}_0) b_1 p \equiv 0 (\text{mod } p^2)$. It follows immediately that $a_1 = \tilde{a}_0 + b_1 p$ is the unique integer satisfying (1) – (3).

Now suppose we already have $a_0, \dots, a_{n-1}$. As before, from (2) and (3), we need $a_n = a_{n-1} + b_n p^n$ for some $0 \leq b_n \leq p - 1$. Expanding $F(a_{n-1} + b_n p^n)$ as for $n = 1$, we have

$$F(a_n) = F(a_{n-1} + b_n p^n) \equiv F(a_{n-1}) + F'(a_{n-1}) b_n p^n (\text{mod } p^{n+1}).$$

But we know by our inductive hypothesis that $F(a_{n-1}) \equiv 0 (\text{mod } p^n)$. Write $F(a_{n-1}) \equiv \alpha p^n (\text{mod } p^{n+1})$, for $\alpha \in \{0, 1, \dots, p-1\}$, so that $F(a_n) \equiv 0 (\text{mod } p^{n+1})$ becomes

$$\alpha p^n + F'(a_{n-1}) b_n p^n \equiv 0 (\text{mod } p^{n+1}). \tag{2.1}$$

Hence $\alpha + F'(a_{n-1})b_n \equiv 0 (\text{mod } p)$. Since $a_{n-1} \equiv a_0 (\text{mod } p)$, we have

$$F'(a_{n-1}) \equiv F'(a_0) \not\equiv 0 (\text{mod } p).$$

Thus, there is a unique $b_n \in \{0, \ldots, p-1\}$ such that equation (2.1) holds. Hence $a_n = a_{n-1} + b_n p^n$ uniquely satisfies the desired properties. □

We are now ready to prove Hensel's Lemma. In the notation of Claim 2.31, let $a = \tilde{a}_0 + b_1 p + b_2 p^2 + \cdots$, the so-called base p expansion of a, which we will see converges later in Theorem 2.28. For all $n \geq 0$, we have $F(a) \equiv F(a_n) \equiv 0 (\text{mod } p^{n+1})$. Hence $F(a) = 0$. To prove uniqueness, suppose that there were another such $\tilde{a} \in \mathbb{Z}_p$. Then we would have a different sequence $\{\tilde{a}_n\}_{n \geq 1}$, satisfying (1) – (3) of Claim 2.31. But that would violate the uniqueness statement of the claim. □

Proposition 2.32. *For any prime p, $\mathbb{Q}_p$ contains exactly p solutions $a_0, \ldots, a_{p-1}$ to the equation $x^p - x = 0$, where $a_i \equiv i (\text{mod } p)$. In fact, $a_i \in \mathbb{Z}_p$ for all i.*

Proof. Let $F(x) = x^p - x$, so that $F'(x) = px^{p-1} - 1$ as in Hensel's Lemma. For $b = 0, \ldots, p-1$, we have $F(b) \equiv 0 (\text{mod } p)$, and $F'(b) = pb^{p-1} - 1 \equiv -1 \not\equiv 0 (\text{mod } p)$. Thus, Hensel's Lemma gives us the desired $a_0, \ldots, a_{p-1} \in \mathbb{Z}_p \subset \mathbb{Q}_p$. □

The set $\{a_0, \ldots, a_{p-1}\}$ in Proposition 2.32 of p-adic numbers is named after Oswald Teichmüller, who like Hensel was a German mathematician. Unfortunately, whereas Hensel was known for his invention of p-adic numbers, Teichmüller is instead known for being a passionate supporter of the National Socialists.

Definition 2.33. The p-adic numbers $\{a_0, \ldots, a_{p-1}\}$ in Proposition 2.19 are called the *Teichmüller representatives* of $\{0, \ldots, p-1\}$.

2.4 $\log(1+X)$, $\exp(X)$, and $\Upsilon(X, Y)$

In order to prove our main theorem, there are three specific functions which will be particularly useful. Before introducing them, we will need the following two concepts.

Definition 2.34. Given a power series $f(X) = \sum_{n=0}^{\infty} a_n X^n$ with $a_i \in \Omega$, we define the *radius of convergence* of f to be

$$r = \frac{1}{\limsup |a_n|_p^{1/n}}.$$

Thus $1/r$ is the least real number such that for any $C > 1/r$ there are only finitely many $n > 0$ such that $|a_n|_p^{1/n} > C$.

Proposition 2.35. *Given a series $f(X) \in \Omega[[X]]$ and radius r as above, then for any $x \in \Omega$, the series converges if $|x|_p < r$ and diverges if $|x|_p > r$.*

Proof. If $|x|_p < r$, we write $|x|_p = (1-\varepsilon)r$ for $\varepsilon \in (0,1]$. Then $|a_n x^n|_p = (r{|a_n|_p}^{1/n})^n(1-\varepsilon)^n$. With only finitely many n for which $|a_n|_p^{1/n} > 1/(r - \frac{1}{2}\varepsilon r)$, we have

$$\lim_{n\to\infty} |a_n x^n|_p \leq \lim_{n\to\infty} \Big(\frac{(1-\varepsilon)r}{(1-\frac{1}{2}\varepsilon)r)}\Big)^n = \lim_{n\to\infty} \Big(\frac{1-\varepsilon}{1-\frac{1}{2}\varepsilon}\Big)^n = 0.$$

Thus, the series converges by Theorem 2.28. Similarly, if $|x|_p > r$, write $|x|_p = (1+\varepsilon)r$ for $\varepsilon \in (0,\infty)$. then $a_n x^n \not\to 0$ as $n \to \infty$. This completes the proof and thus justifies our use of the term "radius of convergence" above. □

Example 2.36. Consider the series $g(X) = \sum_{n=1}^{\infty} (-1)^{n+1} X^n/n$. Writing $a_n = (-1)^{n+1}/n$, we have $|a_n|_p = p^{\text{ord}_p n}$, and hence $\lim_{n\to\infty} |a_n|_p^{1/n} = 1$. Thus, the series $g(x)$ converges if $|x|_p < 1$ and diverges if $|x|_p > 1$. When $|x|_p = 1$, we have $|a_n x^n|_p = p^{\text{ord}_p n} \geq 1$. Hence $|a_n|_p |x|_p^n \not\to 0$ and the series diverges. Thus $g(X)$ converges only on the disc $D(1^-)$.

Example 2.37. Let $h(X) = \sum_{n=0}^{\infty} X^n/n!$. Then h has radius of convergence $p^{-1/(p-1)}$. To see why, note that

$$\text{ord}_p(n!) = \sum_{i=1}^{\infty} \Big\lfloor \frac{n}{p^i} \Big\rfloor \leq \sum_{i=1}^{\infty} \frac{n}{p^i} = \frac{n}{p-1},$$

where the first equality can be shown as follows: Write $n! = 1 \cdot 2 \cdots (n-1) \cdot n$, and note that there are $\left\lfloor \frac{n}{p} \right\rfloor$ numbers between 1 and n divisible by p. Similarly, there are $\left\lfloor \frac{n}{p^2} \right\rfloor$ numbers between 1 and n divisible by p^2, and continuing in this fashion it is easy to see why the equality holds. Hence

$|a_n|_p = |1/n!|_p = p^{\operatorname{ord}_p n!} < p^{n/(p-1)}$. Thus $r \geq p^{-1/(p-1)}$, so that the series $h(x)$ converges when $|x|_p < p^{-1/(p-1)}$.

Now suppose $|x|_p = p^{-1/(p-1)}$. Let $n = p^m$. Then

$$\operatorname{ord}_p(n!) = \operatorname{ord}_p(p^m!) \leq 1 + p + \cdots + p^{m-1} = \frac{p^{m-1}}{p-1},$$

and therefore $\operatorname{ord}_p(x^n/n!) = p^m \operatorname{ord}_p x - p^{m-1}/(p-1)$. However, $\operatorname{ord}_p x = 1/(p-1)$, yielding

$$\operatorname{ord}_p(x^n/n!) = \frac{p^m}{p-1} - \frac{p^m - 1}{p-1} = \frac{1}{p-1}.$$

Thus $|a_n x^n|_p = |x^n/n!|_p \not\to 0$ as $n \to \infty$. Hence, the series diverges when $|x|_p = p^{-1/(p-1)}$. By Property 2.35, it must also diverge for $|x|_p > p^{1/(p-1)}$.

The reader may notice that our functions $g(X)$ and $h(X)$ above have power series representations very similar to the classical Maclaurin Series for $\log(1+X)$ and $\exp(X)$. Indeed, the only difference is that the coefficients of g and h are considered as elements of Ω, not $\mathbb{C}$. Thus, we make the following definition.

Definition 2.38. The *p-adic logarithm*, denoted $\log_p$, is defined to be the function

$$\log_p(1+X) : D(1^-) \to \Omega, \quad \text{defined by } \log_p(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} X^n/n.$$

The *p-adic exponential function*, denoted $\exp_p$, is defined to be the function

$$\exp_p(X) : D(p^{-1/(p-1)^-}) \to \Omega, \quad \text{defined by } \exp_p(X) = \sum_{n=0}^{\infty} X^n/n!.$$

These p-adic analogs of log and exp have many (though not all) of the properties familiar to us from classical mathematics.

Theorem 2.39. (i) $\log_p(1+x)$ *converges for* $x \in D(1^-)$, *and* $\exp_p(x)$ *converges for* $x \in D(p^{-1/(p-1)^-})$.
(ii) $\log_p(1+X) + \log_p(1+Y) = \log_p\Big((1+X)(1+Y)\Big)$, *and* $\exp_p(X)\exp_p(Y) = \exp_p(X+Y)$.
(iii) $\log_p(1 + \exp_p(x) - 1) = x$, *and* $\exp_p\big(\log_p(1+x)\big) = 1 + x$ *for* $x \in D(p^{-1/(p-1)^-})$.

Proof. (Sketch.) For the proof of (i), see Examples 2.36 and 2.37, respectively. For (ii), we simply manipulate power series. For $\exp_p(X)$, let $x, y \in D(p^{-1(p-1)^{-}})$. Then

$$\begin{aligned}
\exp_p(x+y) &= \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{n!} \frac{n!}{(n-k)k!} x^{n-k} y^k = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{x^{n-k}}{(n-k)!} \frac{y^k}{k!} \\
&= \Big(\sum_{n=0}^{\infty} \frac{x^m}{m!} \Big) \Big(\sum_{k=0}^{\infty} \frac{y^k}{k!} \Big) = \exp_p(x) \exp_p(y).
\end{aligned}$$

The proof for $\log_p(1+X)$ is similar. We omit the proof of part (iii), and refer the reader to [3, pp. 117 – 118] or [2, pp. 79 – 81]. □

We finish this section by introducing a function $\Upsilon(X,Y) \in \Omega[[X,Y]]$ which will play a crucial role in the proof of our main theorem. To understand it, note that the expression $(1+Y)^X$ should be understood to mean $\exp_p\big(X \log_p(1+Y)\big)$.

Definition 2.40. Define $\Upsilon(X,Y) \in \mathbb{Q}[[X,Y]]$ by

$$\Upsilon(X,Y) = (1+Y)^X \prod_{i \geq 1} (1+Y^{p^i})^{(X^{p^i} - X^{p^{i-1}})/p^i}.$$

Note that we need only finitely many terms in the above product to obtain the coefficient of $X^n Y^m$, so that $\Upsilon(X,Y)$ is a well-defined infinite series $\sum a_{m,n} X^n Y^m \in 1 + X\mathbb{Q}_p[[X,Y]] + Y\mathbb{Q}_p[[X,Y]]$. The series Υ will prove useful later, in Lemma 3.6, to establish a certain identity of exponentials.

Proposition 2.41. *The infinite series* $\Upsilon(X,Y) = \sum a_{m,n} X^n Y^m \in 1 + X\mathbb{Q}_p[[X,Y]] + Y\mathbb{Q}_p[[X,Y]]$ *has coefficients* $a_{m,n} \in \mathbb{Z}_p$.

Proof. Omitted. See [2, p. 95]. □

Chapter 3

Traces, Linear Maps, and Linear Operators

3.1 Characters and Lifts

We begin with the following definition.

