King's College London
Department of Natural and Mathematical Sciences

Dwork's Theorem

Alexandre Daoud

Submitted in part fulfilment of the requirements for the degree of
Master in Science in Mathematics of King's College London, March 2016

Abstract

Dwork's Theorem concerns the generating function for the number of points on affine algebraic varieties defined over finite fields. If $\mathbb{F}_q$ is a finite field for some prime power q and $\mathbb{F}_{q^s}$ are its finite extensions then the generating function encodes information about the number of points N_s of the variety in each extension. The theorem states that the generating function is necessarily rational; this allows us to completely determine N_t for every positive integer t by the N_i for some $1 \leq i \leq s$. Bernard Dwork's celebrated proof of this theorem, which is originally a conjecture of André Weil, employs p-adic functional analysis. In this dissertation, we aim to provide a rigorous exposition of the proof of the theorem. Along the way, we shall examine the theory of p-adic numbers and understand their deep contributions to this program. Towards the end of this dissertation, we shall discuss the Weil conjectures in generality and observe how Dwork's Theorem fits into the general framework as originally proposed by Weil.

Acknowledgements

I would first like to thank my supervisor Professor David Burns for suggesting this project topic to me. Without his guidance and comments, I surely would not have been able to complete this dissertation.

I would also like to thank my family and friends for their support - in particular my parents who have been a constant, unperturbed source of encouragement throughout my studies and, indeed, my life.

Finally I would like to acknowledge the various academic and teaching staff at King's College London. It is thanks to their combined efforts during my degree that I have been able to reach this far in my studies.

Contents

Chapter 1

Introduction

1.1 Historical Background

For millennia, mathematicians have been fascinated by polynomials. Their beauty is two-fold, encompassing both the simplicity of their expression and their deep connections with a multitude of mathematical fields. Their theory is certainly enormous in scope - indeed, many people dedicate their entire lives to the study of these objects, contributing rich results that are of fundamental importance to the mathematics we do everyday. The theory of polynomials is where we begin our discussion of Dwork's Theorem.

Carl Friedrich Gauss was one such mathematician who studied polynomials. In his famous *Disquisitiones Arithmeticae*, Gauss presented a method for finding the number of solutions for congruences of the form $ax^3 - by^3 \equiv 1 \pmod{p}$ for some prime p of the form $p = 3n + 1$ and integers a and b. He employed so-called Gauss sums which, in some sense, are a finite field analogue of the Gamma function. In subsequent publications, Gauss applied his method to tackle similarly formed problems. Clearly, determining the number of solutions to $ax^3 - by^3 = 1$ over the rational numbers would seem utterly non-trivial at first glance. It turns out that by examining such a polynomial modulo a prime p, we might be able to determine the behaviour of solutions in the rational numbers. An example of this is the Hasse-Minkowski Theorem which implies that a quadratic form has a solution in the rational numbers if and only if it has a solution in the real numbers and the p-adic numbers for each prime p. In some sense, the principle allows us to patch together local solutions to form a global solution. This local-global trope is the first step to motivating the study of Dwork's Theorem.

Our second motivating factor for the study of Dwork's Theorem is the infamous Riemann hypothesis. Riemann's work on the zeroes of his zeta-function provided a conjecture which has tantalised mathematicians for over a century. Emile Artin married the Riemann hypothesis with the aforementioned ideas by constructing a zeta-function for curves over finite fields. He exhibited that an analogue of the Riemann hypothesis holds for certain curves and conjectured that the result holds true for all curves. Weil proved that Artin's conjecture indeed holds for all curves and further conjectured that the zeta-function of a general, smooth, projective variety has certain properties, including the analogue of the Riemann hypothesis. What is now known as Dwork's Theorem was the first of these conjectures to have been proven.

1.2 Understanding the statement of Dwork's Theorem

We now turn our sights towards the statement of Dwork's Theorem. To this end, we first recall a few key results from the theory of finite fields.

Let p be a prime number, $\mathbb{F}_p$ the finite field of order p and denote $K = \overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$. Then

<u>FF1</u> For each positive integer s, there exists a unique field of order p^s, which we denote $\mathbb{F}_{p^s}$, satisfying $[\mathbb{F}_{p^s} : \mathbb{F}_p] = s$. Conversely, any finite field necessarily has prime power order.

<u>FF2</u> $\mathbb{F}_{p^s}$ is the set of all elements of K satisfying $x^{p^s} - x = 0$. Conversely, given any positive integer s, the roots of the polynomial $x^{p^s} - x = 0$ form a field of p^s elements.

<u>FF3</u> $\mathbb{F}_{p^s}^{\times}$ is a cyclic group of order $p^s - 1$.

For a rigorous treatment of the above facts, the reader is invited to check any standard text on Galois Theory such as [Ste89]. We are now ready to introduce the main notions involved in the statement of Dwork's Theorem.

Definition 1.2.1. Let K be a field. We define the **n-dimensional affine space over K** to be

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

Definition 1.2.2. Let K be a field and $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ a polynomial. We define the **affine hypersurface** defined by f in $\mathbb{A}_K^n$ to be

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

We define the **dimension** of H_f to be the number $n - 1$. We say that H_f is an **affine curve** if the dimension of H_f is 1.

Definition 1.2.3. Let H_f be an affine hypersurface defined over a field K. If L/K is a field extension then we define the **L-points** of H_f to be

$$H_f(L) = \{\, (x_1, \ldots, x_n) \in \mathbb{A}_L^n \mid f(x_1, \ldots, x_n) = 0 \,\}$$

We now specialise to the case where K is a finite field. Fix a prime p and let $q = p^s$ for some positive integer s. Let $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ define an $n - 1$ dimensional affine hypersurface over $\mathbb{F}_q$, say H_f. We are interested in determining the number of K-points of H_f for some finite extension $K/\mathbb{F}_q$. To this end, let

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

define an integer sequence, indexed by s. A natural question to ask about an integer sequence is whether or not it exhibits recursive behaviour. That is to say, is it possible to determine N_s for all $s \geq t$ given that we know N_i for all $1 \leq i < t$? The theory of generating functions is often used to determine the solution to such a question which motivates the following definition:

Definition 1.2.4. Let H_f be an affine hypersurface defined over a finite field $\mathbb{F}_q$. We define the **zeta-function** of H_f to be

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

The reason for this choice of generating function over the more natural $\sum_{i=1}^{\infty} N_i T^i$ will become apparent later on in this dissertation.

Armed with these notions, we can now understand the statement of Dwork's Theorem:

Theorem 1.2.5 (Dwork's Theorem). *Let H_f be an affine hypersurface defined over a finite field $\mathbb{F}_q$. Then the zeta-function of H_f is a rational function.*

Dwork's Theorem implies that the generating function for the integer sequence N_s has a closed form as the ratio of two polynomials. This allows us to read off each N_s using the following:

$$N_s = \frac{1}{(s-1)!}\left[\frac{d^s}{dT^s}\log Z(H_f/\mathbb{F}_q;T)\right]_{T=0}$$

In particular, this implies that there exist algebraic numbers $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ such that

$$N_s = \sum_{i=1}^{n} \alpha_i^s - \sum_{i=1}^{m} \beta_i^s$$

In the terminology of the original problem, we see that there exists a $t \in \mathbb{N}$ such that for all $s \geq t$, the number of $\mathbb{F}_{q^s}$-points of H_f are completely determined by all N_i for $1 \leq i < t$.

Example 1.2.6. Let $\mathbb{F}_q$ be a finite field and H the hypersurface consisting of all points of $\mathbb{A}^n_{\mathbb{F}_q}$. Then clearly, for any finite extension $\mathbb{F}_{q^s}/\mathbb{F}_q$ we have $N_s = q^{sn}$. It follows that

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

By the logarithmic derivative formula, we can easily see that $N_s = N_1^s$ for all $s > 1$. This verifies the implications of Dwork's Theorem for this particular hypersurface.

Example 1.2.7. Let H_f be the hypersurface over $\mathbb{F}_q$ defined by the polynomial $f(X_1, \ldots, X_4) = X_1X_4 - X_2X_3 - 1$.

We first consider the case when $X_3 = 0$. In this case, the equation defining H_f reduces to $X_1X_4 = 1$. Since X_2 no longer contributes anything to this equation, there are q^s choices for it. Now, since $\mathbb{F}_{q^s}$ is a field, every non-zero element has a multiplicative inverse and there are thus $q^s - 1$ choices of pairs of X_1 and X_4. It follows that the case where $X_3 = 0$ contributes $q^s(q^s-1)$ elements to $H_f(\mathbb{F}_{q^s})$.

Now suppose that $X_3 \neq 0$. Then X_1 and X_4 can be chosen to be an element of $\mathbb{F}_q$. X_3 can only be chosen from $\mathbb{F}_q^\times$. X_2 is thus fixed by these choices and, in this case, there are $q^s q^s(q^s-1)$ elements contributed to $H_f(\mathbb{F}_{q^s})$. We therefore have that

$$N_s = q^{3s} - q^{2s} + q^{2s} - q^s = q^{3s} - q^s$$

The zeta-function of H_f is thus given by

$$Z(H_f/\mathbb{F}_q;T) = \exp\left(\sum_{s=1}^{\infty} \frac{(q^{3s}-q^s)T^s}{s}\right) = \frac{\exp(\sum_{s=1}^{\infty}(q^3T)^s/s)}{\exp(\sum_{s=1}^{\infty}(qT)^s/s)} = \frac{1-qT}{1-q^3T}$$

Dwork proved this result by a remarkable application of so-called p-adic functional analysis. In the next chapter, we shall construct the p-adic numbers and study some interesting properties surrounding their field extensions which will prove very useful in our discussion of the proof of Dwork's Theorem.

Chapter 2

The p-adic numbers

2.1 Absolute values and $\mathbb{Q}_p$

The p-adic numbers are a collection of countably many distinct extensions of the arithmetic of the rational numbers. They were first introduced in the late 1890s by Kurt Hensel and have proven extremely useful in a myriad of number theoretic problems. To motivate our construction, we briefly recall the standard construction of the real numbers from the rational numbers.

Consider the absolute value function $|\cdot|$ which maps a rational number to its magnitude. We complete the rational numbers with respect to this absolute value by considering the set S of all Cauchy sequences with rational elements. If $\{ a_n \}$ and $\{ b_n \}$ are two such Cauchy sequences then we define an equivalence relation where $\{ a_n \} \sim \{ b_n \}$ if and only if $\lim_{i\to\infty} |a_i - b_i| \to 0$. The real numbers are then obtained by quotienting S out by $\sim$. It is easy to check that this yields a field after defining the standard operations on these equivalence classes.

The p-adic numbers are obtained by applying this process to a so-called non-Archimedean absolute value.

Proposition 2.1.1. *Let p be a prime number and $x = a/b \in \mathbb{Q}$ be non-zero. If $x = a/b = p^\alpha c/d$ where c and d are coprime to p then the function $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{ \infty \}$[1] defined by*

$$v_p(x) = \begin{cases} \alpha & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases}$$

is a valuation of $\mathbb{Q}$, referred to as the ***p-adic valuation****.*

Proof. By the definition of v_p, it is clear that $v_p(x) = \infty$ if and only if $x = 0$. Hence it suffices to show that for all $x, y \in \mathbb{Q}$ we have $v_p(xy) = v_p(x) + v_p(y)$ and $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$ where equality holds in the latter statement if and only if $v_p(x) \neq v_p(y)$.