Definition 3.1. Let G be a finite group. Let $\Omega^\times$ denote the multiplicative group of nonzero numbers in Ω. Then an Ω-*valued character* of G is a homomorphism $\psi : G \to \Omega^\times$.

Note that since G is finite, we have $\psi(a)^{\#G} = 1$ for all $a \in G$. Thus the image of G under a character is contained in the set of roots of unity in Ω.

Definition 3.2. Let $\mathbb{F}_q$ be a finite field with $q = p^s$ elements. For any $a \in \mathbb{F}_q$, we define the *trace* of a to be

$$\operatorname{Tr} a = a + a^p + a^{p^2} + \ldots + a^{p^{s-1}}.$$

Remark 3.3. We can give an interpretation of the trace in terms of Galois Theory. From Fact A.10, we know that $\operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ consists entirely of automorphisms of the form $\sigma_i(a) = a^{p^i}$, so that

$$\operatorname{Tr} a = \sum_{\sigma \in \operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \sigma(a).$$

Proposition 3.4. *Let $\varepsilon \in \Omega$ be a p^{th} root of unity. Let p be prime, let $s \geq 1$ be an integer, and let $q = p^s$. For any $a \in \mathbb{F}_p$, the map $a \mapsto \varepsilon^{\operatorname{Tr} a}$ is an Ω-valued character of the additive group of $\mathbb{F}_q$.*

Proof. Let $\Gamma = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. By Remark 3.3 and the fact that $\mathrm{Frob}_p \in \Gamma$, we have

$$(\operatorname{Tr} a)^p = \mathrm{Frob}_p(\operatorname{Tr} a) = \sum_{\sigma\in\Gamma} \mathrm{Frob}_p(\sigma(a)) = \sum_{\sigma\in\Gamma} \sigma(a) = \operatorname{Tr} a,$$

so that $\operatorname{Tr} a \in \mathbb{F}_p$. Also, we have

$$\operatorname{Tr}(a+b) = \sum_{\sigma\in\Gamma} \sigma(a+b) = \sum_{\sigma\in\Gamma} \sigma(a) + \sigma(b) = \operatorname{Tr}(a) + \operatorname{Tr}(b),$$

so that $a + b \mapsto \varepsilon^{\operatorname{Tr}(a+b)} = \varepsilon^{\operatorname{Tr} a + \operatorname{Tr} b} = \varepsilon^{\operatorname{Tr} a} \cdot \varepsilon^{\operatorname{Tr} b}$. □

Our goal for the rest of this section will be to find a p-adic power series whose evaluation at the Teichmüller representative $t \in \Omega$ of a, is equal to $\varepsilon^{\operatorname{Tr} a}$. Later on, we will use this Teichmüller lifting to establish a nice relationship between a polynomial f and the sequence $\{N_s\}_{s\geq 1}$ described in Section 3 of Chapter 1.

Fix a primitive p^{th} root of unity $\varepsilon \in \Omega$, and let $\lambda = \varepsilon - 1$.

Proposition 3.5. $\mathrm{ord}_p\, \lambda = 1/(p-1)$.

Proof. Since ε is a root of $x^{p-1} + \ldots + x + 1 = \frac{x^p - 1}{x-1}$, we see that λ is a root of

$$f(x) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1} x^{p-2} + \ldots + \binom{p}{2} x + \binom{p}{1}.$$

Case 1. If $|\lambda|_p > |p|_p^{1/(p-1)}$, then $|\lambda|_p^{p-1} > |p|_p |\lambda|_p^i$ for all $0 \leq i \leq p-2$. Then, by the Isosceles Triangle Principle, $|f(\lambda)|_p = |\lambda|_p^{p-1} \neq 0$, a contradiction.

Case 2. If $|\lambda|_p < |p|_p^{1/(p-1)}$, then $|\lambda|_p^{p-1} < |p|$, and $|p|_p |\lambda^i|_p < |p|_p$ for all $1 \leq i \leq p-2$. So $|f(\lambda)|_p = |p|_p \neq 0$, again a contradiction.

Therefore, $|\lambda|_p = |p|_p^{1/(p-1)}$, i.e., $\mathrm{ord}_p\, \lambda = 1/(p-1)$. □

We now seek a p-adic expression for

$$(1+\lambda)^{t + t^p + t^{p^2} + \ldots + t^{p^{s-1}}} = \varepsilon^{\operatorname{Tr} a}.$$

Ideally, we would like a function Θ such that $\Theta(T) = \varepsilon^T$, to get

$$\Theta(t)\Theta(t^p) \cdots \Theta(t^{p^{s-1}}) = \varepsilon^{t + t^p + \cdots + t^{p^{s-1}}} = \varepsilon^{\operatorname{Tr} a}.$$

Unfortunately, it is not even clear what ε^T would mean. Instead, we define a slightly more complicated function, but one that actually does the trick.

Recall the series $\Upsilon(X,Y) \in \mathbb{Q}[[X,Y]]$, introduced in Section 4 of Chapter 2, and given by

$$\Upsilon(X,Y) = (1+Y)^X \prod_{j\geq 1} (1+Y^{p^j})^{(X^{p^j}-X^{p^{j-1}})/p^j}.$$

We consider $\Upsilon(X,Y)$ as a series in X with Y fixed, so that

$$\Upsilon(X,Y) = \sum_{n=0}^{\infty} \bigl(X^n \sum_{m=n}^{\infty} a_{m,n} Y^m\bigr), \quad a_{m,n} \in \mathbb{Z}_p,$$

where we use the fact that $\Upsilon(X,Y)$ is a product of power series, each of which has *its* coefficients $a_{m,n} = 0$ for $m < n$. We now set

$$\Theta(T) = \Upsilon(T,\lambda) = \sum_{n=0}^{\infty} a_n T^n,$$

where $a_n = \sum_{m=n}^{\infty} a_{m,n}\lambda^m$. Since λ^n divides each term of a_n and $a_{m,n} \in \mathbb{Z}_p$, we have $\operatorname{ord}_p a_n \geq n/(p-1)$. Thus, in particular, $\Theta(t)$ converges for $t \in D(p^{-1/(p-1)^-})$.

Lemma 3.6. *Let p be prime, let $s \geq 1$ be an integer, and let $q = p^s$. Let $a \in \mathbb{F}_q$, and let $t \in \Omega$ be the corresponding Teichmüller representative. Then*

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

Proof. We begin by observing that the following identity holds in $\Omega[[Y]]$:

$$\Upsilon(t,Y)\Upsilon(t^p,Y)\cdots\Upsilon(t^{p^{s-1}},Y) = (1+Y)^{t+t^p+t^{p^2}+\ldots+t^{p^{s-1}}}.$$

To see this, note that after cancellation, the left hand side is

$$(1+Y)^{t+t^p+\ldots+t^{p^{s-1}}}(1+Y^p)^{(t^{p^s}-t)/p}(1+Y^{p^2})^{(t^{p^{s+1}}-t^p)/p^2}(1+Y^{p^3})^{(t^{p^{s+2}}-t^{p^2})/p^3}\cdots.$$

But $t^{p^s} = t$, leaving $(1+Y)^{t+t^p+t^{p^2}+\ldots+t^{p^{s-1}}}$ as desired. Substituting $Y = \lambda$ gives

$$\Theta(t)\Theta(t^p)\cdots\Theta(t^{p^{s-1}}) = (1+\lambda)^{t+t^p+\ldots+t^{p^{s-1}}} = \varepsilon^{\operatorname{Tr} a}. \qquad \square$$

Thus, given a field $\mathbb{F}_q$ with $q = p^s$ elements, and $t \in \Omega$ the Teichmüller representative of $a \in \mathbb{F}_q$, we have found a p-adic power series $\Theta(T)\Theta(T^p)\cdots\Theta(T^{p^{s-1}})$ which gives $\varepsilon^{\operatorname{Tr} a}$ when evaluated at t. Moreover, since our lifting Θ converges for $t \in D(p^{-1/(p-1)^-})$, we have convergence on some disc in Ω containing the closed unit disc. This is especially important because we will be working with the Teichmüller representatives, which have absolute value 1.

3.2 Linear Operators and Traces

Throughout this section, fix $n \geq 1$ an integer.

Definition 3.7. We denote by R the ring of formal power series in n indeterminates over Ω:

$$R = \Omega[[X_1, X_2, \ldots, X_n]].$$

Given $u = (u_1, \ldots, u_n) \in \mathbb{N}^n$, we use the notation $X^u = X_1^{u_1} X_2^{u_2} \cdots X_n^{u_n}$. Furthermore, for $q \in \mathbb{Z}^+$, we write $qu = (qu_1, \ldots, qu_n)$. (The q's we will later be considering will be of the form $q = p^s$ for p prime, but the following definitions make sense for any positive integer q.) Let U be the set of all ordered n-tuples of nonnegative integers, so that we can characterize R by

$$R = \Big\{ \sum_{u \in U} a_u X^u \mid a_u \in \Omega \Big\}.$$

Under this characterization, we can thus view R as a vector space over Ω.

We now define three linear maps over Ω from R to itself that will be of importance throughout the proof of Dwork's Theorem.

Definition 3.8. For each $G \in R$ we define a linear map, also denoted $G : R \to R$, by $r \mapsto Gr$. For each $q \in \mathbb{Z}^+$ we define a linear map $T_q : R \to R$ by

$$r = \sum_{u \in U} a_u X^u \mapsto T_q(r) = \sum_{u \in U} a_{qu} X^u.$$

Finally, we define $\Psi_{q,G} = T_q \circ G : R \to R$.

In order to get a better feel for what is going on with the map $\Psi_{q,G}$, we have the following example.

Example 3.9. Let $G = \sum_{w \in U} g_w X^w$. Then

$$\Psi_{q,G}(X^u) = T_q\Big(\sum_{u \in U} g_w X^{w+u}\Big) = T_q\Big(\sum_{w \in U} g_{w-u} X^w\Big) = \sum_{v \in U} g_{qv-u} X^v,$$

where we understand g_u to be 0 if not all coordinates of u are nonnegative.

Proposition 3.10. *Let* $G(x) = \sum_{v \in U} g_v x^v \in R$, *and define* $G_q(X) = G(X^q) = \sum_{v \in U} g_v X^{qv}$. *Then*

$$G \circ T_q = T_q \circ G_q = \Psi_{q,G_q}.$$

Proof. Given $r \in R$, write $r = \sum_{u \in U} a_u X^u$. Then $T_q(r) = \sum_{u \in U} a_{qu} X^u$, and hence

$$G\Big(T_q(r)\Big) = \Big(\sum_{v \in U} g_v X^v\Big)\Big(\sum_{u \in U} a_{qu} X^u\Big) = \sum_{w \in U}\Big(\sum_{v \in U} a_{q(v-w)} g_v\Big) X^w,$$

where we have substituted $w = u + v$. (As before, we understand a_u to be 0 if any coordinates of u are negative.)

On the other hand, consider

$$G_q(r) = \Big(\sum_{v \in U} g_v X^{qv}\Big)\Big(\sum_{u \in U} a_u X^u\Big) = \sum_{w \in U}\Big(\sum_{v \in U} g_v a_{w-qv}\Big) X^w.$$

Let $b_w = \sum_{v \in U} g_v a_{w-qv}$. Note that $b_w \in \Omega$ since it is a finite sum. Thus,

$$T_q\Big(G_q(r)\Big) = \sum_{w \in U} b_{qw} X^w = \sum_{w \in U}\Big(\sum_{v \in U} g_v a_{qv-qw}\Big) X^w = \sum_{w \in U}\Big(\sum_{v \in U} a_{q(v-w)} g_v\Big) X^w = G\Big(T_q(r)\Big). \quad \square$$

Next, we define a particular set $R_0 \subset R$ with some nice properties.

Definition 3.11. Define $\|\cdot\|$ on U by $\|u\| = \sum_{i=1}^{n} u_i$. Now let

$$R_0 = \left\{ G = \sum_{w \in U} g_w X^w \in R \;\middle|\; \text{for some } M > 0,\ \operatorname{ord}_p g_w \geq M\|w\| \text{ for all } w \in U \right\}.$$

Thus, R_0 consists of power series whose coefficients approach zero particularly rapidly in Ω. We will see in Proposition 4.1 that given a in the closed disc of radius 1 about the origin, $\Theta(aX^w) \in R_0$. This will be especially useful to us in light of the following proposition.

Proposition 3.12. *R_0 is closed under multiplication and under the map $T_q : G \mapsto G_q$.*

Proof. Closure under multiplication is clear. For closure under T_q, suppose $G = \sum_{w \in U} g_w x^w \in R_0$. Then there is some $N > 0$ such that $\operatorname{ord}_p g_w \geq N\|w\|$ for all $w \in U$. Note that $\|qw\| = q\|w\|$. Let $M = N/q > 0$. Then for all $w \in U$,

$$\operatorname{ord}_p g_{qw} \geq N\|w\| = Mq\|w\| = M\|qw\|. \qquad \square$$

Definition 3.13. Let V be a finite dimensional vector space over a field K, and let $\{a_{ij}\}$ denote the matrix of a map $A : V \to V$ with respect to a basis. Then the trace of A is defined to be

$$\operatorname{Tr} A = \sum_{i \geq 0} a_{ii}.$$

Note that given this definition, the trace of A is independent of our choice of basis. However, since R is an *infinite* dimensional vector space over Ω, we will want to have a more general definition of trace.

Definition 3.14. Let $\Lambda : R \to R$ be a linear operator such that $\Lambda(X^u) = \sum_{v \in U} a_{uv} X^v$ for all $u \in U$. We say that Λ is *admissible* if for all $h(X) = \sum_{u \in U} b_u X^u \in R_0$, we have that $\sum_{u \in U} a_{uv} b_u$ converges, and $\Lambda(\sum_{u \in U} b_u X^u) = \sum_{u \in U} b_u \Lambda(X^u)$.

Definition 3.15. Let $\Lambda : R_0 \to R_0$ be admissible. Define $a_{uv} \in \Omega$ for each $u, v \in U$ by $\Lambda(X^u) = \sum_{v \in U} a_{uv} X^v$. We then define the *trace* of Λ, denoted $\operatorname{Tr}(\Lambda)$, to be $\sum_{u \in U} a_{uu}$, if this sum converges in Ω.

Remark 3.16. We see from Example 3.9 that $\Psi = \Psi_{q,G}$ fits the conditions of Definition 3.15 and sends elements X^u to $\sum_{v \in U} g_{qv-u} X^v$. Hence

$$\operatorname{Tr}(\Psi) = \sum_{u \in U} g_{qu-u} = \sum_{u \in U} g_{(q-1)u},$$

which clearly converges for $G \in R_0$.

Using the above value for $\operatorname{Tr}(\Psi)$, we can now state and prove our main lemma for this section.

Lemma 3.17. *Let p be prime, let $r \geq 1$ be an integer, and let $q = p^r$. Let $G \in R_0$, let $\Psi = \Psi_{q,G}$, and let $s \geq 1$. Then $\operatorname{Tr}(\Psi^s)$ converges, and*

$$(q^s - 1)^n \operatorname{Tr}(\Psi^s) = \sum_{\substack{x \in \Omega^n \\ x^{q^s-1}=1}} G(x)G(x^q)G(x^{q^2}) \cdots G(x^{q^{s-1}}),$$

where we use the notation $x = (x_1, \ldots, x_n) \in \Omega^n$, and $x^{q^s-1} = 1$ to mean $x_j^{q^s-1} = 1$ for all $j = 1, 2, \ldots, n$.

Proof. We begin with the following claim.

Claim 3.18. *Let $s \geq 1$ be an integer. Let $G \in R_0$, and let $G_q(X) = G(X^q)$. Then*

$$\Psi_{q,G}^s = \Psi_{q^s, G \cdot G_q \cdots G_{q^{s-1}}}.$$

Proof. We proceed by induction on s. When $s = 1$ this is obvious. Suppose $\Psi_{q,G}^s = \Psi_{q^s, G \cdot G_q \cdots G_{q^{s-1}}}$ and consider $\Psi_{q,G}^{s+1}$. By our inductive hypothesis, we have

$$\Psi_{q,G}^{s+1} = \Psi_{q,G}^s \circ \Psi_{q,G} = \Psi_{q^s, G \cdot G_q \cdots G_{q^{s-1}}} \circ \Psi_{q,G} = T_{q^s} \circ \big(G \cdot G_q \cdots G_{q^{s-1}}\big) \circ T_q \circ G. \tag{3.1}$$

By Proposition 3.10, $G_{q^{s-1}} \circ T_q = T_q \circ (G_{q^{s-1}})_q = T_q \circ G_{q^{s-1} \cdot q} = T_q \circ G_{q^s}$. Thus, we move T_q to the left s times, transforming (3.1) to

$$T_{q^s} \circ \big(G \cdot G_q \cdots G_{q^{s-1}}\big) \circ T_q \circ G = T_{q^s} \circ T_q \circ \big(G_q \cdot G_{q^2} \cdots G_{q^s} \cdot G\big) = T_{q^{s+1}} \circ \big(G \cdot G_q \cdots G_{q^s}\big). \quad \square$$

To prove the Lemma, let $H = G \cdot G_q \cdots G_{q^{s-1}} = \sum_{w \in U} h_w X^w$. Since $G \in R_0$ and R_0 is closed under the map $G \to G_q$, we have $G_{q^i} \in R_0$ for each $i = 1, \ldots, s-1$. Since R_0 is also closed under multiplication, we have $H \in R_0$. Therefore, we know from Claim 3.18 and Example 3.9 that

$$\Psi^s(X^u) = \Psi_{q,G}^s(X^u) = \Psi_{q^s,H}(X^u) = \sum_{u \in U} h_{q^s v - u} X^v.$$

Thus, as in Remark 3.16 with h in place of g and q^s in place of q, we see that

$$\operatorname{Tr}(\Psi^s) = \sum_{u \in U} h_{q^s u - u} = \sum_{u \in U} h_{(q^s-1)u}.$$

Since $H \in R_0$, we know that $|h_i|_p \to 0$ as $i \to \infty$. Thus the trace converges.

Fix $w = (w_1, \dots, w_n) \in U$. By Lemma 1.6, we note that for each $i = 1, 2, \dots, n$, we have

$$\sum_{\substack{x_i \in \Omega \\ x_i^{q^s-1}=1}} x_i^{w_i} = \begin{cases} (q^s - 1) & \text{if } (q^s-1)|w_i \text{ for all } i = 1, \dots, n \\ 0 & \text{otherwise.} \end{cases}$$

Thus,

$$\sum_{\substack{x \in \Omega^n \\ x^{q^s-1}=1}} x^w = \prod_{i=1}^{n} \Big(\sum_{x_i^{q^s-1}=1} x_i^{w_i} \Big) = \begin{cases} (q^s - 1)^n & \text{if } (q^s-1)|w_i \text{ for all } i = 1, \dots, n \\ 0 & \text{otherwise.} \end{cases}$$

Hence,

$$\sum_{\substack{x \in \Omega^n \\ x^{q^s-1}=1}} H(x) = \sum_{w \in U} h_w \sum_{\substack{x \in \Omega^n \\ x^{q^s-1}=1}} x^w = (q^s-1)^n \sum_{u \in U} h_{(q^s-1)u} = (q^s-1)^n \operatorname{Tr}(\Psi^s). \qquad \square$$

The above lemma will play a crucial role in proving the main theorem of Chapter 4. Having successfully extended the definition of a trace to handle infinite vector spaces, we will now need a final section in order to similarly extend the definition of a determinant.

3.3 Determinants

Let K be a field and let A be an $r \times r$ matrix with entries $a_{ij} \in K$. Let T be an indeterminate, and let 1 denote the $r \times r$ identity matrix I_r. Then $1 - AT$ is an $r \times r$ matrix with entries in $K[T]$, and

$$\det(1 - AT) = \sum_{m=0}^{r} b_m T^m,$$

with

$$b_m = (-1)^m \sum_{\substack{1 \le u_1 < \cdots < u_m \le r \\ \sigma \in S(\{u_1, \dots, u_m\})}} \operatorname{sgn}(\sigma) a_{u_1,\sigma(u_1)} a_{u_2,\sigma(u_2)} \cdots a_{u_m,\sigma(u_m)},$$

where $S(X)$ is the group of permutations on X.

We wish to extend the above discussion to linear operators on R. Suppose that $\Lambda : R_0 \to R_0$ is an admissible linear operator. Motivated by the discussion of $\det(1 - AT)$ above, we define the expression $\det(1 - \Lambda T)$ to be

$$\det(1 - \Lambda T) = \sum_{m=0}^{\infty} b_m T^m \in \Omega[[T]],$$

where

$$b_m = (-1)^m \sum_{\substack{1\le u_1<\cdots<u_m \\ \sigma\in S(\{u_1,\ldots,u_m\})}} \operatorname{sgn}(\sigma) a_{u_1,\sigma(u_1)} a_{u_2,\sigma(u_2)} \cdots a_{u_m,\sigma(u_m)}.$$

This definition of $\det(1-\Lambda T)$ still makes sense as a formal power series in $\Omega[[T]]$, as long as the expression for each b_m converges.

Let $G = \sum_{w\in U} g_w T^w \in R_0$, so that for some M we have $\operatorname{ord}_p g_w \ge M\|w\|$ for all $w \in U$. Recall that Ψ sends elements X^u to $\sum_{v\in U} g_{qv-u}X^v$. We then have

$$\operatorname{ord}_p(g_{q\sigma(u_1)-u_1} g_{q\sigma(u_2)-u_2} \cdots g_{q\sigma(u_m)-u_m}) \ge M\sum_{i=1}^m \|q\sigma(u_i)-u_i\| = M(q-1)\sum_{i=1}^m \|u_i\|.$$

Thus, $\operatorname{ord}_p b_m \to \infty$ as $m \to \infty$. More precisely, order U according to modified lexographic order, i.e., define $u \ge w$ if $\|u\| > \|w\|$, or if $\|u\| = \|w\|$ and $u_1 > w_1$, or if $\|u\| = \|w\|$ and $u_1 = w_1$ and $u_2 > w_2$, etc. Let $V = \{u \in U \mid w \ge u\}$. Then $\frac{1}{\#V}\sum_{u\in V} \|u_i\| \to \infty$ as $\#V \to \infty$. Hence

$$\frac{1}{m}\operatorname{ord}_p b_m \to \infty \text{ as } m \to \infty,$$

so that

$$\det(1-\Psi T) = \sum_{m=0}^{\infty} b_m T^m$$

is well-defined and has an infinite radius of convergence.

Proposition 3.19. *Let A be a square matrix with entries in Ω. Then we have the following identity of formal power series in $\Omega[[T]]$:*

$$\det(1-AT) = \exp_p\Big(-\sum_{s=1}^{\infty} \operatorname{Tr}(A^s)T^s/s\Big).$$

Proof. Recall that the determinant and trace are invariant under a change of basis. Since Ω is an algebraically closed field, A is conjugate to an upper triangular matrix, for example, its Jordan Canonical form [6, Chapter 7]. That is, there is an invertible matrix C such that CAC^{-1} is upper triangular. Without loss of generality, then, we may assume that A, and hence A^s for each $s \ge 1$, is upper triangular. Thus,

$$\det(1 - AT) = \prod_{i=1}^{r}(1 - a_{ii}T) = \prod_{i=1}^{r}\exp_p\Big(\log_p(1 - a_{ii}T)\Big) = \prod_{i=1}^{r}\exp_p\Big(-\sum_{s=1}^{\infty}(a_{ii}T)^s/s\Big)$$

$$= \exp_p\Big(-\sum_{s=1}^{\infty}\sum_{i=1}^{r} a_{ii}^s T^s/s\Big) = \exp_p\Big(-\sum_{s=1}^{\infty}\mathrm{Tr}(A^s)T^s/s\Big) \qquad \Box$$

We now generalize Proposition 3.19. Fix an admissible linear operator $\Lambda : R_0 \to R_0$ given by $\Lambda : X^u \mapsto \sum_{v \in U} a_{uv}X^v$.

Definition 3.20. List the elements of U in order as $u_1 < u_2 < \dots$ according to graded lexicographic order. For $\Lambda : R_0 \to R_0$ admissible as above, and $n \geq 1$, we define A_n to be the matrix $\{a_{u_i u_j}\}_{1 \leq i,j \leq n}$.