To this end, let $x = a/b$ and $y = c/d$. Then we may write $x = p^\alpha m/n$ and $y = p^\beta j/k$ with p coprime to the integers m, n, j and k. We then have that $v_p(xy) = v_p(p^{\alpha+\beta}(mj)/(nk))$ whence $v_p(xy) = \alpha + \beta = v_p(x) + v_p(y)$.

Now, if any of x,y or $x + y$ are zero then the last property follows trivially. Hence we may assume

[1] here we are extending the ordering and additive group law of $\mathbb{Z}$ to $\mathbb{Z} \cup \{ \infty \}$ with $\infty \geq x$ and $\infty + x = x + \infty = \infty$ for all $x \in \mathbb{Z}$

they are non-zero and so is their sum. Then

$$\begin{aligned} v_p(x+y) = v_p\left(\frac{ad+bc}{bd}\right) &= v_p(ad+bc) - v_p(b) - v_p(d) \\ &\geq \min\{v_p(ad), v_p(bc)\} - v_p(b) - v_p(d) \qquad (2.1) \\ &= \min\{v_p(x), v_p(y)\} \end{aligned}$$

Note that equality holds in Equation 2.1 if and only if $ad \neq bc$ and thus the proposition is proved. □

Definition 2.1.2. Let p be a prime number. Then we define the **p-adic absolute value** on $\mathbb{Q}$ to be the function $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ defined by

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

Each axiom of absolute values can be checked for $|\cdot|_p$ from the corresponding axiom for v_p. In fact, $|\cdot|_p$ satisfies a much stronger property than the triangle inequality, namely for all $x, y \in \mathbb{Q}$, we have $|x+y|_p \leq \max\{|x|_p, |y|_p\}$. This is thanks to the inequality axiom for the valuation v_p. Such an inequality is called the **ultrametric inequality** and absolute values satisfying this property are called **non-Archimedean**. Absolute values that only satisfy the triangle inequality are referred to as **Archimedean** - a standard example of this is the magnitude mapping on $\mathbb{Q}$ which we will henceforth denote by $|\cdot|_\infty$.

We have seen that, given any prime number p, we can define another absolute value on $\mathbb{Q}$ depending on p. If we complete $\mathbb{Q}$ with respect to this absolute value, we obtain the field of p-adic numbers, henceforth denoted $\mathbb{Q}_p$.

Firstly, we extend the absolute value $|\cdot|_p$ to $\mathbb{Q}_p$. Given any equivalence class $\alpha \in \mathbb{Q}_p$, we choose a representative $\{\, \alpha_i \,\}$ and we define $|\alpha|_p = \lim_{i\to\infty} |\alpha_i|_p$. Clearly this definition is independent of the choice of representative; however, we must show that such a limit necessarily exists. If $\lim_{i\to\infty} |\alpha_i|_p = 0$ then the limit is clearly defined. If not then for all $\varepsilon > 0$, there exists an $N \in \mathbb{N}$ such that for all $i > N$ we have $|\alpha_i|_p > \varepsilon$. Since $\{\, \alpha_i \,\}$ is Cauchy, we have that for all $n > N$, $|\alpha_n - \alpha_i|_p < \varepsilon$. On the other hand, $|\alpha_n - \alpha_i|_p \leq \max\{|\alpha_n|_p, |\alpha_i|_p\} > \varepsilon$. To avoid a contradiction, we must have that $|\alpha_n|_p = |\alpha_i|_p$ and thus the limit is defined.

We now look at the structure of the elements of $\mathbb{Q}_p$. In some sense, these elements can be expressed as power series in p.

Definition 2.1.3. We define the **p-adic integers**, denoted $\mathbb{Z}_p$, as follows:

$$\mathbb{Z}_p = \{\, \alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1 \,\}$$

Lemma 2.1.4. *Let $x \in \mathbb{Q}$ be a rational number such that $|x|_p \leq 1$. Then for all $i \in \mathbb{N}$ there exists an integer $\alpha \in \mathbb{Z}$ satisfying $|\alpha - x|_p \leq p^{-i}$ and $\alpha \in \{\, 0, 1, \ldots, p^i - 1 \,\}$.*

Theorem 2.1.5. *Let $\alpha \in \mathbb{Q}_p$ be a p-adic number. Then there exists a unique representative Cauchy sequence of α, say $\{ a_i \}$, such that for all $i \in \mathbb{N}$,*

1. $0 \leq a_i < p^i$
2. $a_i \equiv a_{i+1} \pmod{p^i}$

For a proof of this result, see [Kob84, p.11–12]. Theorem 2.1.5 allows us to write any $\alpha \in \mathbb{Q}_p$ in the form

$$\alpha = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + a_2 p^2 + \dots$$

for some $m \in \mathbb{N}$ and $a_i \in \mathbb{F}_p$. Such a base p expansion makes the arithmetic of the p-adic numbers very simple to work with and gives a much more intuitive picture as opposed to the more abstract Cauchy sequence construction.

Example 2.1.6. The additive inverse in $\mathbb{Q}_p$ is given by

$$-1 = \sum_{i=0}^{\infty} (p-1)p^i$$

Indeed, if we add 1 to this series, it is clear that the terms will cancel to give 0.

The following result will be of theoretical importance to us throughout the rest of the discussion. It highlights a unique characteristic of non-Archimedean absolute values which is in stark contrast to Archimedean absolute values.

Proposition 2.1.7. *Let $\{ a_i \} \subseteq \mathbb{Q}_p$ be a sequence of p-adic numbers. Then the series*

$$S = \sum_{i=0}^{\infty} a_i$$

converges if and only if the absolute values of the terms of $\{ a_i \}$ converges to 0.

Proof. The forward implication is clear from elementary analysis. For the opposite implication, let S_N represent the N^{th} partial sum of S. Then

$$\begin{aligned} |S_M - S_N|_p &= |a_{N+1} + a_{N+2} + \cdots + a_M|_p \\ &\leq \max\{|a_{N+1}|_p, \dots, |a_M|_p\} \end{aligned}$$

Passing to the limit $M, N \to \infty$ on both sides, we see that $\lim_{N\to\infty} S_N = 0$. □

2.2 Hensel's Lemma and Ostrowski's Theorem

Hensel's Lemma is a result concerning solutions of polynomial equations in $\mathbb{Q}_p$. The result implies that if a polynomial $f(X) \in \mathbb{Z}_p[X]$ has a root modulo p then it has a root in $\mathbb{Z}_p$. Such a root is obtained by 'lifting' the solution inductively to higher powers of p. Hensel's Lemma (and generalisations thereof) will be of the utmost importance in discussing the proof of Dwork's Theorem.

Theorem 2.2.1 (Hensel's Lemma). *Let $f(X) = c_m x^m + \cdots + c_0 \in \mathbb{Z}_p[X]$ be a polynomial. Denote by $f'(X)$ the formal derivative of $f(X)$. Suppose there exists an $a_0 \in \mathbb{Z}_p$ such that $f(a_0) \equiv 0 \pmod{p}$ and $f'(a_0) \not\equiv 0 \pmod{p}$. Then there exists a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a \equiv a_0 \pmod{p}$.*

Proof. We claim that there exists a unique sequence of rational integers $\{ a_i \}$ such that for all $n \geq 1$ we have

1. $f(a_n) \equiv 0 \pmod{p^{n+1}}$
2. $a_n \equiv a_{n-1} \pmod{p^n}$
3. $0 \leq a_n < p^{n+1}$

We shall prove the existence of such a sequence by induction.

Indeed, let $n = 1$. Let $\tilde{a}_0$ represent the unique element of $\mathbb{F}_p$ congruent to a_0 mod p. Now if an integer a_1 were to satisfy conditions (2) and (3), it would be of the form $\tilde{a}_0 + b_1 p$ for some $0 \leq b_1 < p$. Using the binomial theorem, we proceed by investigating the behaviour of $f(a_1)$ modulo p^2:

$$\begin{aligned} f(a_1) = f(\tilde{a}_0 + b_1 p) &= \sum_{i=1}^{m} c_i (\tilde{a}_0 + b_1 p)^i \\ &= \sum_{i=1}^{m} (c_i \tilde{a}_0^i + i c_i \tilde{a}_0^{i-1} b_1 p + \mathcal{O}(p^2)) \\ &\equiv \sum_{i=1}^{m} c_i \tilde{a}_0^i + \left(\sum_{i=1}^{m} i c_i \tilde{a}_0^{i-1} \right) b_1 p \pmod{p^2} \\ &= f(\tilde{a}_0) + f'(\tilde{a}_0) b_1 p \end{aligned}$$

By hypothesis, we have that $f(a_0) \equiv 0 \pmod{p}$. Hence we can always find an $\alpha \in \{ 0, 1, \ldots, p-1 \}$ such that $f(\tilde{a}_0) \equiv \alpha p \pmod{p^2}$. Hence

$$\begin{aligned} f(a_1) \equiv 0 \pmod{p^2} &\iff \alpha p + f'(\tilde{a}_0) b_1 p \equiv 0 \pmod{p^2} \\ &\iff \alpha + f'(\tilde{a}_0) b_1 \equiv 0 \pmod{p} \end{aligned}$$

By hypothesis we have $f'(a_0) \not\equiv 0 \pmod{p}$ and thus this equation can always be solved for b_1. Using Lemma 2.1.4, we can choose $b_1 \in \{ 0, 1, \ldots, p-1 \}$ such that $b_1 \equiv -\alpha / f'(\tilde{a}_0) \pmod{p}$.

Now assume that the claim is true for all $a_1, \ldots, a_{n-1}$. We need to show that it is true for a_n. Conditions (2) and (3) again imply that we require $a_n = a_{n-1} + b_n p^n$ with $0 \leq b_n < p$. Inserting this into the polynomial $f(X)$ and ignoring terms divisible by p^{n+1} we have

$$\begin{aligned} f(a_n) &= f(a_{n-1} + b_n p^n) \\ &\equiv f(a_{n-1}) + f'(a_{n-1}) b_n p^n \pmod{p^{n+1}} \end{aligned}$$

By the induction hypothesis, we know that $f(a_{n-1}) \equiv 0 \pmod{p^n}$. Hence we can write $f(a_{n-1}) \equiv \alpha' p^n \pmod{p^{n+1}}$. We now have

$$\alpha p^n + f'(a_{n-1})b_n p^n \equiv 0 \pmod{p^{n+1}} \iff \alpha' + f'(a_{n-1})b_n \equiv 0 \pmod{p}$$

Furthermore, since $a_{n-1} \equiv a_0 \pmod{p}$ it follows that $f'(a_{n-1}) \equiv f'(a_0) \not\equiv 0 \pmod{p}$. We can then solve for b_n in the above equation as done before for b_1. This completes the proof of the claim.

Now let $a = \tilde{a}_0 + b_1 p + \dots$. For all $n \geq 0$ we have $f(a) \equiv f(a_n) \equiv 0 \pmod{p^{n+1}}$ and thus $f(a) = 0$. The uniqueness of such an a follows directly from the uniqueness of the sequence. This completes the proof of the theorem. □

Example 2.2.2. Let p be an odd prime. Hensel's Lemma allows us to prove that $\mathbb{Z}_p$ contains a $(p-1)^{th}$ root of unity. Indeed, consider the polynomial $f(X) = X^{p-1} - 1$. By FF2, we have that every non-zero element of $\mathbb{F}_p$ is a root of $f(X)$. Furthermore, the formal derivative of $f(X)$ is given by $f'(X) = (p-1)X^{p-2}$. We have that

$$f'(X) \equiv -X^{p-2} \pmod{p}$$

whose only root modulo p is 0. Appealing to Hensel's lemma, we see that $\mathbb{Z}_p$ contains exactly $p-1$ $(p-1)^{th}$ roots of unity.