Remark 3.21. Intuitively, what we are doing here is thinking of Λ as representing an "infinite matrix" that maps elements from R_0 to R_0. We can then think of A_n as the $n \times n$ matrix formed from the upper left-hand corner of our infinite matrix. The hope is that for sufficiently large n, we can somehow capture enough information about Λ to let us carry out our analysis using regular (i.e., finite) matrices.

Definition 3.22. Let B be any matrix with coefficients in Ω. Then we define $|B| = \max_{i,j} |(B)_{ij}|_p$. Similarly, for $\Lambda : R_0 \to R_0$ admissible, we define $|\Lambda| = \max_{i,j} |a_{ij}|$, if this maximum exists.

Definition 3.23. Let $\Lambda : R_0 \to R_0$ be admissible, and suppose for any $\delta > 0$ there is an integer L such that for all i we have $|a_{i\ell}|_p, |a_{\ell i}|_p < \delta$ whenever $\ell \geq L$. Then we say Λ *converges*, or *is convergent.*

Note that if Λ is convergent in the above sense, then this implies that $\mathrm{Tr}(\Lambda)$ exists.

Proposition 3.24. *Suppose Λ converges. Then for all $\varepsilon > 0$, there exists an integer $N \geq 1$ such that for all $n \geq N$, all coefficients of the power series* $\det(1 - \Lambda T) - \det(1 - A_nT) \in \Omega[[T]]$ *have p-adic absolute value less than ε.*

Proof. Note first that $|\Lambda|$ exists, and let $\mathcal{M} = |\Lambda|$. By definition, the coefficient of T^m in $\det(1-\Lambda T)$ is

$$\hat{b}_m = (-1)^m \sum_{\substack{1 \le u_1 < \cdots < u_m \\ \sigma \in S(\{u_1,\ldots,u_m\})}} \operatorname{sgn}(\sigma) \prod_{i=1}^{\infty} a_{u_i,\sigma(u_i)}.$$

Similarly, the coefficient of T^m in $\det(1 - A_n T)$ is

$$b_m = (-1)^m \sum_{\substack{1 \le u_1 < \cdots < u_m \le n \\ \sigma \in S(\{u_1,\ldots,u_m\})}} \operatorname{sgn}(\sigma) a_{u_1,\sigma(u_1)} a_{u_2,\sigma(u_2)} \cdots a_{u_m,\sigma(u_m)}.$$

Therefore,

$$\hat{b}_m - b_m = (-1)^m \sum_{\substack{u_1,\ldots,u_{m-1} \ge 1 \\ u_m > n \\ \sigma \in S(\{u_1,\ldots,u_m\})}} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{u_i,\sigma(u_i)}.$$

But $\Big|\prod_{i=1}^{m-1} a_{u_i,\sigma(u_i)}\Big|_p \le \mathcal{M}^{m-1}$. Given $\varepsilon > 0$, the convergence of Λ implies that we can find L such that for all $n \ge L$ and all i, we have $|a_{ni}|_p < \varepsilon/\mathcal{M}^{m-1}$. Given $n \ge L$, then for all $u_1, \ldots, u_{m-1} \ge 1$ and $u_m > n$, we have

$$\Big|\prod_{i=1}^{m} a_{u_i,\sigma(u_i)}\Big|_p = \Big|a_{u_m,\sigma(u_m)}\Big|_p \cdot \Big|\prod_{i=1}^{m-1} a_{u_i,\sigma(u_i)}\Big|_p < \frac{\varepsilon}{\mathcal{M}^{m-1}} \cdot \mathcal{M}^{m-1} = \varepsilon.$$

Thus, since $|\cdot|_p$ is non-Archimedean,

$$|\hat{b}_m - b_m|_p \le \max_{\substack{u_1,\ldots,u_{m-1} \ge 1 \\ u_m > n \\ \sigma \in S(\{u_1,\ldots,u_m\})}} \Big|\prod_{i=1}^{m} a_{u_i,\sigma(u_i)}\Big|_p < \varepsilon. \qquad \square$$

Proposition 3.25. *Let $\Lambda : R_0 \to R_0$ converge and be admissible, and let $\mathcal{M} = |\Lambda|$. Then for all $\varepsilon > 0$, there is an integer $N \ge 1$ such that for all integers $n \ge N$ and $s \ge 1$, we have $|\operatorname{Tr}(\Lambda^s) - \operatorname{Tr}\big((A_n)^s\big)|_p < \mathcal{M}^{s-1}\varepsilon$.*

Proof. We begin with a claim.

Claim 3.26. *For all $\varepsilon > 0$, there is an integer $N \ge 1$ such that $|\Lambda^s - (A_n)^s| \le \mathcal{M}^{s-1}\varepsilon$ for all $n \ge N$.*

Proof. We proceed by induction on s. The base case of $s = 1$ is trivial. For our inductive hypothesis, suppose the claim holds for s. Observe that $|(A_n)^s| \leq |\Lambda^s| \leq M^s$ for all n. Thus,

$$\begin{aligned}|\Lambda^{s+1} - (A_n)^{s+1}| &= |\Lambda^s\Lambda - (A_n)^s A_n| = |\Lambda^s\Lambda - \Lambda^s A_n + \Lambda^s A_n - (A_n)^s A_n| \\ &= |\Lambda^s(\Lambda - A_n) + A_n(\Lambda^s - (A_n)^s)| \\ &\leq \max\{|\Lambda^s| \cdot |\Lambda - A_n|, |A_n| \cdot |\Lambda^s - (A_n)^s|\} \leq M^s\varepsilon,\end{aligned}$$

where the triangle inequality for operators is immediate from that for Ω and by Definition 3.22. □

Thus, given $\varepsilon > 0$, we choose N as in Claim 3.26. Then for all $n \geq N$, we have

$$\left|\operatorname{Tr}(\Lambda^s) - \operatorname{Tr}\left((A_n)^s\right)\right|_p \leq |\Lambda^s - (A_n)^s| \leq M^{s-1}\varepsilon,$$

where the last inequality follows Claim 3.26. □

Ultimately we will want to show that $\exp_p\left(-\sum_{s=1}^{\infty}\operatorname{Tr}(\Lambda^s)T^s/s\right)$ and $\exp_p\left(-\sum_{s=1}^{\infty}\operatorname{Tr}\left((A_n)^s\right)T^s/s\right)$ have p-adically close coefficients. Thus, we begin by showing the following inequality over a disc.

Proposition 3.27. *Let Λ be as above with $\mathcal{M} = |\Lambda|$. Let $\varepsilon > 0$. Then for $|t|_p \leq 1/(p\mathcal{M})$ and n sufficiently big, we have*

$$\left|-\sum_{s=1}^{\infty}\frac{\operatorname{Tr}(\Lambda^s)}{s}t^s - \sum_{s=1}^{\infty}\frac{\operatorname{Tr}((A_n)^s)}{s}t^s\right|_p < \varepsilon.$$

Proof. Observe that $|p^s/s|_p \leq 1$ for all integers $s \geq 1$. Let $\varepsilon > 0$. Then there exists an integer N such that for all $n \geq N$,

$$\begin{aligned}\left|-\sum_{s=1}^{\infty}\frac{\operatorname{Tr}(\Lambda^s)}{s}T^s - \sum_{s=1}^{\infty}\frac{\operatorname{Tr}((A_n)^s)}{s}T^s\right|_p &= \left|\sum_{s=1}^{\infty}\operatorname{Tr}(\Lambda^s) - \operatorname{Tr}((A_n)^s)\right|_p\left|T^s/s\right|_p \\ &\leq \mathcal{M}^{s-1}\varepsilon \cdot |p^s/s|_p/\mathcal{M}^s \leq \varepsilon/\mathcal{M},\end{aligned}$$

where the first inequality is by Proposition 3.25. Thus we can replace ε with $\varepsilon\mathcal{M}$ to obtain the desired result. □

Definition 3.28. Let $f = \sum_{i=0}^{\infty} a_i T^i$ and let $g = \sum_{i=0}^{\infty} b_i T^i$ be power series in $\Omega[[T]]$. Given $r > 0$, we define

$$\|f - g\|_r = \max_{n\geq 0}\{|a_n - b_n|_p r^n\}.$$

Thus, if f and g converge on the closed disc $D(r)$, then for all $x \in D(r)$,

$$|f(x) - g(x)|_p = \Big| \sum_{i=1}^{\infty} (a_n - b_n) x^n \Big|_p \leq \|f - g\|_r.$$

Lemma 3.29. *Suppose* $\lim_{n\to\infty} f_n = f$ *in* $\Omega[[T]]$ *and* $g \in \Omega[[T]]$. *Suppose further there are radii* $r, \rho > 0$ *such that:*

(1) g *converges on* $D(\rho)$,

(2) f *and* f_n *converge on* $D(r)$, *and*

(3) $\|f\|_r \leq \rho$ *and* $\|f_n\|_r \leq \rho$,

where (2) and (3) hold for n *sufficiently large. Then* $\lim_{n\to\infty} g \circ f_n = g \circ f$ *with respect to* $\| \cdot \|_r$, *i.e., for all* $\varepsilon > 0$, *there exists* N *such that for all* $n \geq N$, *we have* $\|g \circ f_n - g \circ f\|_r < \varepsilon$.

Proof. Write $g(T) = \sum_{n=0}^{\infty} b_n T^n$. Pick $N \geq 1$ so that for all $m \geq N$, we have that f and f_n converge on $D(r)$ with $\|f\|_r, \|f_n\|_r \leq \rho$. Then for any $m \geq N$,

$$\|g(f_m) - g(f)\|_r = \| \sum_{n=0}^{\infty} b_n \big(f^n - f_m^n\big) \|_r = \| \sum_{n=0}^{\infty} b_n \big(f - f_m\big)(f^{n-1} + f^{n-2} f_m + \cdots + f {f_m}^{n-2} + {f_m}^{n-1}) \|_r.$$

But

$$\|b_n\big(f^{n-1} + \cdots + {f_m}^{n-1}\big)\|_r \leq L, \quad \text{where} \quad L = \max_{n\geq 1} \big\{ \max_m \{\|f\|_r, \|f_m\|_r\}^{n-1} \cdot |b_n|_p \big\}.$$

Since $g(f)$ and $g(f_m)$ converge, L exists. Hence,

$$\|g(f_m) - g(f)\|_r \leq \|f - f_m\|_r L.$$

Let $\varepsilon > 0$. For sufficiently large m, we have $\|f - f_m\|_r < L/\varepsilon$. Thus $\|g(f_m) - g(f)\|_r < \varepsilon$. □

Corollary 3.30. *Let* $\varepsilon > 0$. *Then there exists an integer* N *such that whenever* $n \geq N$,

$$\Big\| \exp_p \big(- \sum_{s=1}^{\infty} \mathrm{Tr}(\Psi^s) T^s / s\big) - \exp_p \big(- \sum_{s=1}^{\infty} \mathrm{Tr}(A_n^s) T^s / s\big) \Big\|_r < \varepsilon.$$

Proof. Let $\rho = |p|_p^{1/(p-1)}$. Let $f = -\sum_{s=1}^{\infty} \mathrm{Tr}\,\big((\Psi^s)\big) T^s / s$, let $f_m = -\sum_{s=1}^{\infty} \mathrm{Tr}\,\big((A_m)^s\big) T^s / s$, and let $g(T) = \exp(T)$. Since f and f_m converge on some disc $D(r)$ and have zero constant term, there exist N and r so that $\|f\|_r, \|f_m\|_r < \rho$ for m sufficiently large. The corollary then follows from Lemma 3.29. □

We now combine the above results in the following theorem.

Theorem 3.31. *Let $\Psi = \Psi_{q,G}$ for q a prime power and $G \in R_0$. Then the series* $\det(1 - \Psi T)$ *is a well-defined element of $\Omega[[T]]$ with infinite radius of convergence, and we have the following identity of formal power series in $\Omega[[T]]$:*

$$\det(1 - \Psi T) = \exp_p \big(-\sum_{s=1}^{\infty} \mathrm{Tr}(\Psi^s) T^s/s \big).$$

Proof. Take $\varepsilon > 0$. By Proposition 3.24, we can find N_1 such that whenever $n \geq N_1$, the coefficients of $\det(1 - \Psi T) - \det(1 - A_n T)$ have p-adic absolute value less than ε, hence

$$\| \det(1 - \Psi T) - \det(1 - A_n T) \|_r < \varepsilon$$

for any $0 < r < 1$. Note that A_n is a regular (i.e., finite) matrix, giving the strict equality

$$\det(1 - A_n T) = \exp_p \Big(-\sum_{s=1}^{\infty} \mathrm{Tr} \left((A_n)^s) \right) T^s/s \Big)$$

by the discussion at the start of this section. But we know from Corollary 3.30 that we can find N_2 and $r > 0$ such that whenever $n \geq N_2$,

$$\Big\| \exp \Big(-\sum_{s \geq 1} \mathrm{Tr}(\Psi^s) T^s/s \Big) - \exp \Big(-\sum_{s \geq 1} \mathrm{Tr}((A_n)^s) T^s/s \Big) \Big\|_r < \varepsilon.$$

Set $N = \max\{N_1, N_2\}$, so that

$$\Big\| \det(1 - \Psi T) - \exp_p \Big(-\sum_{s=1}^{\infty} \mathrm{Tr}(A^s) T^s/s \Big) \Big\|_r < \varepsilon.$$

Letting ε go to 0, we have that

$$\Big\| \det(1 - \Psi T) - \exp_p \Big(-\sum_{s=1}^{\infty} \mathrm{Tr}(A^s) T^s/s \Big) \Big\|_r = 0.$$

Since $r > 0$, the desired inequality now follows immediately from the definition of $\| \cdot \|_r$. $\square$

Chapter 4

The Zeta-Function is p-adic Meromorphic

We begin by stating and proving the following proposition which will be useful later on. Recall that R_0 was defined in Definition 3.11 and Θ was defined just prior to Lemma 3.6.

Proposition 4.1. *Let $X^w = X_1^{w_1} \cdots X_n^{w_n}$, and let $a \in D(1)$, the closed disc of radius 1 about the origin. Then $\Theta(aX^w) \in R_0$.*

Proof. The result is trivially true if $\|w\| = 0$; so suppose $\|w\| > 0$. Recall $\Theta(T) = \sum_{j=0}^{\infty} a_j T^j$, where $\operatorname{ord}(a_j) \geq j/(p-1)$. Thus,

$$\Theta(aX_1^{w_1} \cdots X_n^{w_n}) = \sum_{j=0}^{\infty} a_j a^j X^{jw} = \sum_{v \in U} g_v X^v,$$

where $g_v = a_j a^j$ when $v = jw$ for some $j \in \mathbb{N}$, and $g_v = 0$ otherwise. Note that $a \in D(1)$ means $|a|_p \leq 1$, i.e., $\operatorname{ord} a \geq 0$. Hence, for $v = jw$,

$$\operatorname{ord}(g_v) = j \cdot \operatorname{ord}(a) + \operatorname{ord}(a_j) \geq \operatorname{ord}(a_j) \geq j/(p-1). \tag{4.1}$$

Note also that $\|v\| = j\|w\|$, so that $j = \|v||/\|w\|$. Combining this with (4.1) yields

$$\operatorname{ord}(g_v) \geq \|v\|/\big(\|w\|(p-1)\big).$$

Let $M = 1/\big(\|w\|(p-1)\big)$. Then $\operatorname{ord}(g_v) \geq M\|v\|$ for $v = jw$, and of course the same inequality holds for v not of this form, since then $g_v = 0$. Hence $\Theta(aX^w) \in R_0$. □

Definition 4.2. A power series in $\Omega[[T]]$ with infinite radius of convergence is said to be *p-adic entire*. The quotient of two p-adic entire functions is said to be *p-adic meromorphic.*

Observe that the product of p-adic entire functions is entire, and thus the product of meromorphic functions is meromorphic.

The following Theorem is the main result of this section.

Theorem 4.3. *Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$. Then $Z(H_f/\mathbb{F}_q; T) \in \mathbb{Z}[[T]] \subset \Omega[[T]]$ is a ratio of entire functions in $1 + T\Omega[[T]]$, and thus is p-adic meromorphic.*

Proof. For the hypersurface H_f defined by $f(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$, we proceed by induction on n, the number of variables. If $n = 0$, then H_f is empty, $N_s = 0$ for all s, the zeta-function is identically 1, and our assertion is trivially true. Now suppose it holds for $1, \ldots, n-1$ variables.

We now set the following definitions.

$$N'_s = \#\{(x_1, \ldots, x_n) \in \left(\mathbb{F}_{q^s}^{\times}\right)^n \mid f(x_1, \ldots, x_n) = 0\},$$

$$Z'(H_f/\mathbb{F}_q; T) = \exp\big(\sum_{s \geq 1} N'_s T^s/s\big).$$

This leads us to the following claim.

Claim 4.4. *It suffices to show that $Z'(H_f/\mathbb{F}_q; T) = \exp(\sum_{s=1}^{\infty} N'_s T^s/s)$ is p-adic meromorphic.*

Proof. Note first that $Z(H_f/\mathbb{F}_q; T) = Z'(H_f/\mathbb{F}_q; T) \cdot \exp(\sum_{s=1}^{\infty}(N_s - N'_s)T^s/s)$. Next, note that the exp factor on the right-hand side is the zeta-function for the (possibly not disjoint) union of the hypersurfaces H_i, where H_i is the common zero set of f and X_i. It is clear that the zeta-function for H_i is the same as that for $\tilde{H}_i$, the zero set of $\tilde{f}_i(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots X_n) = f(X_1, \ldots, X_{i-1}, 0, X_{i+1}, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$. There are then three cases for the zeta-function of these H_i.

Case 1. $H_i = \emptyset$. Then the zeta-function for H_i is 1.

Case 2. H_i is a copy of $\mathbb{A}^{n-1}_{\mathbb{F}_q}$ contained in $\mathbb{A}^n_{\mathbb{F}_q}$. In this case, we have shown explicitly in Example 1.11 that the zeta-function is p-adic meromorphic.

Case 3. H_i is a lower dimensional hypersurface and hence meromorphic by our inductive hypothesis. More generally, given any $i_1, \ldots, i_r$, let $H(i_1, \ldots, i_r)$ be the common zero set of f and $X_{i_1}, \ldots, X_{i_r}$. Then the associated zeta-function is the same as that of $\tilde{H}(i_1, \ldots, i_r) \subseteq \mathbb{A}^{n-r}_{\mathbb{F}_q}$, the zero set of $\tilde{f}_{i_1,\ldots,i_r} \in \mathbb{F}_q[\ldots, \hat{X}_{i_1}, \ldots, \hat{X}_{i_r}, \ldots]$, where $\tilde{f}_{i_1,\ldots,i_r}(x_1, \ldots, x_n)$ is defined to be $f(x_1, \ldots, x_n)$ with $x_{i_1}, \ldots, x_{i_r}$ replaced by 0's. Thus the zeta-function $Z(H(i_1, \ldots, i_r)/\mathbb{F}_q; T)$ is meromorphic by hypothesis.

By the Inclusion/Exclusion Principle, we have

$$N_s - N_s' = \big|\bigcup_i H_i\big| = \sum_{i_1} \big|H_{i_1}\big| - \sum_{i_1 < i_2} \big|H_{i_1} \cap H_{i_2}\big| + \sum_{i_1 < i_2 < i_3} \big|H_{i_1} \cap H_{i_2} \cap H_{i_3}\big| - \ldots \pm \big|\bigcap H_{i_j}\big|.$$

But $H_{i_1} \cap \ldots \cap H_{i_r} = H(i_1, \ldots, i_r)$, so that the associated zeta-function $Z\big(\tilde{H}(i_1, \ldots, i_r)\big)$ is p-adic meromorphic as shown above. Thus, $\exp\Big(\sum_{s=1}^{\infty}(N_s - N_s')T^s/s\Big)$ is a product of p-adic meromorphic functions, and hence meromorphic. □

To prove our theorem for $Z'(H_f/\mathbb{F}_q; T)$, we begin by fixing notation. Let $q = p^r$, and fix an integer $s \geq 1$. For $a \in \mathbb{F}_{q^s}$, let $t \in \Omega$ denote its Teichmüller representative. Given a p^{th} root of unity ε, we know from Lemma 3.6 that we can write:

$$\varepsilon^{\operatorname{Tr} a} = \Theta(t)\Theta(t^p)\Theta(t^{p^2}) \cdots \Theta(t^{p^{rs-1}}).$$

Next we will need to make use of the following claim.

Claim 4.5.

$$\sum_{x \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\operatorname{Tr}(xu)} = \begin{cases} -1, & \textit{if } u \in \mathbb{F}_{q^s}^{\times} \\ q^s - 1, & \textit{if } u = 0. \end{cases}$$

Proof. We will show the equivalent identity

$$\sum_{x \in \mathbb{F}_{q^s}} \varepsilon^{\operatorname{Tr}(xu)} = \begin{cases} 0, & \text{if } u \in \mathbb{F}_{q^s}^{\times} \\ q^s, & \text{if } u = 0, \end{cases}$$

from which the claim follows immediately. Let $S = \sum_{x \in \mathbb{F}_{q^s}} \varepsilon^{\operatorname{Tr}(xu)}$. Now set $y = x - a$, so that

$$S = \sum_{y \in \mathbb{F}_{q^s}} \varepsilon^{\operatorname{Tr}(au+yu)} = \sum_{y \in \mathbb{F}_{q^s}} \varepsilon^{\operatorname{Tr}(au)}\varepsilon^{\operatorname{Tr}(yu)} = \varepsilon^{\operatorname{Tr}(au)} \sum_{y \in \mathbb{F}_{q^s}} \varepsilon^{\operatorname{Tr}(yu)} = \varepsilon^{\operatorname{Tr}(au)} \cdot S. \tag{4.2}$$

If $u = 0$, then $S = \sum_{x \in \mathbb{F}_{q^s}} \varepsilon^0 = q^s$. If $u \neq 0$, we know from Remark A.9 and Claim A.11 that there is an element $b \in \mathbb{F}_{q^s}$ with nonzero trace in $\mathbb{F}_p$. Thus, $\varepsilon^{\mathrm{Tr}(b)} \neq 1$. By equation (4.2), $S = \varepsilon^{\mathrm{Tr}(b)} \cdot S$. Since $\varepsilon^{\mathrm{Tr}(b)} \neq 1$, we have $S = 0$. □

We now consider the sum

$$\sum_{x_0,\ldots,x_n \in \mathbb{F}_{q^s}^\times} \varepsilon^{\mathrm{Tr}(x_0 f(x_1,\ldots,x_n))} = \sum_{x_0 \in \mathbb{F}_{q^s}^\times} \sum_{x_1,\ldots,x_n \in \mathbb{F}_{q^s}^\times} \varepsilon^{\mathrm{Tr}(x_0 f(x_1,\ldots,x_n))} = q^s N_s' - (q^s - 1)^n, \tag{4.3}$$

where the final equality is by Claim 4.5 with $x = x_0$ and $u = f(x_1, \ldots, x_n)$, and by analyzing the following two cases.

Case 1. $f(x_1, \ldots, x_n) = 0$. Summing across all $x_0 \in \mathbb{F}_{q^s}^\times$, this will add $q^s - 1$ to the sum in (4.3). Since this occurs N_s' times, a total of $(q^s - 1)N_s' = q^s N_s' - N_s'$ is contributed to the sum.

Case 2. $f(x_1, \ldots, x_n) \neq 0$. Summing across all $x_0 \in \mathbb{F}_{q^s}^\times$, this will add -1 to the sum in (4.3). This will occur for all but the N_s' points from the first case, thus adding $\big((q^s - 1)^n - N_s'\big)(-1) = N_s' - (q^s - 1)^n$.

We are thus left with $q^s N_s' - N_s' + N_s' - (q^s - 1)^n = q^s N_s' - (q^s - 1)^n$, as claimed in (4.3).