We end this section with a result that is of independent interest. For a proof of this theorem, see [Kob84, p.3–5]. Recall that two absolute values $|\cdot|_1$ and $|\cdot|_2$ defined on a field K are said to be **equivalent** if they induce the same topology on K; this is equivalent to saying that $|\cdot|_1 = |\cdot|_2^\alpha$ for some strictly positive $\alpha \in \mathbb{R}$.

Theorem 2.2.3 (Ostrowski's Theorem)**.** *Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. Then $|\cdot|$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.*

Ostrowski's Theorem immediately implies that the only possible non-trivial completions of $\mathbb{Q}$ are the p-adic numbers or the real numbers. This is another manifestation of the local-global phenomenae discussed earlier on in the introduction.

2.3 Absolute values on finite extensions of $\mathbb{Q}_p$

The main goal of this chapter is to construct an algebraically closed, complete field containing $\mathbb{Q}_p$. This will allow us to do analysis in a p-adic setting while also guaranteeing that all polynomials have roots. It turns out, as we shall soon see, that the p-adic situation is very different to the real situation. Indeed, the complex numbers can be obtained simply by adjoining $i = \sqrt{-1}$ to $\mathbb{R}$. We are not so lucky in the p-adic setting - there exists no such number, algebraic over $\mathbb{Q}_p$, which yields the p-adic analogue of $\mathbb{C}$.

Hence we must investigate the behaviour of finite field extensions of $\mathbb{Q}_p$. The first order of business is extending the p-adic absolute value $|\cdot|_p$ to finite extensions $K/\mathbb{Q}_p$.

Let V be a vector space defined over a field K equipped with an absolute value $|\cdot|$. Recall that two norms $||\cdot||_1$ and $||\cdot||_2$ on V are **equivalent** if they generate the same topology on V. Throughout this section, we shall provide some results concerning vector spaces over fields without proof. Such proofs can be found in either [Rob00, p.90-96] or [Gou93, p.123-136].

Theorem 2.3.1. *Let K be a field complete with respect to an absolute value and V a vector space over K. Then all norms on V are equivalent.*

Corollary 2.3.2. *Let K be a finite extension of $\mathbb{Q}_p$. Then there exists at most one absolute value on K extending $|\cdot|_p$.*

Let K be a finite extension of $\mathbb{Q}_p$ and let $\alpha \in K$ be of degree n over $\mathbb{Q}_p$. We seek to determine how $|\alpha|_p$ is defined if such an absolute value were to exist. Let L be a Galois extension of $\mathbb{Q}_p$ containing K. Let $G = \mathrm{Gal}(L/\mathbb{Q}_p)$. Suppose that $|\cdot|$ is an extension of the p-adic absolute value to L. By Corollary 2.3.2, $|\cdot|$ is the unique absolute value on L extending $|\cdot|_p$. It is easy to see that $|\sigma(\cdot)|$ is again an absolute value for all $\sigma \in G$ and so $|\sigma(\cdot)| = |\cdot|$. Hence the absolute value of α is equal to the absolute value of each of its conjugates. Now recall the **norm** of α from $\mathbb{Q}_p(\alpha)$ to $\mathbb{Q}_p$ is given by

$$\mathrm{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha) = \prod_{i=1}^{n} a_i$$

where the a_i are the conjugates of α. By definition, this is an element of $\mathbb{Q}_p$, namely the constant term of the minimal polynomial of α (up to a sign). Hence we may write

$$\begin{aligned} |\,\mathrm{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p &= |\,\mathrm{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)| \\ &= \left|\prod_{i=1}^{n} a_i\right| \\ &= |\alpha|^n \end{aligned}$$

Thus if there were to exist an absolute value $|\cdot|$ extending $|\cdot|_p$ to a finite extension $K/\mathbb{Q}_p$, it would necessarily be given by

$$|\alpha| = |\,\mathrm{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/n}$$

where n is the degree of the minimal polynomial of α over $\mathbb{Q}_p$. It remains to show that our definition of $|\cdot|$ is indeed an absolute value.

We must first take a detour and state some results regarding the topologies of p-adic fields. Recall that a topological space is **locally compact** if every point has a compact neighbourhood.

Lemma 2.3.3. *$\mathbb{Q}_p$ is locally compact with respect to the topology induced by $|\cdot|_p$.*

Proof. We claim that it suffices to show that $\mathbb{Z}_p$ is compact. Indeed, $\mathbb{Z}_p$ is simply the unit ball centered at 0. Then, given any non-zero point $x \in \mathbb{Q}_p$, $x + \mathbb{Z}_p$ is a compact neighbourhood of x. It then follows that $\mathbb{Q}_p$ would be locally compact.

Now since $|\cdot|_p$ induces the metric topology on $\mathbb{Z}_p$, it suffices to show that $\mathbb{Z}_p$ is sequentially compact. To this end, let $\{ \alpha_n \}$ be a sequence of p-adic integers. We need to show that $\{ \alpha_n \}$ has a convergent subsequence. We may write

$$\alpha_n = \sum_{i=0}^{\infty} a_i^{(n)} p^i$$

for all $n \in \mathbb{N}$. Appealing to the pigeonhole principle, there exists an element $c_0 \in \mathbb{F}_p$ such that $a_0^{(n)} = c_0$ for infinitely many n. Hence there exists a sequence of natural numbers n_j, indexed over j, such that $\{ \alpha_{n_j} \}$ is a sequence of p-adic integers all with the same first p-adic digit. We may continue this process inductively to obtain a collection of sequences, say $\{ \alpha_n^{(m)} \}_{n\in\mathbb{N}}$ for all $m \geq 0$. Here the m represents the fact that all terms in $\{ \alpha_n^{(m)} \}$ are the same up to, and including, the m^{th} p-adic digit. Taking the diagonal sequence of this collection, $\{ \alpha_k^{(k)} \}_{k\in\mathbb{N}}$, yields a subsequence of $\{ \alpha_n \}$ that converges to a p-adic integer. Thus the lemma is proved. □

Let K be a field equipped with an absolute value $|\cdot|$, V an n-dimensional vector space over K and $\{ v_1, \ldots, v_n \}$ a K-basis for V. Given $v = a_1v_1 + \cdots + a_nv_n \in V$, we define the **sup-norm** on V to be

$$|v|_{\text{sup}} = \max_{1\leq i\leq n} |a_i|$$

It is readily verified that the sup-norm is indeed a vector space norm.

Proposition 2.3.4. *Let K be a locally compact field equipped with an absolute value $|\cdot|$. Then any finite dimensional normed vector space over K is locally compact.*

Corollary 2.3.5. *Let K be a locally compact field equipped with an absolute value $|\cdot|$. Let V be a finite dimensional vector space over K. Then, with respect to some basis, the set*

$$S = \{ v \in V \mid |v|_{\text{sup}} = 1 \}$$

is compact.

We are finally ready to show that our proposed absolute value satisfies the conditions we desire:

Theorem 2.3.6. *Let K be a finite extension of $\mathbb{Q}_p$ and $\alpha \in K$. Let $n = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$. Then*

$$|\alpha|_K := |\operatorname{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/n}$$

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

Proof. It is clear from the definition of $\operatorname{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)$ that $|\alpha|_K = 0$ if and only if $\alpha = 0$. Furthermore, the definition of the norm also implies that $|\cdot|_K$ extends the original p-adic absolute value on $\mathbb{Q}_p$. Indeed, if $\alpha \in \mathbb{Q}_p$ then its minimal polynomial is $X - \alpha$ over $\mathbb{Q}_p$. Looking at the constant term of this shows that $|\cdot|_K$ agrees with the earlier definition for $\mathbb{Q}_p$. Now, by an equivalent definition, $\mathrm{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)$ is the determinant of the linear map

$$\mu_\alpha : \mathbb{Q}_p(\alpha) \mapsto \mathbb{Q}_p(\alpha)$$

$$x \mapsto \alpha x$$

Since determinants commute with matrix multiplication, so does $|\cdot|_K$. It remains to show that $|\cdot|_K$ satisfies the ultrametric inequality. Choose a $\mathbb{Q}_p$-basis for K, say $\{ v_1, \ldots, v_m \}$. Lemma 2.3.3 implies that $\mathbb{Q}_p$ is locally compact. Corollary 2.3.5 then implies that the set

$$S = \{ \alpha \in K \mid |\alpha|_{\text{sup}} = 1 \}$$

is compact with respect to the chosen basis. Since $|\cdot|_p$ is a continuous function[2] on K, and any continuous function is bounded on a compact set, it follows that for all $\alpha \in S$ we have

$$0 < c \leq |\alpha|_K \leq C$$

for some $c, C \in \mathbb{R}$. Now, given any $x \in K^\times$, we may choose a $\lambda \in \mathbb{Q}_p$ such that $|x|_{\text{sup}} = |\lambda|_p$. Thus $|x/\lambda|_{\text{sup}} = 1$ and we have

$$c \leq \left|\frac{x}{\lambda}\right|_K \leq C$$

This implies that

$$c|\lambda|_p \leq |x|_K \leq C|\lambda|_p \iff c\,|x|_{\text{sup}} \leq |x|_K \leq C\,|x|_{\text{sup}}$$

Now suppose that $|x|_K \leq 1$. Then

$$|1+x|_K \leq C\,|1+x|_{\text{sup}} \leq C \max\{|1|_{\text{sup}}, |x|_{\text{sup}}\} \leq C \max\{|1|_{\text{sup}}, c^{-1}\} = \varepsilon = \varepsilon \max\{|1|_K, |x|_K\}$$

for some $\varepsilon \in \mathbb{R}$.

Now, for the general case, suppose that $|y|_p \geq |x|_p$ for some $y, x \in \mathbb{K}^\times$. Then $|x/y|_p \leq 1$ and we can apply the above inequality to get

$$\left|1 + \frac{x}{y}\right|_K \leq \varepsilon \max\left\{|1|_K, \left|\frac{x}{y}\right|_K\right\}$$

Multiplying through by $|y|_K$ yields

$$|x+y|_K \leq \varepsilon \max\{|x|_K, |y|_K\}$$

To complete the proof, we note that $|\cdot|_K$ extends $|\cdot|_p$ which forces $\varepsilon = 1$. □

Henceforth, we shall denote this new absolute value by $|\cdot|_p$ as is befitting for an extension of the original p-adic absolute value on $\mathbb{Q}_p$.

[2] the determinant of μ_α is a continuous function on K since it can be expressed as the characteristic polynomial of μ_α

The theorem clearly implies that there exists a unique non-Archimedean absolute value on the algebraic closure of $\mathbb{Q}_p$ extending $|\cdot|_p$ on $\mathbb{Q}_p$. Indeed, if $\alpha \in \overline{\mathbb{Q}_p}$ then the absolute value of α in a finite extension of $\mathbb{Q}_p$ containing α is independent of the actual extension chosen - it depends simply on the element itself. It therefore makes sense to let $|\alpha|_p$ on $\overline{\mathbb{Q}_p}$ be equal to $|\alpha|_p$ in any finite extension of $\mathbb{Q}_p$ that contains α.