Next, replace the coefficients in $X_0 f(X_1, \ldots, X_n) \in \mathbb{F}_q[X_0, X_1, \ldots, X_n]$ with their Teichmüller representatives. This gives us a new function

$$F(X_0, X_1, \ldots, X_n) = \sum_{i=1}^{N} a_i X^{w_i} \in \Omega[X_0, X_1, \ldots, X_n],$$

where each $a_i \in \Omega$ satisfies $a_i^{q^s} = a_i$, and where $w_i = (w_{i0}, w_{i1} \ldots, w_{in}) \in U$.

By (4.3) and Lemma 3.6, we have

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

We then define

$$G(X_0, \ldots, X_n) = \prod_{i=1}^{N} \Theta(a_i X^{w_i}) \Theta(a_i^p X^{p w_i}) \cdots \Theta(a_i^{p^{r-1}} X^{p^{r-1} w_i}),$$

whence

$$q^s N_s' = (q^s - 1)^n + \sum_{x_0,\ldots,x_n \in \mathbb{F}_{q^s}^\times} G(x) \cdot G(x^q) \cdot G(x^{q^2}) \cdots G(x^{q^{s-1}}). \tag{4.4}$$

But we know from Proposition 4.1 that $\Theta(a_i^{p^j} X^{p^j w_i}) \in R_0$. Since R_0 is closed under multiplication, we have

$$G(X_0, \ldots, X_n) \in R_0 \subset \Omega[[X_0, \ldots, X_n]].$$

By Lemma 3.17, equation (4.4) gives

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

where $\Psi = \Psi_{q,G} = T_q \circ G$. By the binomial theorem,

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

and hence

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

We then define Δ by

$$\Delta(T) = \det(1 - AT) = \exp_p\Big(-\sum_{s=1}^{\infty} \operatorname{Tr}(\Psi^s) T^s / s \Big),$$

so that

$$\begin{aligned} Z'(H_f/\mathbb{F}_q; T) &= \exp_p\Big(\sum_{s=1}^{\infty} N_s' T^s / s \Big) \\ &= \prod_{i=0}^{n} \Big[\exp_p\Big(\sum_{s=1}^{\infty} q^{s(n-i-1)} T^s / s \Big) \Big]^{(-1)^i \binom{n+1}{i}} \times \prod_{i=0}^{n+1} \Big[\exp_p\Big(\sum_{s=1}^{\infty} q^{s(n-i)} \operatorname{Tr}(\Psi^s) T^s / s \Big) \Big]^{(-1)^i \binom{n+1}{i}} \\ &= \prod_{i=1}^{n} \Big(1 - q^{n-i-1} T \Big)^{(-1)^{i+1} \binom{n+1}{i}} \prod_{i=0}^{n+1} \Delta\Big(q^{n-i} T \Big)^{(-1)^{i+1} \binom{n+1}{i}}, \end{aligned}$$

where we note our use of Theorem 2.38. Hence by Theorem 3.31, each term in this product is a p-adic entire function of the desired form, raised to an integer power. Thus $Z'(H_f/\mathbb{F}_q; T)$ is p-adic meromorphic. □

Chapter 5

A Rational Function Criterion

Before proving our main theorem, we must first establish the following criterion for when a power series can be written as a rational function.

Theorem 5.1. *Let K be any field. Let $F(T) = \sum_{i=0}^{\infty} a_i T^i \in K[[T]]$. For $m, s \geq 0$, let $A_{s,m}$ be the following $(m+1) \times (m+1)$ matrix:*

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

Let $D_{s,m} = \det(A_{s,m})$. Then $F(T)$ is a rational function if and only if there exist non-negative integers m and S such that $D_{s,m} = 0$ for all $s \geq S$.

Proof. For the forward implication, suppose $F(T) = P(T)/Q(T)$, where

$$P(T) = \sum_{i=0}^{n} b_i T^i, Q(T) = \sum_{i=0}^{m} c_i T^i \in K[T],$$

and $Q(T) \neq 0$. Thus $F(T) \cdot Q(T) = P(T)$, so that equating coefficients of T^i for $i > \max(n, m)$ gives:

$$\sum_{j=0}^{m} a_{i-m+j} \cdot c_{m-j} = 0. \tag{5.1}$$

Let $S = \max(0, n - m + 1)$. For $s \geq S$, applying (5.1) with $i = s + m, s + m + 1, \ldots, s + 2m$ gives

$$\begin{aligned} a_s c_m + a_{s+1} c_{m-1} + \cdots + a_{s+m} c_0 &= 0 \\ a_{s+1} c_m + a_{s+2} c_{m-1} + \cdots + a_{s+m+1} c_0 &= 0 \\ &\vdots \\ a_{s+m} c_m + a_{s+m+1} c_{m-1} + \cdots + a_{s+2m} c_0 &= 0, \end{aligned}$$

so that $(c_0, c_1, \ldots, c_m) \cdot A_{s,m} = 0$ under matrix multiplication. Thus, since $Q \neq 0$, we have $D_{s,m} = \det(A_{s,m}) = 0$ for $s \geq S$.

For the reverse implication, note that $m = 0$ implies F is a polynomial and we are done. So without loss of generality, let $m \geq 1$ be the smallest positive integer such that for some non-negative integer S we have $D_{s,m} = 0$ for all $s \geq S$.

Claim 5.2. *$D_{s,m-1} \neq 0$ for all $s \geq S$.*

Proof. Suppose that $D_{s,m-1} = 0$ for some $s \geq S$. Then some nontrivial linear combination of the first m rows $r_0, r_1, \ldots r_{m-1}$ of $A_{s,m}$ is 0 in all but perhaps the last column. Let r_k be the first row with nonzero coefficient in this linear combination, that is, there are $\alpha_1, \ldots, \alpha_{m-k-1} \in K$ such that the row vector r_k differs from $\alpha_1 r_{k+1} + \alpha_2 r_{k+2} + \cdots + \alpha_{m-k-1} r_{m-1}$ in at most the last column. In our matrix $A_{s,m}$, we now subtract the above linear combination from row r_k, leaving the determinant $D_{s,m} = 0$ unchanged. This leaves us with two cases:

(1) $k > 0$. Then our new matrix looks like

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

Consider the square matrix consisting of all but the first row and last column above. Since there is a row consisting entirely of 0's, we see that this matrix has determinant 0. On the other hand, our new matrix was formed from $A_{s+1,m-1}$ by row operations that did not involve the deleted first row. Thus $D_{s+1,m-1} = 0$.

(2) $k = 0$. This gives us

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

If $\beta = 0$, then the $m \times m$ matrix formed by deleting the last row and first column has determinant 0. However, this matrix came from row operations on $A_{s+1,m-1}$, none of which involved the deleted last row. Thus, $D_{s+1,m-1} = 0$. On the other hand, if $\beta \neq 0$, then the $m \times m$ matrix formed by deleting the first row and last column has determinant zero; but this matrix is exactly $A_{s+1,m-1}$, so that $D_{s+1,m-1} = 0$ since $D_{s,m} = 0$.

By induction, then, we have $D_{t,m-1} = 0$ for all $t \geq S$, contradicting the minimality of m. □

Thus $D_{s,m} = 0$ and $D_{s,m-1} \neq 0$ for any $s \geq S$. Hence we can find a linear combination of the rows in $A_{s,m}$ which vanishes, and in which the coefficient of the last row is nonzero. In particular, for any $s \geq S$, the last row r_{m+1} of $A_{s,m}$ is a linear combination of the preceding rows $r_0, r_1, \ldots, r_m$. So any solution to

$$a_S c_m + a_{S+1} c_{m-1} + \cdots + a_{S+m} c_0 = 0$$
$$\vdots$$
$$a_{S+m-1} c_m + a_{S+m} c_{m-1} + \cdots + a_{S+2m-1} c_0 = 0$$

is also a solution to

$$a_{S+m} c_m + a_{s+m+1} c_{m-1} + \cdots + a_{s+2m} c_0 = 0,$$

and, by induction, to the equation

$$a_s c_m + a_{s+1} c_{m-1} + \cdots + a_{s+m} c_0 = 0$$

for every $s \geq S$. That is, for all $s \geq S$ the coefficent of T^{s+m} in $\left(\sum_{i=0}^{m} c_i T^i\right) \cdot \left(\sum_{i=1}^{\infty} a_i T^i\right)$ is 0. Thus $F(T) = \sum_{i=1}^{\infty} a_i T^i$ is a quotient of two polynomials. □

Chapter 6

Dwork's Theorem

6.1 Proof of the Theorem

Proposition 6.1. *The coefficient of T^i in $Z(H_f/\mathbb{F}_q;T)$ is bounded above by q^{ni}.*

Proof. We begin by observing that $N_s \leq \#\mathbb{A}^n_{\mathbb{F}_{q^s}} = q^{ns}$. Thus the coefficients of $Z(H_f/\mathbb{F}_q;T) = \exp(\sum_{s=1}^{\infty} N_s T^s/s)$ are clearly less than or equal to those of $\exp(\sum_{s=1}^{\infty}(q^{ns})T^s/s)$. But

$$\exp(\sum_{s=1}^{\infty}(q^{ns})T^s/s) = \exp(\sum_{s=1}^{\infty}(q^nT)^s/s) = \exp(-\log(1-q^nT)) = 1/(1-q^nT) = \sum_{i=0}^{\infty} q^{ni}T^i. \quad \square$$

Lemma 6.2. $Z(H_f/\mathbb{F}_q;T) \in 1 + T\mathbb{Z}[[T]]$.

Proof. For any $P = (x_1,\ldots,x_n) \in H_f(\overline{\mathbb{F}}_q)$, define $\mu(P)$ to be the minimal positive integer such that $x_i \in \mathbb{F}_{q^{\mu(P)}}$ for all $i = 1,\ldots,n$. Fix $r \geq 1$, and consider a point $P \in H_f(\overline{\mathbb{F}}_q)$ such that $\mu(P) = r$.

Claim 6.3. *For all $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) - \{e\}$, we have $\sigma(P) \neq P$.*

Proof. Suppose $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ satisfies $\sigma(P) = P$. Let L be the fixed field $L = (\mathbb{F}_{q^r})_{\langle\sigma\rangle} = \{x \in \mathbb{F}_{q^r} \mid \sigma(x) = x\}$. Since σ fixes P, we know that $P \in H_f(L)$. Thus, by the minimality of r, we have $L = \mathbb{F}_{q^r}$, so that $\langle\sigma\rangle = \{e\}$. $\square$

Thus, P has $\#\,\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) = r$ distinct Galois conjugates in $\mathbb{F}_{q^r}$. Given $P \in H_f(\mathbb{F}_{q^r})$, we can view P as also sitting inside $H_f(\mathbb{F}_{q^{2r}}), H_f(\mathbb{F}_{q^{3r}}), \ldots$. Note that $\mathbb{F}_{(q^r)^i}$ are the only algebraic extensions of $\mathbb{F}_{q^r}$. Letting r and P vary, we define

$$\mathcal{P}(r) = \{P \in H_f(\mathbb{F}_{q^r}) : \mu(P) = r\}.$$

We can now write our zeta function $Z(H_f/\mathbb{F}_q; T)$ as

$$\exp\Big(\sum_{s=1}^{\infty} N_s T^s/s\Big) = \exp\Big(\sum_{s=1}^{\infty} \sum_{P \in H_f(\mathbb{F}_{q^s})} T^s/s\Big) = \exp\Big(\sum_{r=1}^{\infty} \sum_{P \in \mathcal{P}(r)} \sum_{t=1}^{\infty} \frac{T^{rt}}{rt}\Big). \tag{6.1}$$

Note that $\sum_{t=1}^{\infty} \frac{T^{rt}}{rt} = \frac{1}{r} \sum_{t=1}^{\infty} \frac{(T^r)^t}{t} = -\frac{1}{r}\log(1-T^r)$. Applying this fact to (6.1) gives

$$\begin{aligned} Z(H_f/\mathbb{F}_q; T) &= \exp\Big(\sum_{r=1}^{\infty} \sum_{P \in \mathcal{P}(r)} -\frac{1}{r}\log(1-T^r)\Big) \\ &= \exp\Big(\sum_{r=1}^{\infty} -\frac{1}{r}\log(1-T^r) \cdot \#\{\mathcal{P}(r)\}\Big). \end{aligned}$$

However, the previous paragraph implies that $r | \#\{\mathcal{P}(r)\}$. We can thus write $\#\{\mathcal{P}(r)\} = r \cdot n_r$, for some $n_r \in \mathbb{N}$. This gives us

$$\exp\Big(\sum_{r=1}^{\infty} -n_r \cdot \log(1-T^r)\Big) = \prod_{r=1}^{\infty} \Big(\frac{1}{1-T^r}\Big)^{n_r} = \prod_{r=1}^{\infty} \Big(\sum_{j=0}^{\infty} T^{jr}\Big)^{n_r} \in 1 + \mathbb{Z}[[T]]. \qquad \square$$

Before we prove Dwork's Theorem, we state the following classical result of p-adic analysis.