2.4 Structure and ramification of finite extensions of $\mathbb{Q}_p$

We now look towards examining the structure of certain key finite extensions of $\mathbb{Q}_p$. Let K be a finite extension of $\mathbb{Q}_p$ of degree n. Then there exists a unique extension of the p-adic absolute value to K. Given $\alpha \in K$, we can recover the p-adic valuation on K as follows:

$$v_p(\alpha) = -\log_p |\alpha|_p = -\log_p |\operatorname{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/n} = -\frac{1}{n}\log_p |\operatorname{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p$$

It is easily verified that v_p is a valuation on K from the corresponding properties of $|\cdot|_p$.

Now, v_p is clearly a homomorphism between the multiplicative group $K^\times$ and the additive group of $\mathbb{Q}$. In particular, $\operatorname{im}(v_p) \subseteq (1/n)\mathbb{Z}$. Choose some $a/e \in \operatorname{im}(v_p)$ such that a and e are coprime and e is the largest possible denominator. Then, by Bézout's identity, there exists integers x and y such that $ax + ey = 1$. It follows that

$$x\frac{a}{e} = \frac{1}{e} - y$$

Now, $x(a/e), y \in (1/n)\mathbb{Z}$ whence $1/e \in (1/n)\mathbb{Z}$. But e was chosen to be the greatest possible divisor of n so infact $\operatorname{im}(v_p) = (1/e)\mathbb{Z}$. e is referred to as the **index of ramification** of K over $\mathbb{Q}_p$. If $e = 1$ then K is an **unramified** extension. If $e = n$ then K is **totally ramified**.

Definition 2.4.1. Let $K/\mathbb{Q}_p$ be a finite extension of degree n. We define the **valuation ring** of K to be the set

$$\mathcal{O}_K = \{\, \alpha \in K \mid |\alpha|_p \leq 1 \,\}$$

whose unique maximal ideal is

$$\mathfrak{p}_K = \{\, \alpha \in K \mid |\alpha|_p < 1 \,\}$$

The fact that $\mathcal{O}_K$ is a ring and $\mathfrak{p}_K$ is the unique maximal ideal of $\mathcal{O}_K$ follows from the definition of $|\cdot|_p$. We call the field $\mathcal{O}_K/\mathfrak{p}_K$ the **residue field** of K. The following proposition justifies referring to $\mathcal{O}_K$ as the ring of integers of K:

Proposition 2.4.2. *Let $K/\mathbb{Q}_p$ be a finite extension of degree n. Then $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}_p$ in K.*

Proof. Let $\alpha \in K$ be integral over $\mathbb{Z}_p$. Then α is a root of some polynomial, say

$$f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in \mathbb{Z}_p$$

We claim that $|\alpha|_p \leq 1$. Suppose, for a contradiction, that $|\alpha|_p > 1$. Then

$$\begin{aligned} |\alpha|_p^m = |\alpha^m|_p = |a_{m-1}\alpha^{m-1} + \cdots + a_0|_p &\leq \max_{0 \leq i \leq m-1} |a_i \alpha^i|_p \\ &= \max_{0 \leq i \leq m-1} |\alpha^i|_p = |\alpha|_p^{m-1} \end{aligned}$$

which is a contradiction. Hence $\alpha \in \mathcal{O}_K$.

Now suppose that $\alpha \in \mathcal{O}_K$. We need to show that α is integral over $\mathbb{Z}_p$. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over $\mathbb{Q}_p$. Since all α_i have the same norm, we must have that $|\alpha_i|_p \leq 1$ for all $1 \leq i \leq n$. Let $f(X)$ be the minimal polynomial of α over $\mathbb{Q}_p$. Then the coefficients of $f(X)$ are sums and products of the α_i and thus the coefficients themselves must all lie in $\mathbb{Z}_p$. Hence α is integral over $\mathbb{Z}_p$. □

Proposition 2.4.3. *Let $K/\mathbb{Q}_p$ be a finite extension of degree n. Let e be the ramification index of the extension. If $\pi \in K$ satisfies $v_p(\pi) = 1/e$ then $\mathfrak{p}_K = \pi\mathcal{O}_K$. Such a π is referred to as a **uniformiser** of K.*

Proof. Since $\mathfrak{p}_K$ is the unique maximal ideal of $\mathcal{O}_K$, we must have that $\pi\mathcal{O}_K \subseteq \mathfrak{p}_K$.

Now let $x \in \mathfrak{p}_K$, we need to show that $x = \alpha\pi$ for some $\alpha \in \mathcal{O}_K$. This is equivalent to showing that $x\pi^{-1} \in \mathcal{O}_K$. We have that

$$v_p(x\pi^{-1}) = v_p(x) - v_p(\pi) = v_p(x) - \frac{1}{e}$$

Since e is the index of ramification of $K/\mathbb{Q}_p$ and $v_p(x) > 0$, we must have that $v_p(x) > 1/e$. This implies that $v_p(x\pi^{-1}) > 0$ which is equivalent to $x\pi^{-1} \in \mathcal{O}_K$. We therefore have that $\mathfrak{p}_K \subseteq \pi\mathcal{O}_K$ as desired. □

The following two results relate the index of ramification of a p-adic field to its degree over $\mathbb{Q}_p$. Their proofs can be found in [Gou93, p.146].

Proposition 2.4.4. *Let $K/\mathbb{Q}_p$ be a finite extension of degree n. Then $\mathcal{O}_K/\mathfrak{p}_K$ is a field extension of $\mathbb{F}_p$ of degree at most n; this is referred to as the **inertial degree** of K.*

Theorem 2.4.5. *Let $K/\mathbb{Q}_p$ be a finite extension of degree n. If e is the index of ramification of K and f is its inertial degree then $n = ef$.*

It turns out that Hensel's Lemma generalises to p-adic field extensions $K/\mathbb{Q}_p$. The following formulation will be very useful, especially for the proof of Dwork's Theorem

Theorem 2.4.6 (Hensel's Lemma)**.** *Let K be a finite extension of $\mathbb{Q}_p$ and $\pi \in K$ a uniformiser. Let $f(X) = c_nX^n + \cdots + c_0 \in \mathcal{O}_K[X]$. Denote by $f'(X)$ the formal derivative of $f(X)$. Suppose there exists an $a_0 \in \mathcal{O}_K$ such that $f(a_0) \equiv 0 \pmod{\pi\mathcal{O}_K}$ and $f'(a_0) \not\equiv 0 \pmod{\pi\mathcal{O}_K}$. Then there exists a unique algebraic integer $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv a_0 \pmod{\pi\mathcal{O}_K}$ and $f(\alpha) = 0$.*

Proof. The proof of this theorem is exactly the same as that of Theorem 2.2.1. We need only replace $\mathbb{Z}_p$ by $\mathcal{O}_K$ and reduction modulo p by reduction modulo $\pi\mathcal{O}_K$. □

Corollary 2.4.7. *Let $K/\mathbb{Q}_p$ be a finite extension. If f is the inertial degree of K then $\mathcal{O}_K^\times$ contains the cyclic group of $(p^f-1)^{th}$ roots of unity.*

Proof. The non-zero elements of the residue field $\mathcal{O}_K/\mathfrak{p}_K$ are a cyclic group of p^f-1 elements. These elements are the roots of the polynomial $f(X) = X^{p^f-1}-1$ over $\mathbb{O}_K/\mathfrak{p}_K$. We may choose a lift of these roots in $\mathcal{O}_K^\times$ and use this for Hensel's Lemma. Indeed, $f'(X) = -X^{p^f-2}$ which is non-zero for $X \neq 0$. Hensel's Lemma then shows that $\mathcal{O}_K^\times$ contains the cyclic group of $(p^f-1)^{th}$ roots of unity. □

Theorem 2.4.8. *There exists a unique unramified extension of $\mathbb{Q}_p$ of degree f and it is obtained by adjoining a primitive $(p^f-1)^{th}$ root of unity to $\mathbb{Q}_p$.*

Proof. Fix a generator $\overline{\alpha}$ of $\mathbb{F}_{p^f}^\times$ and let $\overline{f}(X) = X^f + \overline{a}_{f-1}X^{f-1} + \cdots + \overline{a}_0$ be its minimal polynomial over $\mathbb{F}_p$. For all $1 \leq i \leq f-1$, choose a lift of $\overline{a_i}$ in $\mathbb{Z}_p$ and label it a_i. Let $f(X) = X^f + a_{f-1}X^{f-1} + \cdots + a_0$. Then $f(X) \in \mathbb{Z}_p$ is irreducible over $\mathbb{Q}_p$. Indeed, if it were reducible, then we could write

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

for some $g(X), h(X) \in \mathbb{Z}_p[X]$. Reducing modulo p yields a decomposition of $\overline{f}(X)$ which contradicts the fact that $\overline{f}(X)$ is irreducible. Now let $\alpha \in \overline{\mathbb{Q}_p}$ be a root of $f(X)$. Let $K = \mathbb{Q}_p(\alpha)$ so that $[K : \mathbb{Q}_p] = f$. Now, $\alpha \in \mathcal{O}_K$ since it is the integral closure of $\mathbb{Z}_p$ in $\overline{K}$. Clearly, $\alpha + \mathfrak{p}_K$ is a root of $\overline{f}(X)$ in $\mathcal{O}_K/\mathfrak{p}_K$. We therefore have that $[\mathcal{O}_K/\mathfrak{p}_K : \mathbb{F}_p] \geq f$. By Proposition 2.4.4, we know that $f = [\mathcal{O}_K/\mathfrak{p}_K : \mathbb{F}_p] \leq [K : \mathbb{Q}_p] = f$. Hence $[\mathcal{O}_K/\mathfrak{p}_K : \mathbb{F}_p] = [K : \mathbb{Q}_p] = f$. By Theorem 2.4.5, we must have that the index of ramification is 1 and thus K is an unramified extension of $\mathbb{Q}_p$.

We now show that K is obtained by adjoining a primitive $(p^f-1)^{th}$ root of unity to $\mathbb{Q}_p$ and this is the unique such unramified extension of $\mathbb{Q}_p$. By Corollary 2.4.7, we have that K contains all the $(p^f-1)^{th}$ roots of unity. To prove that $K = \mathbb{Q}_p(\omega)$ for some primitive $(p^f-1)^{th}$ root of unity ω, we claim that the smallest extension of $\mathbb{Q}_p$ that contains all the $(p^f-1)^{th}$ roots of unity is of degree f and is therefore necessarily equal to K.

We have that $\mathbb{Q}_p \subseteq L = \mathbb{Q}_p(\omega) \subseteq K$. The conjugates of ω are the $(p^f-1)^{th}$ roots of unity and thus $\mathcal{O}_L/\mathfrak{p}_L$ must contain $\mathbb{F}_{p^f} \cong \mathcal{O}_K/\mathfrak{p}_K$. Since $[\mathcal{O}_L/\mathfrak{p}_L : \mathbb{F}_p] \leq [L : \mathbb{Q}_p]$, we must have that $[L : \mathbb{Q}_p] \geq f$. But then $f = [K : \mathbb{Q}_p] \geq [L : \mathbb{Q}_p] \geq f$ whence $[K : \mathbb{Q}_p] = [L : \mathbb{Q}_p]$. Hence $K = \mathbb{Q}_p(\omega)$ and we are done. □

2.5 The Teichmüller Lift

The following is of fundamental importance to Dwork's proof and merits its own section.

Recall from the previous section that there exists a unique unramified extension of degree f of $\mathbb{Q}_p$, say K, that is obtained by adjoining a primitive $(p^f-1)^{th}$ root of unity to $\mathbb{Q}_p$. K contains all the $(p^f-1)^{th}$ roots of unity and these can be obtained through lifting from the residue field of K to $\mathcal{O}_K$. This process of lifting elements of finite fields to roots of unity is called the **Teichmüller lift** and the p-adic roots of unity are the **Teichmuüller representatives** of the elements of $\mathbb{F}_{p^f}^\times$. Note that we can extend the Teichmüller lift to include the 0 element of $\mathbb{F}_{p^f}$ whose Teichmüller representative in the relevant p-adic field is 0.

More formally, let $f>0$ and K_f the unique unramified extension of $\mathbb{Q}_p$ of degree f. Then there exists a unique multiplicative group homomorphism called the Teichmüller lift

$$\tau_f : \mathbb{F}_{p^f} \to \mathcal{O}_{K_f}$$
$$a \mapsto \tau_f(a)$$

such that the following diagram commutes

$$\begin{tikzcd} & \mathcal{O}_{K_f} \arrow[dr, "\text{mod } \mathfrak{p}_{K_f}"] & \\ \mathbb{F}_{p^f} \arrow[ur, "\tau_f"] \arrow[rr, "\text{id}"'] & & \mathcal{O}_{K_f}/\mathfrak{p}_{K_f} \end{tikzcd}$$

Hence if $\mu_{p^f-1}(\mathcal{O}_{K_f})$ is the cyclic group consisting of the $(p^f-1)^{th}$ roots of unity in $\mathcal{O}_{K_f}$ then τ_f is a multiplicative homomorphism between $\mathbb{F}_{p^f}$ and $\mu_{p^f-1}(\mathcal{O}_{K_f}) \cup \{0\}$ such that $\tau_f(0)=0$.

2.6 Constructing $\mathbb{C}_p$

Recall, from earlier on in this chapter, that we are aiming to construct an algebraically closed, complete field containing $\mathbb{Q}_p$. We are now finally ready to construct such a field.

We first prove a result which shows the contrast between the behaviour of $\mathbb{C}$ and $\overline{\mathbb{Q}_p}$.

Proposition 2.6.1. *$\overline{\mathbb{Q}_p}$ has infinite degree over $\mathbb{Q}_p$.*

Proof. Let K be any finite extension of $\mathbb{Q}_p$ and $d \geq 2$. If π is a uniformiser for K then, clearly, $\pi\mathcal{O}_K$ is a prime ideal. Now consider the polynomial $X^d - \pi \in \mathcal{O}_K[X]$. This is Eisenstein at π and is thus irreducible over K. Hence, for each K, there exists an infinite family of irreducible polynomials so we must have that $\overline{\mathbb{Q}_p}$ is an infinite extension of $\mathbb{Q}_p$. □

This is clearly very different to the Archimedean case where $[\mathbb{C}:\mathbb{R}]=2$. The following result shows us that we are not yet done with constructing a p-adic analogue to $\mathbb{C}$.

Proposition 2.6.2. *$\overline{\mathbb{Q}_p}$ is not complete with respect to $|\cdot|_p$.*

Proof. It suffices to exhibit a Cauchy sequence $\{ c_i \} \subseteq \overline{\mathbb{Q}}_p$ that does not converge to any limit $c \in \overline{\mathbb{Q}}_p$. We first construct a sequence of roots of unity $\{ \zeta_i \}$, each lying in an unramified extension of $\mathbb{Q}_p$. Letting $\zeta_1 = 1$, we choose the next terms in the sequence with these conditions in mind:

1. $\zeta_{i-1} \in \mathbb{Q}_p(\zeta_i)$
2. $[\mathbb{Q}_p(\zeta_i) : \mathbb{Q}_p(\zeta_{i-1})] > i$

Indeed, let ζ_i be a primitive $(p^{(i+1)!}-1)^{th}$ root of unity for all $i \geq 2$. For the first condition, we first observe that $\mathbb{Q}_p(\zeta_{i-1}) \subseteq \mathbb{Q}_p(\zeta_i)$ if ζ_{i-1} divides ζ_i. Clearly, $i!|(i+1)!$ from which it follows that $p^{i!} - 1|p^{(i+1)!} - 1$. We thus see that $\zeta_{i-1}|\zeta_i$. Finally, we have that $[\mathbb{Q}_p(\zeta_i) : \mathbb{Q}_p] = (i+1)!$ and $[\mathbb{Q}_p(\zeta_{i-1}) : \mathbb{Q}_p] = i!$. Hence $[\mathbb{Q}_p(\zeta_i) : \mathbb{Q}_p(\zeta_{i-1})] = i + 1$.

Now consider the series $\sum_{i=0}^{\infty} \zeta_i p^i$ whose partial sums clearly form a Cauchy sequence in $\overline{\mathbb{Q}}_p$. We claim that this sequence does not converge to any limit in $\overline{\mathbb{Q}}_p$. Suppose, for a contradiction, that it converges to $c \in \overline{\mathbb{Q}}_p$. By definition, c is the root of a monic irreducible polynomial over $\mathbb{Q}_p$. Suppose that the degree of such a polynomial is d so that $[\mathbb{Q}_p(c) : \mathbb{Q}_p] = d$. Let c_d denote d^{th} partial sum of our series and consider

$$c - c_d = \sum_{i=d+1}^{\infty} \zeta_i p^i$$

Using the fact that $|\zeta_i|_p = 1$, we have

$$|c - c_d|_p \leq \sum_{i=d+1}^{\infty} |\zeta_i p^i|_p = \sum_{i=d+1}^{\infty} |p^i|_p \leq p^{-(d+1)}$$

Let σ be a $\mathbb{Q}_p$-automorphism of $\overline{\mathbb{Q}}_p$. σ must preserve $|\cdot|_p$ so we have that

$$|\sigma(c) - \sigma(c_d)|_p = |\sigma(c - c_d)|_p = |c - c_d|_p \leq p^{-(d+1)}$$

By construction, we have $[\mathbb{Q}_p(\zeta_d) : \mathbb{Q}_p(\zeta_{d-1})] = d + 1$. Hence there exist $d + 1$ $\mathbb{Q}_p(\zeta_{d-1})$-automorphisms of $\mathbb{Q}_p(\zeta_d)$. These fix all $\zeta_1, \ldots, \zeta_{d-1}$ but have distinct images of ζ_d.

If $i \neq j$ we have

$$\begin{aligned}\sigma_i(c_d) - \sigma_j(c_d) &= \left(\sum_{i=0}^{d-1} \zeta_i p^i + \sigma_i(\zeta_d) p^d\right) - \left(\sum_{i=0}^{d-1} \zeta_i p^i + \sigma_j(\zeta_d) p^d\right) \\ &= (\sigma_i(\zeta_d) - \sigma_j(\zeta_d)) p^d\end{aligned}$$

Now $\sigma_i(\zeta_d)$ and $\sigma_j(\zeta_d)$ are distinct $(p^{(i+1)!} - 1)^{th}$ roots of unity and thus they are not congruent modulo p. We thus have that

$$|\sigma_i(c_d) - \sigma_j(c_d)|_p = p^{-d}$$

We thus see that when applying the ultrametric inequality, equality infact holds:

$$\begin{aligned}&= \max\{|\sigma_i(c) - \sigma_i(c_d)|_p, |\sigma_i(c_d) - \sigma_j(c_d)|_p, |\sigma_j(c) - \sigma_j(c_d)|_p\}\\ &= p^{-d}\end{aligned}$$

This implies that $\sigma_i(c) \neq \sigma_j(c)$. Therefore, $\sigma_1(c), \ldots, \sigma_{d+1}(c)$ are $d+1$ distinct conjugates of c which means that the minimal polynomial of c over $\mathbb{Q}_p$ has degree $d+1$. This is clearly a contradiction as it was assumed that d was the degree of such a polynomial. Hence the Cauchy sequence $\{ c_i \}$ does not converge to any element in $\overline{\mathbb{Q}}_p$ and we are done. □

The previous theorem suggests to us that we should pass to the completion of $\overline{\mathbb{Q}_p}$ with respect to $|\cdot|_p$. Proceeding in the same way as we did earlier from $\mathbb{Q}$ to $\mathbb{Q}_p$, we construct the field of **complex p-adic numbers**, denoted $\mathbb{C}_p$. We may also extend $|\cdot|_p$ and v_p to $\mathbb{C}_p$ in exactly the same fashion. Hence we have a p-adic field that contains $\overline{\mathbb{Q}_p}$ as a dense subset and is complete with respect to a non-Archimedean absolute value $|\cdot|_p$. If we can show that $\mathbb{C}_p$ is algebraically closed then we have achieved our goal of constructing a p-adic analogue to $\mathbb{C}$.

Before we can accomplish this, we require the following small lemma:

Lemma 2.6.3 (Krasner's Lemma)**.** *Let K be a field complete with respect to a non-Archimedean absolute value $|\cdot|$. Let $f(X) \in K[X]$ be a polynomial with roots $\alpha = \alpha_1, \ldots, \alpha_n \in \overline{K}[X]$. If $\beta \in \overline{K}$ is such that*

$$|\beta - \alpha| < |\beta - \alpha_i|$$

for all $1 < i \leq n$ then $K(\alpha) \subseteq K(\beta)$

Proof. Let $L = K(\beta)$ and $F = L(\alpha_1, \ldots, \alpha_n)$. Then F/L is a Galois extension since F is the splitting field for the polynomial $f(X)$ over L. Let $\sigma \in \mathrm{Gal}(F/L)$ be an L-automorphism of F. Since $|\cdot|$ is invariant under the action of σ, we have

$$|\beta - \alpha| = |\sigma(\beta - \alpha)| = |\beta - \sigma(\alpha)|$$

Using this, we have

$$|\alpha - \sigma(\alpha)| \leq \max\{|\alpha - \beta|, \beta - \sigma(\alpha)\} = |\alpha - \beta| < |\alpha - \alpha_i|$$

for all $1 < i \leq n$. Since σ was arbitrary, we must have that $\alpha = \sigma(\alpha)$. Hence $\alpha \in L = K(\beta)$. □

Proposition 2.6.4. *$\mathbb{C}_p$ is algebraically closed.*

Proof. Let $\alpha \in \overline{\mathbb{C}_p}$. Let $f(X) = \sum_{i=1}^{n} a_i X^i \in \mathbb{C}_p[X]$ denote its minimal polymomial. Scaling $f(X)$, we may assume that it is an element of $\mathcal{O}_{\mathbb{C}_p}[X]$ and thus $|\alpha|_p \leq 1$. Let $\varepsilon = \min_{1 \leq i \leq n}(|\alpha - \alpha_i|_p)$ where the $\alpha = \alpha_1, \ldots, \alpha_n \in \overline{\mathbb{C}_p}$ are the conjugates of α. By construction, $\overline{\mathbb{Q}_p}$ is dense in $\mathbb{C}_p$ so we may choose $g(X) = \sum_{i=1}^{n} b_i X^i \in \mathcal{O}_{\overline{\mathbb{Q}_p}}$ such that $|a_i - b_i|_p < \varepsilon^n$.