Theorem 6.4 (p-adic Weierstrass Preparation Theorem)**.** *If $B(T) \in \Omega[[T]]$ is a p-adic entire function, then for any R there exists a polynomial $P(T)$ and a p-adic power series $H(T) \in 1 + T\Omega[[T]]$ which converges and is non-zero on the closed disc $D(R)$ of radius R, such that $B(T) = P(T) \cdot H(T)$.*

Proof. Omitted. See [2, pp. 105 – 106]. □

We are now ready to prove our main result.

Theorem 6.5 (Dwork)**.** *The zeta function of any affine hypersurface is a ratio of two polynomials with coefficients in $\mathbb{Q}$.*

Proof. For brevity, we use the notation $Z(T) = Z(H_f/\mathbb{F}_q;T)$. We showed in Theorem 4.3 that $Z(T) \in 1+T\mathbb{Z}[[T]]$ is p-adic meromorphic, so we can write $Z(T) = A(T)/B(T)$, where $A(T), B(T) \in 1+T\Omega[[T]]$ are p-adic entire functions. Applying the Weierstrass Preparation Theorem to $B(T)$ with $R = q^{2n}$, there exist a polynomial $P(T) \in 1+T\Omega[T]$ and a p-adic power series $H(T) \in 1+T\Omega[[T]]$ that converges and is non-zero on $D(q^{2n})$, such that $B(T) = P(T) \cdot H(T)$. In particular, $H(T)$ has a reciprocal $G(T) \in 1+T\Omega[[T]]$ that is also convergent on $D(q^{2n})$, and thus we can write $B(T) = P(T)/G(T)$. Let $F(T) = A(T) \cdot G(T)$, which converges on $D(q^{2n})$ since $G(T)$ converges on $D(q^{2n})$ and $A(T)$ is p-adic entire. To summarize, we have:

$$F(T) = P(T) \cdot Z(T),$$

where $F(T) \in 1+T\Omega[[T]]$ converges on $D(q^{2n})$ and $P(T) = 1+T\Omega[T]$.

For the remainder of the proof, write $F(T) = \sum_{i=0}^{\infty} b_i T^i \in 1+T\Omega[[T]], P(T) = \sum_{i=0}^{e} c_i T^i \in 1+T\Omega[T]$, and $Z(T) = \sum_{i=0}^{\infty} a_i T^i \in 1+T\mathbb{Z}[[T]]$.

Fix $m = 2e+1$, so that $m > 2e$. (Note $e = \deg P$.) Let $A_{s,m}$ be the $(m+1)\times(m+1)$ matrix

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

and let $D_{s,m} = \det(A_{s,m})$. We will show that $D_{s,m} = 0$ for s sufficiently large, and then Lemma 6.1 will imply that $Z(T)$ is a rational function.

Equating coefficients in $F(T) = P(T) \cdot Z(T)$ gives

$$b_{j+e} = a_{j+e} + c_1 a_{j+e-1} + c_2 a_{j+e-2} + \ldots + c_e a_j. \tag{6.2}$$

With the c_k's as coefficients, we can use linear combinations of the columns in $A_{s,m}$ to form $B_{s,m}$, the $(m+1)\times(m+1)$ matrix

$$\begin{pmatrix} a_s & a_{s+1} & \cdots & a_{s+e-1} & b_{s+e} & \cdots & b_{s+m} \\ a_{s+1} & a_{s+2} & \cdots & a_{s+e} & b_{s+e+1} & \cdots & b_{s+m+1} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+m+e-1} & b_{s+m+e} & \cdots & b_{s+2m} \end{pmatrix}$$

Note that going from $A_{s,m}$ to $B_{s,m}$ leaves the determinant unchanged, since the coefficient of a_{j+e} in (6.2) is 1. We thus use $B_{s,m}$ to help estimate $D_{s,m}$.

By Proposition 6.1, we know that $|a_i|_\infty \leq q^{in}$. In our matrix $A_{s,m}$, then,

$$|a_{s+i}|_\infty \leq q^{n(s+i)} \leq q^{n(s+2m)}, \quad \text{for each } i = 0, \ldots, 2m.$$

Thus we have the crude estimate

$$|D_{s,m}|_\infty \leq (m+1)! \cdot q^{n(s+2m)(m+1)} = (m+1)! \cdot q^{2nm(m+1)} q^{ns(m+1)}.$$

Next, we use our matrix $B_{s,m}$ to estimate $|D_{s,m}|_p$. Pick $\alpha \in \Omega$ such that $|\alpha|_p = q^{2n}$. Then $F(\alpha) = \displaystyle\sum_{i=0}^{\infty} b_i \cdot \alpha^i$ converges, since $\alpha \in D(q^{2n})$. So for sufficiently large i, we have $|b_i|_p \cdot q^{2ni} = |b_i \cdot \alpha^i|_p < 1$, or equivalently, $|b_i|_p < q^{-2ni}$.

Note that $D_{s,m} = \det(B_{s,m})$ is a sum of terms, each of which is a product of e of the a_i's and $(m+1-e)$ of the b_i's. But since each $a_i \in \mathbb{Z} \subset \mathbb{Z}_p$, we have $|a_i|_p \leq 1$. Thus each of the terms in the sum has p-adic absolute value bounded above by $(\max |b_i|_p)^{m+1-e}$. Hence, $|D_{s,m}|_p$ is also bounded above by $(\max |b_i|_p)^{m+1-e} < q^{-2ns(m+1-e)}$ for s sufficiently large. Recall that $m = 2e+1 > 2e$, so that

$$|D_{s,m}|_p < q^{-2ns(m+1-e)} = q^{-ns(2m+2-2e)} < q^{-ns(m+2)}.$$

We now multiply together our two bounds, to get

$$|D_{s,m}|_p \cdot |D_{s,m}|_\infty < q^{-ns(m+2)} \cdot (m+1)! \cdot q^{2nm(m+1)} q^{ns(m+1)} = \frac{(m+1)! \cdot q^{2nm(m+1)}}{q^{ns}} < 1,$$

for s sufficiently large.

Note that $D_{s,m} \in \mathbb{Z}$, since each $a_i \in \mathbb{Z}$. Suppose $D_{s,m}$ is non-zero, and let $\ell = \operatorname{ord}_p(D_{s,m})$. Then we can write $D_{s,m} = p^\ell \cdot r$, where p does not divide r. Then

$$|r|_\infty = |1 \cdot r|_\infty = |p^{-\ell} \cdot p^\ell \cdot r|_\infty = p^{-\ell} \cdot |p^\ell \cdot r|_\infty = |D_{s,m}|_p \cdot |D_{s,m}|_\infty < 1.$$

But $r \in \mathbb{Z}$, so $r = 0$, and hence $D_{s,m} = p^\ell r = 0$, a contradiction. Thus $D_{s,m} = 0$ and Dwork's Theorem is proved. □

6.2 Corollaries of Dwork's Theorem

Before going any further, we pause to reflect on Dwork's Theorem and its significance for solving systems of polynomial equations over finite fields. More specifically, the following proposition tells us that we can write any N_s as $\sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s$ for some finite set of complex numbers $\alpha_1, \ldots, \alpha_t$ and $\beta_1, \ldots, \beta_u$. Since a finite number of N_s is sufficient to determine all of the α_i and β_i, we will thus have a simple formula with which we can explicitly compute *all* the remaining N_s.

Proposition 6.6. *$Z(T) = \exp\Big(\sum_{s=1}^{\infty} \frac{N_s}{s} T^s\Big)$ is a rational function $P(T)/Q(T)$ with coefficients in $\mathbb{Q}$ having no poles or zeros at $T = 0$, if and only if there exist $\alpha_1, \ldots, \alpha_t \in \mathbb{C}$ and $\beta_1, \ldots, \beta_u \in \mathbb{C}$ such that*

$$N_s = \sum_{i=1}^{t} \alpha_i^s - \sum_{i=1}^{u} \beta_i^s, \textit{ for all } s = 1, 2, 3, \ldots,$$

where $\prod_{i=1}^{t}(1 - \alpha_i T), \prod_{i=1}^{u}(1 - \beta_i T)$ have all coefficients in $\mathbb{Q}$.

Proof. Suppose N_s is of the above form. That is,

$$N_s = \alpha_1^s + \ldots + a_t^s - (\beta_1^s + \ldots + \beta_u^s).$$

Then our zeta-function $Z(T)$ is

$$Z(T) = \frac{\prod_{i=1}^{t} \exp\Big(\sum_{s\geq 1}(\alpha_i^s T^s)/s\Big)}{\prod_{i=1}^{u} \exp\Big(\sum_{s\geq 1}(\beta_i^s T^s)/s\Big)} = \frac{\prod_{i=1}^{t}\big(-\log(1-\alpha_i T)\big)}{\prod_{i=1}^{u}\big(-\log(1-\beta_i T)\big)} = \frac{\prod_{i=1}^{u}(1-\beta_i T)}{\prod_{i=1}^{t}(1-\alpha_i T)}. \tag{6.3}$$

Thus $Z(T) = P(T)/Q(T)$ is a rational function with coefficients in $\mathbb{Q}$, and $Z(0) = P(0) = Q(0) = 1$.

For the reverse implication, suppose $Z(T) \in \mathbb{Q}(T)$, and write

$$Z(T) = \frac{P(T)}{Q(T)}, \text{ where } P(T), Q(T) \in 1 + T\mathbb{Q}[T].$$

Motivated by equation (6.3), let $\alpha_1, \ldots, \alpha_t$ be the reciprocals of the roots of $Q(T)$, listed with multiplicity. Similarly, let $\beta_1, \ldots, \beta_u$ be the reciprocals of the roots of $P(T)$, also listed with multiplicity. We thus obtain the desired result. □

Definition 6.7. Let K be a field and let $f_1, \dots, f_m \in K[X_1, \dots, X_n]$. If M is a field containing K, then

$$H_{f_1,\dots,f_m}(M) = \{(x_1, \dots, x_n) \in \mathbb{A}^n_M \mid f_i(x_1, \dots, x_n) = 0 \text{ for all } i = 1, \dots, m\}$$

is the *affine variety* defined by $f_1, \dots, f_m$.

Corollary 6.8 (Dwork's Theorem for Affine Varieties)**.** *Let $f_1, \dots, f_m \in \mathbb{F}_q[X_1, \dots, X_n]$ and let $\tilde{N}_s = \#\big(H_{f_1,\dots,f_m}(\mathbb{F}_{q^s})\big)$. Define $\tilde{Z}(T) = \exp\Big(\sum_{s\geq 1} \tilde{N}_s T^s/s\Big)$. Then $\tilde{Z}(T) \in \mathbb{Q}(T)$.*

Proof. The case $m = 1$ is Dwork's Theorem. For $m = 2$, observe that

$$\tilde{N}_s = \#\big(H_{f_1,f_2}(\mathbb{F}_{q^s})\big) = \#\big(H_{f_1}(\mathbb{F}_{q^s})\big) + \#\big(H_{f_2}(\mathbb{F}_{q^s})\big) - \#\big(H_{f_1\cdot f_2}(\mathbb{F}_{q^s})\big),$$

so that $\tilde{Z}(T)$ is a product of rational functions by Dwork's Theorem. For the general case, note that

$$H_{f_{i_1}\cdots f_{i_r}}(\mathbb{F}_{q^s}) = \bigcap_{j=1}^{r} H_{f_{i_j}}(\mathbb{F}_{q^s}).$$

Thus by the Inclusion/Exclusion Principle from Chapter 1, we have

$$\tilde{N}_s = \sum_{i_1\leq m} \#(H_{f_{i_1}}(\mathbb{F}_{q^s})) - \sum_{i_1<i_2\leq m} \#(H_{f_{i_1}f_{i_2}}(\mathbb{F}_{q^s})) + \cdots + \\ \sum_{i_1<\cdots<i_r\leq m} \#(H_{f_{i_1}\cdots f_{i_r}}(\mathbb{F}_{q^s})) + \cdots + (-1)^{m+1}\#(H_{f_1\cdots f_m}(\mathbb{F}_{q^s})).$$

Hence Dwork's Theorem implies $\tilde{Z}(T)$ is a product of rational functions. □

Definition 6.9. Let K be any field, and let $f \in K[X_0, \dots, X_n]$ be a homogeneous polynomial. If M is a field containing K, then

$$\hat{H}_f(M) = \{(x_0, \dots, x_n) \in \mathbb{P}^n_M \mid f(x_0, \dots, x_n) = 0\}$$

is the *projective hypersurface* defined by f.