Let $\beta_1, \ldots, \beta_n \in \overline{\mathbb{Q}_p}$ be the roots of $g(X)$. Then

$$\prod_{i=1}^{n} |\alpha - \beta_i|_p = g(\alpha) = |g(\alpha) - f(\alpha)|_p \leq \max_{1 \leq i \leq n} \{|a_i - b_i|_p\} < \varepsilon^n$$

Hence there exists at least one $1 \leq i \leq n$ such that $|\alpha - \beta_i|_p < \varepsilon = \min_{1 \leq i \leq n} |\alpha - \alpha_i|_p$. Appealing to Krasner's Lemma, we see that $\mathbb{C}_p(\alpha) \subseteq \mathbb{C}_p(\beta_i) = \mathbb{C}_p$. Since α was an arbitrary element of $\overline{\mathbb{C}_p}$, the proposition is proved. □

We have thus finally accomplished what we set out to do: we have constructed the p-adic analogue to $\mathbb{C}$. $\mathbb{C}_p$ is the smallest algebraically closed field that contains $\mathbb{Q}$ and is complete with respect to the p-adic absolute value $|\cdot|_p$. It is thus a perfect domain in which to perfom p-adic analysis and its usefulness will be immeasurable in the proof of Dwork's Theorem.

Chapter 3

p-adic analysis

The aim of this chapter is to investigate elementary p-adic analysis. In order to discuss Dwork's proof, we require an understanding of some of the standard mathematical functions. We also aim to prove two key results, Dwork's Lemma and the Weierstrass Preparation Theorem, which are at the heart of the proof of Dwork's Theorem.

3.1 The exponential, logarithm and binomial expansion

The main objects of study throughout this chapter will be power series with $\mathbb{C}_p$ coefficients. We will denote the ring of such objects by $\mathbb{C}_p[[X]]$. Let c and r be positive and strictly positive real numbers respectively. We denote the closed disc of radius r about c in $\mathbb{C}_p$ by $D_c[r]$. Similarly, we denote the open disc by $D_c(r)$. If $c = 0$ then we will drop the subscript and simply write $D[r]$ and $D(r)$.

We also recall Proposition 2.1.7 from Chapter 2 which states that a series converges with respect to a non-Archimedean absolute value if and only if the absolute values of its terms converge to 0.

Definition 3.1.1. Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in \mathbb{C}_p[[X]]$ be a power series. We define the **radius of convergence** of $f(X)$ to be

$$r = \limsup_{n\to\infty} |a_n|_p^{-\frac{1}{n}}$$

It is readily verified by a standard analytic argument that $f(X)$ converges if $|X|_p < r$ and diverges if $|X|_p > r$ (see [Kob84, p.76-77] for more details). If $X = r$ then one usually must check the convergence of the series explicitly.

Proposition 3.1.2. *Let $f(X) \in \mathbb{Z}_p[[X]]$ be a power series. Then $f(X)$ converges on $D(1)$.*

Proof. Let $f(X) = \sum_{i=0}^{\infty} a_i X^i$ for some $a_i \in \mathbb{Z}_p$ and suppose that $x \in D(1)$. Then, by hypothesis, $|x|_p < 1$ and $|a_i|_p \leq 1$ for all i. It thus follows that $|a_n x^n|_p \leq |x|_p^n$. This goes to 0 as $n \to \infty$ and hence $f(X)$ converges on $D(1)$. □

Proposition 3.1.3. *Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in \mathbb{C}_p[[X]]$ be a power series. If $f(X)$ converges on a (closed or open) disc D then $f(X)$ is continuous on that disc.*

Proof. Let $x, y \in D$. We assume that $x \neq 0$. Suppose there exists a $\delta > 0$ such that $|x - y|_p < \delta$ and

$\delta < |x|_p$. It follows immediately from the ultrametric inequality that $|x|_p = |y|_p$. Then

$$\begin{aligned}|f(x) - f(y)|_p &= \left|\sum_{i=0}^{\infty}(a_i x^i - a_i y^i)\right|_p \\ &\leq \max_{i\geq 0}\{|a_i x^i - a_i y^i|_p\} \\ &= \max_{i\geq 0}\{|a_i|_p(x-y)(x^{i-1} + x^{i-2}y + \cdots + xy^{i-2} + y^{i-1})\}\end{aligned}$$

We now observe that

$$|x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}|_p \leq \max_{1\leq i\leq n}\{|x^{n-1}y^{i-1}|_p\} = |x|_p^{n-1}$$

Hence

$$|f(x) - f(y)|_p \leq \max_{i\geq 0}\{|a_i|_p|x-y|_p|x|_p^{i-1}\} < \frac{\delta}{|x|_p}\max_{i\geq 0}(|a_i x^i|_p)$$

Now by hypothesis, $f(X)$ converges on a disc which means the absolute values of its terms converges to 0 on the same disc. Hence $|a_n x^n|_p$ is bounded above by some real constant. We may therefore, given $\varepsilon > 0$, make $|f(x) - f(y)| < \varepsilon$ by choosing a reasonable $\delta < |x|_p$.

The case where $x = 0$ is an immediate consequence of the convergence of $f(X)$ on D. □

Proposition 3.1.4. *The* **p-*adic logarithm*** *function defined by*

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

is a continuous function from $D(1)$ to $\mathbb{C}_p$.

Proof. We first calculate the radius of convergence of $\log_p(X)$. We have that

$$\lim_{n\to\infty}\left|\frac{(-1)^{n+1}}{n}\right|_p^{1/n} = \lim_{n\to\infty}|n^{-1/n}|_p = 1$$

Hence $\log_p(X)$ has radius of convergence 1. If $|x|_p = 1$ then we have

$$|a_n x^n|_p = |n^{-1}|_p \tag{3.1}$$

but this is greater than or equal to one for all $n \geq 1$. Hence the logarithm converges on $D(1)$. By Proposition 3.1.3, $\log_p(1+X)$ is therefore continuous on $D(1)$. □

Henceforth, the notation $\log_p$ shall refer excusively to the p-adic logarithm and not the standard real base-p logarithm.

Lemma 3.1.5 (Legendre's Formula)**.** *Let $n \in \mathbb{Z}$. Suppose that n has p-adic expansion $a_0 + a_1 p + \cdots + a_m p^m$ for some $a_i \in \mathbb{F}_p$. If $S_n = a_0 + \cdots + a_m$ then*

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

Proof. We first count the number of factors contributing to $v_p(n!)$. It is easy to see that there are $\lfloor n/p \rfloor$ multiples of p in n. Each of these multiples contributes one factor of p to $n!$. Similarly, each multiple of p^2 contributes a factor of p - there are $\lfloor n/p^2 \rfloor$ such factors. We continue like this to obtain an infinite sum for $v_p(n!)$. From the p-adic expansion of n, we see this sum must have only finitely many terms. We thus have that

$$v_p(n!) = \sum_{i=1}^{m} \left\lfloor \frac{n}{p^i} \right\rfloor$$

The lemma then follows upon inserting the p-adic expansion of n into the above equation and applying the standard formula for geometric series. □

Proposition 3.1.6. *The* ***p-adic exponential*** *function defined by*

$$\exp_p(X) = \sum_{i=0}^{n} \frac{X^n}{n!}$$

is a continuous function from $D(p^{-1/(p-1)})$ to $\mathbb{C}_p$.

Proof. We first calculate the radius of convergence of $\exp_p$. By Legendre's Formula, we have that

$$\begin{aligned} r &= \left(\limsup_{n\to\infty} \left| \frac{1}{n!} \right|_p^{1/n} \right)^{-1} \\ &= \left(\limsup_{n\to\infty} p^{(n-S_n)/n(p-1)} \right)^{-1} \\ &= p^{-1/(p-1)} \end{aligned}$$

as desired. Hence by Proposition 3.1.3, $\exp_p(X)$ is continuous on the disc $D(p^{-1/(p-1)})$. □

Theorem 3.1.7. *The p-adic logarithm is an isomorphism between the additive group of $D_1(p^{-1/(p-1)})$ and the multiplicative group of $D(p^{-1/(p-1)})$. It's inverse is the p-adic exponential.*

Proof. Let $x, y \in D(p^{-1/(p-1)})$. It suffices to prove the following three properties:

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

2. $\exp_p(x+y) = \exp_p(x)\exp_p(y)$

3. $\exp_p$ and $\log_p$ are mutually inverse.

It is easy to see that any series that converges under a non-Archimedean absolute value is absolutely convergent and we may thus rearrange terms so that, in the first property, we have

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

for some rational numbers c_{mn}. Now, the first property must hold in $\mathbb{Q}[[X,Y]]$ so the only non-zero coefficients in the above series are $a_{n0} = a_{0n} = \sum_{i=1}^{\infty}(-1)^{n+1}/n$ and thus the first property is proven over $\mathbb{C}_p[[X,Y]]$. The second property follows in exactly the same way.

We can apply the same reasoning to the third property but we must ensure that there are no issues with convergence. Indeed, let $x \in D(p^{-1/(p-1)})$. Then

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

whence $\exp_p(x) - 1 \in D(1)$. It then follows that $\log_p(1 + \exp_p(x) - 1) = x$.

Conversely, we have that

$$v_p(\log_p(1+x)) \geq \min_{n\geq 1} v_p\left(\frac{x^n}{n}\right)$$

We claim that this is greater than $(p-1)^{-1}$. Indeed

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

By inspection we see that the right hand side is equal to 0 when $n = 1, p$ and is greater than 0 everywhere else. The claim is thus proved. Hence $\log_p(1+x) \in D(p^{-1/(p-1)})$ and $\exp_p(\log_p(1+x)) = 1 + x$ as required. □

Definition 3.1.8. Let $a \in \mathbb{C}_p$. We define the **p-adic binomial expansion** to be

$$B_{a,p}(X) = \sum_{n=0}^{\infty} \frac{a(a-1)\dots(a-n+1)}{n!}X^n$$

Proposition 3.1.9. *Let $a \in \mathbb{Z}_p$. Then $B_{a,p}(X) \in \mathbb{Z}_p[[X]]$ and is continuous on $D(1)$.*

Proof. We must first show that

$$\frac{a(a-1)\dots(a-n+1)}{n!} \in \mathbb{Z}_p$$

Consider the polynomial $f(X) = X(X-1)\dots(X-n+1)$. This is clearly a continuous function hence there exists an $a_0 \in \mathbb{Z}$ and a $\delta > 0$ such that if $|a - a_0|_p \leq \delta$ then $|f(a) - f(a_0)|_p \leq 1$. Clearly, we can choose a_0 such that

$$\left|\frac{f(a)}{n!} - \frac{f(a_0)}{n!}\right|_p \leq 1$$

Now, $f(a_0)/n! \in \mathbb{Z}$. This implies that

$$\left|\frac{f(a_0)}{n!}\right|_p \leq 1$$

By the ultrametric inequality, it follows that

$$1 \geq \left|\frac{f(a)}{n!}\right|_p = \left|\frac{a(a-1)\dots(a-n+1)}{n!}\right|_p$$

and thus $B_{a,p}(X) \in \mathbb{Z}_p[[X]]$. By Proposition 3.1.2, $B_{a,p}(X)$ converges on $D(1)$ and is thus continuous on the same disc. □

The binomial expansion is very useful for constructing roots of certain numbers. Indeed, let $a = 1/n$ for some n not divisible by p. Then $a \in \mathbb{Z}_p$ and we have the following given $x \in D(1)$

$$(B_{a,p}(X))^n = 1 + X$$

which follows from consideration of the same identity over $\mathbb{Q}[[X]]$. Hence $B_{a,p}(x)$ is an n^{th} root of $1 + x$. This motivates the following notation for rational a:

$$B_{a,p}(X) = (1 + X)^a$$

3.2 Dwork's Lemma

We will now prove an extraordinary result due to Dwork. Using this lemma, we shall construct a power series which will be of importance to us in the discussion of Dwork's proof.

Recall from elementary ring theory that if R is a commutative ring with unity then $f(X) \in R[[X]]$ is invertible in $R[[X]]$ if and only if the constant term of $f(X)$ is invertible in R.

Theorem 3.2.1 (Dwork's Lemma). *Let* $f(X) = 1 + \sum_{n=1}^{\infty} a_n X^n \in 1 + X\mathbb{Q}_p[[X]]$. *Then* $f(X) \in 1 + X\mathbb{Z}_p[[X]]$ *if and only if*

$$\frac{f(X^p)}{(f(X))^p} \in 1 + pX\mathbb{Z}_p[[X]]$$

Proof. First suppose that $f(X) \in 1 + X\mathbb{Z}_p[[X]]$. Recall that $(a + b)^p \equiv a^p + b^p \pmod p$. Furthermore, if $a \in \mathbb{Z}_p$, then it is easy to see that $a^p \equiv a \pmod p$. Indeed, the constant term, say a_0, of a is an element of $\mathbb{F}_p$ and must satisfy $a_0^{p-1} = 1$. We thus have that $f(X)^p \equiv f(X^p) \pmod p$. Hence $f(X)^p = f(X^p) + pg(X)$ for some $g(X) \in X\mathbb{Z}_p[[X]]$. Now, $f(X)^p \in 1 + \mathbb{Z}_p[[X]]$ is invertible and we then have that

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

as required.

Conversely, we have that

$$f(X^p) = (f(X))^p g(X)$$

for some $g(X) \in 1 + pX\mathbb{Z}_p[[X]]$. Now writing $f(X) = \sum_{i=0}^{\infty} a_i X^i$ and $g(X) = \sum_{i=0}^{\infty} b_i X^i$. We need to show that each $a_i \in \mathbb{Z}_p$. By hypothesis, we have $a_0 = 1$. We prove by induction on i. Suppose the statement is true for all $i < n$. We first examine the coefficients of the left hand side. It is easy to see that if $p|n$ then the coefficient of X^n on the left hand side is $a_{n/p}$. Otherwise, the coefficient is 0.

Expanding the right hand side, we have

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

We first consider A modulo p. We have that

$$\begin{aligned}\left(\sum_{i=0}^{n} a_i X^i\right)^p &\equiv \sum_{i=0}^{\infty} a_i^p X^{pi} \pmod p\\ &= \sum_{i=0}^{\infty} a_i X^{pi}\end{aligned}$$

It is thus clear that the only term contributing to the coefficient of X^n, which is not congruent to 0 modulo p, is $a_{n/p}$ in the case that p divides n. We may thus subtract $a_{n/p}$ from both sides when equating coefficients. By this analysis, we see that all other possible terms that contribute to the coefficient X^n in A are elements of $p\mathbb{Z}_p$. Now, it is easy to see (by a multinomial expansion or otherwise) that the coefficient of X^n in A is of the form $pa_n + \alpha$ for some $\alpha \in p\mathbb{Z}_p$. This is because, by hypothesis, α is a sum of products of a_i's for $i < n$. By hypothesis, these a_i are elements of $\mathbb{Z}_p$ and we have just seen that they are each congruent to 0 modulo p.

Now, the coefficient of X^n in the power series represented by BC is an element of $p\mathbb{Z}_p$. Indeed, each b_i is an element of $p\mathbb{Z}_p$ and the only terms from B that will contribute are similar to the above analysis and are thus also in $p\mathbb{Z}_p$. Rearranging, we thus see that $pa_n \in p\mathbb{Z}_p$ and hence $a_n \in \mathbb{Z}_p$ □

Intuitively, the quotient in Dwork's Lemma is a measure of how well the power series $f(X)$ commutes with the map $X \mapsto X^p$. Formulating the lemma this way, we see that if $f(X)$ commutes up to modulo p with the p^{th} power map then $f(X)$ has p-adic integral coefficients. Note that Dwork's Lemma can be generalised to any number of indeterminates by the same proof.

We will now use Dwork's Lemma to show that a certain power series, which we shall make use of later on, has p-adic integral coefficients.

Proposition 3.2.2. *Let $F(X,Y) \in \mathbb{Q}_p[[X,Y]]$ be defined as follows:*

$$F(X,Y) = B_{X,p}(Y)B_{(X^p-X)/p,p}(Y^p)B_{(X^{p^2}-X^p)/p^2,p}(Y^{p^2})\ldots$$

where $B_{a,p}(X)$ is the p-adic binomial expansion. Then $F(X,Y) \in \mathbb{Z}_p[[X,Y]]$.

Proof. We must first check that this series is a well-defined element of $1 + (X,Y)\mathbb{Q}_p[[X,Y]]$. Using the shorthand notation for $B_{X,p}(Y)$ we have

$$\begin{aligned}F(X,Y) &= (1+Y)^X(1+Y^p)^{(X^p-X)/p}(1+Y^{p^2})^{(X^{p^2}-X^p)/p^2}\dots(1+Y^{p^n})^{(X^{p^n}-X^{p^{n-1}})/p^n}\dots\\ &= \left(\sum_{i=0}^{\infty}\frac{X(X-1)\dots(X-i+1)}{i!}Y^i\right)\times\\ &\prod_{n=1}^{\infty}\left[\sum_{i=0}^{\infty}\frac{X^{p^n}-X^{p^{n-1}}}{p^n}\left(\frac{X^{p^n}-X^{p^n-1}}{p^n}-1\right)\dots\left(\frac{X^{p^n}-X^{p^n-1}}{p^n}-i+1\right)\frac{Y^{ip^n}}{i!}\right]\end{aligned}$$

The above expansion implies that the coefficient of any X^mY^n can be calculated with only finitely many terms of the infinite product. Furthermore, we can easily see that $F(X,Y) = \sum_{m,n\geq 0} a_{mn}X^mY^n \in 1+(X,Y)\mathbb{Q}_p[[X,Y]]$.

It remains to show that $a_{mn} \in \mathbb{Z}_p$. Setting up for Dwork's Lemma gives us

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

We claim that the above is in $1+(pX,pY)\mathbb{Z}_p[[X,Y]]$. Dwork's Lemma would then imply that $F(X,Y)$ has coefficients in $\mathbb{Z}_p$. Now, $1+Y \in 1+Y\mathbb{Z}_p[[Y]]$ and the forward implication of Dwork's Lemma implies that

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

for some $Z(Y) \in \mathbb{Z}_p[[Y]]$. From this we obtain

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

This is obviously an element of $1+(pX,pY)\mathbb{Z}_p[[X,Y]]$ and thus $F(X,Y) \in \mathbb{Z}_p[[X,Y]]$ by Dwork's Lemma. □

3.3 The Weierstrass Preparation Theorem

This section is concerned with proving a p-adic analogue of the classical Weierstrass Preparation Theorem. It is one of the main tools of Dwork's proof of the rationality of the zeta-function. In order to accomplish this, we shall introduce the theory of Newton polygons.

Newton polygons can be thought of as 'physical' representations of certain properties of power series. In most cases, Newton polygons make it easier to read off the radius of convergence of power series.

We shall begin by introducing Newton polygons for polynomials which are a simpler case to handle.

Definition 3.3.1. Let $f(X) = \sum_{i=0}^{n} a_iX^i \in 1+X\mathbb{C}_p[X]$ be a polynomial. Consider the sequence of points in $\mathbb{R}^2$ defined by

$$\alpha_i = (i, v_p(a_i))$$

for $i \geq 0$. We define the **Newton polygon** of $f(X)$ to be the lower convex hull of the sequence $\{ \alpha_i \}$. The **slope** of a segment of the Newton polygon joining the points $(i, a), (i', a')$ is its gradient $(a' - a)/(i' - i)$. Its **length** is $i' - i$.

Let $f(X) = \sum_{i=0}^{n} a_i X^i$. To understand how the Newton polygon of $f(X)$ is constructed, we place pegs at each point $(i, v_p(a_i))$ in $\mathbb{R}^2$. We then connect a wire to the peg at $(0, 0)$ and pull the wire up from beneath all the other pegs. The path the wire takes is the Newton polygon of $f(X)$.

Lemma 3.3.2. *Let $f(X) = \sum_{i=0}^{n} a_i X^i \in 1 + X\mathbb{C}_p[X]$ and let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}_p$ be its roots. Let $\lambda_i = v_p(1/\alpha_i)$. If λ is a slope of the Newton polygon of $f(X)$ with length l, then necessarily l of the λ_i are equal to λ.*

Proof. The following factorisation of $f(X)$ into its recpirocal roots will be helpful in the proof of the lemma:

$$f(X) = \left(1 - \frac{X}{\alpha_1}\right) \ldots \left(1 - \frac{X}{\alpha_n}\right)$$

Let the α_i be numbered such that $\lambda_1 \leq \cdots \leq \lambda_n$. Suppose there is an $r \geq 1$ such that $\lambda_1 = \cdots = \lambda_r < \lambda_{r+1}$. We claim that the Newton polygon of $f(X)$ has first segment joining the points $(0, 0)$ and $(r, r\lambda_1)$.

The coefficients of $f(X)$ are symmetric polynomials in the $1/\alpha_i$ whence it follows that $v_p(a_i) \geq i\lambda_1$. Hence $(i, v_p(a_i))$ lies on or above the line joining the points $(0, 0)$ and $(r, r\lambda_1)$.

Of the r products of the $1/\alpha_i$, the one with minimal p-adic valuation of $r\lambda_1$ is $1/(\alpha_1 \ldots \alpha_r)$, the rest must include a λ_i with $i > r$ and thus all others must have p-adic valuation larger than $r\lambda_1$. Since a_r is the sum of such products, it follows by the ultrametric inequality that $v_p(a_r) = r\lambda_1$. By the same argumentation, we see that, for $i > r$, $v_p(a_i) > i\lambda_1$. Hence the line joining $(0, 0)$ to $(r, r\lambda_1)$ is actually a segment of the Newton polygon.

Now if $\lambda_{r+1} = \cdots = \lambda_s < \lambda_{s+1}$ for some $r + 1 \leq s \leq n$ then we can apply the previous reasoning to see that the next segment is the line joining the points $(r, v_p(\lambda_r))$ and $(s, v_p(\lambda_s))$. Continuing this way we see that the Newton polygon is indeed in the form claimed in the lemma. □

Definition 3.3.3. Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ be a power series (which is not a polynomial). We define the **Newton polygon** of $f(X)$ to be the limit of the Newton polygons of the partial sums of $f(X)$.

We distinguish three different possibilities for the Newton polygon of a power series $f(X) = \sum_{i=0}^{\infty} a_i X^i$:

1. The Newton polygon of $f(X)$ has infinitely many segments, all of finite length

2. The Newton polygon of $f(X)$ has finitely many segments with an infinitely long last segment that contains infinitely many of the points $(i, v_p(a_i))$

3. The Newton polygon of $f(X)$ has finitely many segements with an infinitely long last segment that contains only finitely many of the points $(i, v_p(a_i))$

We now prove a series of lemmata which provide us with the tools we need to prove the p-adic Weierstrass Preparation Theorem.

Lemma 3.3.4. *Let $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\mathbb{C}_p[[X]]$. If b is the supremum of all slopes of the Newton polygon of $f(X)$ then the radius of convergence of $f(X)$ is p^b. In the case that the supremum b is infinite, $f(X)$ converges everywhere in $\mathbb{C}_p$.*

Proof. Suppose that $v_p(x) > -b$. Let $c < b$ be such that $v_p(x) = -c$. Then $v_p(a_i x^i) = v_p(a_i) - ic$. Now, for sufficiently large i, we must have that $(i, v_p(a_i))$ lies above (i, ic) and thus $v_p(a_i x^i) \to \infty$ as $i \to \infty$. Hence $f(X)$ converges at $X = x$.