Corollary 6.10 (Dwork's Theorem for Projective Hypersurfaces)**.** *Let $f \in \mathbb{F}_q[X_0, \dots, X_n]$ be a homogeneous polynomial, and let $\hat{N}_s = \#(\hat{H}_f(\mathbb{F}_{q^s}))$. Define $\hat{Z}(T) = \exp\big(\sum_{s\geq 1} \hat{N}_s T^s/s\big)$. Then $\hat{Z}(T) \in \mathbb{Q}(T)$.*

Proof. Recall that $\mathbb{P}^n_{\mathbb{F}_{q^s}}$ can be written as the disjoint union $\mathbb{A}^n_{\mathbb{F}_{q^s}} \cup \mathbb{A}^{n-1}_{\mathbb{F}_{q^s}} \cup \cdots \cup \mathbb{A}^1_{\mathbb{F}_{q^s}} \cup \{\text{point}\}$. But there is clearly a bijection between the sets $\hat{H}_f \cap \mathbb{A}^i_{\mathbb{F}_{q^s}}$ and $H_{f_i}(\mathbb{F}_{q^s})$, where $f_i(x_0, \ldots, x_{i-1}) = f(x_0, \ldots, x_{i-1}, 1, 0, \ldots, 0) \in \mathbb{F}_q[x_0, \ldots, x_{i-1}]$. Thus, applying Dwork's Theorem to the $H_{f_i}(\mathbb{F}_{q^s})$'s gives the desired result. □

Definition 6.11. Let K be any field, and let $f_1, \ldots, f_m \in K[X_0, \ldots, X_n]$ be homogeneous polynomials. If M is a field containing K, then

$$\bar{H}_{f_1,\ldots,f_m}(K) = \{(x_0, \ldots, x_n) \in \mathbb{P}^n_K \mid f_i(x_0, \ldots, x_n) = 0 \text{ for all } i = 1, \ldots, m\}$$

is the *projective variety* defined by $f_1, \ldots, f_m$.

Corollary 6.12 (Dwork's Theorem for Projective Varieties)**.** *Let $f_1, \ldots, f_m \in \mathbb{F}_q[X_0, \ldots, X_n]$ be homogeneous polynomials, and let $\bar{N}_s = \#(\bar{H}_{f_1,\ldots,f_m}(\mathbb{F}_{q^s}))$. Define $\bar{Z}(T) = \exp\big(\sum_{s \geq 1} \bar{N}_s T^s/s\big)$. Then $\bar{Z}(T) \in \mathbb{Q}(T)$.*

Proof. As in the proof of Corollary 6.8, we use the Inclusion/Exclusion Principle to show

$$\bar{N}_s = \sum_{i_1 \leq m} \#(\bar{H}_{f_{i_1}}(\mathbb{F}_{q^s})) - \sum_{i_1 < i_2 \leq m} \#(\bar{H}_{f_{i_1} f_{i_2}}(\mathbb{F}_{q^s})) + \cdots + \sum_{i_1 < \cdots < i_r \leq m} \#(\bar{H}_{f_{i_1} \cdots f_{i_r}}(\mathbb{F}_{q^s})) + \cdots + (-1)^{m+1} \#(\bar{H}_{f_1 \cdots f_m}(\mathbb{F}_{q^s})).$$

Thus by Corollary 6.10, $\bar{Z}(T)$ is a product of rational functions. □

Bibliography

[1] B. Dwork, On the Rationality of the Zeta-Function of an Algebraic Variety, *American Journal of Mathematics.* **82** (1960), 631–648 .

[2] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions,* Springer-Verlag, New York, 1984.

[3] F.Q. Gouvêa, *p-adic Numbers,* Springer-Verlag, New York, 2003.

[4] D.A. Cox, *Galois Theory,* John Wiley & Sons, Inc., New Jersey, 2004.

[5] I. Stewart, *Galois Theory,* Chapman & Hall, Florida, 1989.

[6] S.H. Friedberg, A.J. Insel, L.E. Spence, *Linear Algebra,* Pearson Education, Inc., New Jersey, 2003.

[7] S.S. Epp, *Discrete Mathematics with Applications,* Brooks/Cole, California, 2004.

[8] N.M. Katz, J. Tate, `http://math.cofc.edu/paul/mem-dwork.pdf`

Appendix A

Galois Theory

We include below a brief review of some results from Galois Theory. For more on the subject, as well as complete proofs of the following facts, see [4].

Definition A.1. If L is a field, then an *automorphism* of L is a field isomorphism $\sigma : L \to L$.

Definition A.2. Given a ring homomorphism of fields $\varphi : F \to L$, we say that L is a *field extension* of F via φ.

Definition A.3. Let L and F be fields, with $F \subset L$ a finite extension. Then the *Galois group* $\mathrm{Gal}(L/F)$ is the set

$$\{\sigma : L \to L \mid \sigma \text{ is an automorphism of } L, \text{ and } \sigma(a) = a \text{ for all } a \in F\}.$$

Proposition A.4. $\mathrm{Gal}(L/F)$ *is a group under composition.*

Proof. Suppose $\sigma, \tau \in \mathrm{Gal}(L/F)$. Then $\sigma \circ \tau$ is an automorphism because σ, τ are. Also, if $a \in F$, then $\sigma \circ \tau(a) = \sigma(\tau(a)) = \sigma(a) = a$, since σ, τ are the identity on F. Thus we have a well-defined operation on $\mathrm{Gal}(L/F)$. Note also that composition of functions is associative. The identity map $1_L : L \to L$ is an automorphism and restricts to the identity on F, so that $1_L \in \mathrm{Gal}(L/F)$. Clearly $\sigma \circ 1_L = 1_L \circ \sigma = \sigma$ for all $\sigma \in \mathrm{Gal}(L/F)$. Thus 1_L is the identity element of $\mathrm{Gal}(L/F)$. Given $\sigma \in \mathrm{Gal}(L/F)$, then because σ is an automorphism, its inverse $\sigma^{-1} : L \to L$ is an automorphism as well. If $a \in F$, then $a = \sigma(a)$, so that $\sigma^{-1}(a) = \sigma^{-1}(\sigma(a)) = a$. Hence $\sigma^{-1} \in \mathrm{Gal}(L/F)$. Thus $\mathrm{Gal}(L/F)$ satisfies the group criterion. □

Definition A.5. Let $F \subset L$ be a finite extension of fields with Galois group $\mathrm{Gal}(L/F)$. Given a subgroup $H \subset \mathrm{Gal}(L/F)$, the *fixed field* of H is

$$L_H = \{a \in L \mid \sigma(a) = a \text{ for all } \sigma \in H\}.$$

Note also that L_H is in fact a field, and $F \subset L_H \subset L$.

Definition A.6. Let $F \subset L$ be a field extension, and note that L forms a vector space over F.
(a) L is a *finite extension* of F if L is a finite-dimensional vector space over F.
(b) The *degree* of L over F, denoted $[L : F]$, is defined to be $\dim_F L$ if L is a finite extension of F, and ∞ otherwise.

Definition A.7. An extension $F \subset L$ is called a *Galois extension* if it is a finite extension where F is the fixed field of $\mathrm{Gal}(L/F)$ acting on L.

We now consider a particularly nice automorphism, named after the German mathematician Ferdinand Georg Frobenius.

Fact A.8. *Let p be prime and let $s \geq 1$ be an integer. Let $q = p^r$, and denote by $\mathbb{F}_q$ the field of q elements. Then the map $\mathrm{Frob}_q : \mathbb{F}_{q^s} \to \mathbb{F}_q$ defined by $\mathrm{Frob}_q(a) = a^q$ is an automorphism of $\mathbb{F}_{q^s}$ that is the identity on $\mathbb{F}_q$; i.e., $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$.*

Remark A.9. Since Galois groups are closed under composition, we see that $(\mathrm{Frob}_q)^i : \mathbb{F}_{q^s} \to \mathbb{F}_q$ defined by $(\mathrm{Frob}_q)^i(a) = a^{q^i}$ is an element of $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q)$. In particular, $a \mapsto a^{q^i}$ is an automorphism of $\mathbb{F}_{q^s}$ that is the identity on $\mathbb{F}_q$.

Fact A.10. *Let p be prime. If $q = p^r$, then $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q) \cong \mathbb{Z}/s\mathbb{Z}$. In particular, $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q) = \{(\mathrm{Frob}_q)^i : i = 0, 1, \ldots, s-1\}$ is a cyclic group of order s.*

We conclude our discussion of Galois Theory with the following claim concerning linear combinations of automorphisms.

Claim A.11. *Let $\sigma_1, \ldots, \sigma_n$ be distinct automorphisms of a field K. Then there is no nontrivial linear combination $\sum a_i \sigma_i$ with $a_1, \ldots, a_n \in K$ such that $\sum a_i \sigma_i(x) = 0$ for every $x \in K$.*

Proof. Suppose our claim is false and consider such a linear combination,

$$a_1\sigma_1(x) + \ldots + a_n\sigma_n(x) = 0. \tag{A.1}$$

Without loss of generality, we assume that $n \geq 1$ is minimal, and that each a_i is non-zero. In fact, if $n = 1$, then $1 = \sigma_1(1) = 0$, a contradiction; so $n > 1$. Since $\sigma_1 \neq \sigma_n$, there must be some $y \in K$ such that $\sigma_1(y) \neq \sigma_n(y)$. Note that $y \neq 0$. We now substitute xy for x in (1.1) to get

$$a_1\sigma_1(xy) + \ldots + a_n\sigma_n(xy) = 0,$$

for all $x \in K$. Thus

$$a_1\sigma_1(x)\sigma_1(y) + \ldots + a_n\sigma_n(x)\sigma_n(y) = 0. \tag{A.2}$$

Multiplying (1.1) by $\sigma_1(y)$ and subtracting the result from (1.2) gives

$$a_2\big(\sigma_1(y) - \sigma_2(y)\big)\sigma_2(x) + \ldots + a_n\big(\sigma_1(y) - \sigma_n(y)\big)\sigma_n(x) = 0.$$

But the coefficient of $\sigma_n(x)$ is $a_n\big(\sigma_1(y) - \sigma_n(y)\big) \neq 0$, contradicting the minimality of n. □

Appendix B

The Weil Conjectures

We say a projective hypersurface $\tilde{H}_{\tilde{f}}$ is *smooth* if the partial derivatives of $\tilde{f}$ with respect to all n variables never vanish simultaneously. Let β be the *Betti number* of $\tilde{H}_{\tilde{f}}$, where the k^{th} Betti number of a space X is related to the k^{th} homology group of a certain manifold corresponding to X. Then for the case of a smooth projective hypersurface, the Weil Conjectures say:

(i) $Z(\tilde{H}_{\tilde{f}}/\mathbb{F}_q;T) = P(T)^{\pm 1}/\big((1-T)(1-qT)\cdots(1-q^{n-1}T)\big)$, where $P(T) \in 1+T\mathbb{Z}[T]$ has degree β, and where we take $P(T)$ when n is even and $P(T)^{-1}$ when n is odd.
(ii) If α is a reciprocal root of $P(T)$, then so is $q^{n-1}\alpha$.
(iii) The complex absolute value of each of the reciprocal roots of $P(T)$ is $q^{(n-1)/2}$.