Conversely, suppose that $\mathrm{ord}_p(x) < -b$. Say $v_p(x) = -c$ for $c > b$. We have $v_p(a_i x^i) = v_p(a_i) - ci$. Now, infinitely many of the $(i, v_p(a_i))$ lie below (i, ci) meaning $v_p(a_i x^i)$ is negative for infinitely many i. Therefore, $f(X)$ can not converge whence $f(X)$ has radius of convergence p^b. □

Lemma 3.3.5. *Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in 1 + X\mathbb{C}_p[[X]]$. If $c \in \mathbb{C}_p$ with $v_p(c) = \lambda$ then the Newton polygon for $f(X/c)$ is constructed by removing the line $y = \lambda x$ from the Newton polygon of $f(X)$*

Proof. Suppose that $f(X/c) = \sum_{i=0}^{\infty} b_i X^i$. Then $v_p(b_i) = v_p(a_i/c^i) = v_p(a_i) - \lambda i$. This is equivalent to taking away the line $y = \lambda x$ from the Newton polygon of $f(X)$. □

Lemma 3.3.6. *Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ with λ_1 the first slope of the Newton polygon of $f(X)$. Suppose $c \in \mathbb{C}_p$ is such that $v_p(c) = \lambda \leq \lambda_1$. Furthermore, suppose that $f(X)$ converges on the disc $D[p^\lambda]$. If $g(x) = (1 - cX)f(x)$ then the Newton polygon of $g(X)$ is constructed by adjoining the Newton polygon of $f(X)$ to that of the polynomial $1 - cX$. Furthermore, if the last slope of $f(X)$ is λ_f then $f(X)$ converges on $D[p^{\lambda_f}]$ if and only if $g(X)$ converges on $D[p^{\lambda_f}]$.*

Proof. We first prove the case where $c = 1$ and $\lambda = 0$. Let $g(X) = \sum_{i=0}^{\infty} b_i X^i$. Since $g(X) = (1-X)f(X)$ we can write $b_{i+1} = a_{i+1} - a_i$ for all $i \geq 0$. Hence

$$v_p(b_{i+1}) \geq \min\{v_p(a_{i+1}), v_p(a_i)\} \tag{3.2}$$

Equality holds in the above proposition if and only if $v_p(a_{i+1}) \neq v_p(a_i)$. Now if $(i, v_p(a_i))$ is a vertex of the Newton polygon of $f(X)$ then, necessarily, $v_p(a_{i+1}) > v_p(a_i)$ whence $v_p(b_{i+1}) = v_p(a_i)$. We can therefore see that the Newton polygon of $g(X)$ has the proposed shape up till at least the last vertex. Since Equation 3.2 holds, we know that $g(X)$ converges wherever $f(X)$ does. It remains to show that if the Newton polygon of $f(X)$ has infinite final slope λ_f then so does the Newton polygon of $g(X)$. Let λ_g be a slope of the Newton polygon of $g(X)$ such that $\lambda_g > \lambda_f$. Then for sufficiently large i, the point $(i+1, v_p(a_i))$ would be below the Newton polygon of $g(X)$. It then follows that $v_p(b_j) > v_p(a_i)$ for all $j \geq i+1$. Since $a_{i+1} = b_{i+1} + a_i$, the properties of the ultrametric inequality imply that $v_p(a_{i+1}) = v_p(a_i)$. Similarly, $v_p(a_{i+1}) = v_p(a_{i+1})$. Continuing in this way, we see that $v_p(a_j) = v_p(a_i)$ for all $j > i$. But this is a contradiction to the assumption that $f(X)$ converges on $D[1]$. Hence there can exist no such slope λ_g.

To prove the general case, we note that $\alpha(X) = f(X/c)$ and $\beta(X) = (1-X)\alpha(X)$ satisfy the conditions required for the previous special case. The previous reasoning then allows us to determine the shape of the Newton polygon of $\beta(X)$. Since $g(X) = \beta(cX)$ we can apply Lemma 3.3.6 to obtain the Newton polygon for $g(X)$. □

Lemma 3.3.7. *Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ be a power series whose Newton polygon has first slope λ_1. If the Newton polygon of $f(X)$ has more than one slope then there exists $y \in \mathbb{C}_p$ satisfying $f(y) = 0$ and $v_p(y) = -\lambda_1$.*

Proof. We first prove the case where $\lambda_1 = 0$. In this case, we clearly have that $v_p(a_i) \geq 0$ for all i. Since the Newton polygon is convex and it has at least two slopes, we must have that $v_p(a_i) \to \infty$ as $i \to \infty$. Let $M \geq 1$ be the greatest natural number such that $v_p(a_M) = 0$. Furthermore, let $f_n(X)$ denote the partial sums of $f(X)$. Lemma 3.3.2 implies that, for all $n \geq M$, $f_n(X)$ has exactly M roots $x_1^{(n)}, \ldots, x_M^{(n)}$ such that $v_p(x_i^{(n)}) = 0$ for all $1 \leq i \leq M$. We inductively define a sequence $\{\, y_n \,\}_{n \geq M}$ by $y_M = x_1^{(M)}$ and for all $n \geq M$ we choose a root $x_i^{(n+1)}$ such that $|x_i^{(n+1)} - y_n|_p$ is minimal. We claim that $\{\, y_n \,\}$ is a Cauchy sequence. Furthermore, the limit of this sequence, say y, will satisfy $f(y) = 0$ as desired.

For all $n \geq M$ let R_n be the collection of all roots of $f_n(X)$ (including all repeated roots). We have that

$$\begin{aligned} |f_{n+1}(y_n) - f_n(y_n)|_p &= |f_{n+1}(y_n)|_p \\ &= \prod_{x \in R_{n+1}} \left|1 - \frac{y_n}{x}\right|_p \end{aligned}$$

Now if $x \in R_{n+1}$ is a zero that is not equal to one of the $x_i^{(n+1)}$ then necessarily $v_p(x) < 0$. By the ultrametric inequality we have

$$v_p\left(1 - \frac{y_n}{x}\right) \geq \min\left\{v_p(1), v_p\left(\frac{y_n}{x}\right)\right\} = \min\{0, v_p(y_n) - v_p(x)\} = 0$$

with equality holding throughout. Hence

$$\begin{aligned}
|f_{n+1}(y_n) - f_n(y_n)|_p &\geq \prod_{i=1}^{M} \left| 1 - \frac{y_n}{x_i^{y_{n+1}}} \right|_p \\
&= \prod_{i=1}^{M} |x_i^{(n+1)} - y_n|_p \\
&\geq |y_{n+1} - y_n|_p^M
\end{aligned}$$

where in the last line we have used the fact that we chose y_{n+1} to minimise $|x_i^{(n+1)} - y_n|_p$. Rewriting this, we observe that

$$|y_{n+1} - y_n|_p^M \leq |f_{n+1}(y_n) - f_n(y_n)|_p = |a_{n+1} y_n^{n+1}|_p = |a_{n+1}|_p$$

By hypothesis, $|a_{n+1}|_p \to 0$ as $n \to \infty$. Hence $\{ y_n \}$ is Cauchy. Denote its limit by $y \in \mathbb{C}_p$. We thus have that $v_p(y) = 0 = -\lambda_1$ as proposed by the lemma.

To show that y satisfies $f(y) = 0$, we first note that $f(y) = \lim_{n\to\infty} f_n(y)$. Furthermore,

$$|f_n(y)|_p = |f_n(y) - f_n(y_n)|_p = \left| \sum_{i=1}^{n} a_i (y^i - y_n^i) \right|_p = |y - y_n|_p \left| \sum_{i=1}^{n} a_i \frac{y^i - y_n^i}{y - y_n} \right|_p$$

We now observe that $|a_i|_p \leq 1$ and that

$$\left| \frac{y^i - y_n^i}{y - y_n} \right|_p = |y^{i-1} + y^{i-2} y_n + \cdots + y_n^{i-1}|_p \leq 1$$

Hence $|f_n(y)|_p \leq |y - y_n|_p$ whence $f(y) = \lim_{n\to\infty} f_n(y) = 0$. This completes the proof for the case where $\lambda_1 = 0$.

To prove the lemma in full generality, let $c \in \mathbb{C}_p$ be any number such that $v_p(c) = \lambda_1$. Let $\alpha(X) = f(X/c)$. Then the Newton polygon of $\alpha(X)$ has first slope 0 and we may apply the previous argumentation to see that there exists $x_0 \in \mathbb{C}_p$ $\alpha(x_0) = 0$ and $v_p(x_0) = 0$. Now take $x = x_0/c$. Then $v_p(x) = -\lambda_1$ and $f(x) = f(x_0/c) = \alpha(x_0) = 0$. □

Lemma 3.3.8. *Let $f(X) = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ and $\alpha \in \mathbb{C}_p$ such that $f(\alpha) = 0$. Let $\beta(X) = 1 + \sum_{i=1}^{\infty} b_i X^i \in 1 + X\mathbb{C}_p[[X]]$ be such that*

$$\beta(X) = f(X) \left(1 + \frac{X}{\alpha} + \frac{X^2}{\alpha^2} + \ldots \right)$$

Note that this is equivalent to dividing $f(X)$ by the polynomial $1 - X/\alpha$. Then $\beta(X)$ converges on the disc $D[|\alpha|_p]$.

Proof. Let $f_n(X)$ denote the n^{th} partial sum of $f(X)$. Equating coefficents we see that

$$b_i = \frac{1}{\alpha^i} + \frac{a_1}{\alpha^{i-1}} + \cdots + \frac{a_{i-1}}{\alpha} + a_i$$

and thus $b_i \alpha^i = f_i(\alpha)$. It then follows that $\lim_{i\to\infty} |b_i \alpha^i|_p = \lim_{i\to\infty} |f_i(\alpha)|_p = 0$. □

Theorem 3.3.9 (Weierstrass Preparation Theorem)**.** *Let $f(X) = \sum_{i=0}^{\infty} a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ be a power* *series converging on a disc $D[p^\lambda]$. If the Newton polygon of $f(X)$ does not have an infinitely long last slope of λ then let N denote the total length of slopes less than or equal to λ. Otherwise, let N be the greatest i such that $(i, v_p(a_i))$ lies on the last segment. Then there exists a degree N polynomial $h(X) \in 1 + X\mathbb{C}_p[X]$ and a power series $g(X) = 1 + \sum_{i=1}^\infty a_i X^i \in 1 + X\mathbb{C}_p[[X]]$ which converges and is non-vanishing on $D[p^\lambda]$ such that*

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

Furthermore, this polynomial is unique and its Newton polygon coincides with that of $f(X)$ up to $(N, v_p(a_N))$.

Proof. We prove the theorem by induction on N. Suppose that $N = 0$. This is equivalent to showing that the inverse power series $g(X)$ of $f(X)$ is convergent and non-vanishing on $D[p^\lambda]$. As in the proof of the previous lemmata, we may reduce to the case where $\lambda = 0$ without loss of generality.

We have that $v_p(a_i) > 0$ and $v_p(a_i) \to \infty$ as $i \to \infty$; we need to show that $v_p(b_i) > 0$ and $v_p(b_i) \to \infty$ as $i \to \infty$. Equating coefficients, we see that

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

for all $i \geq 0$. By induction, it is clear that $v_p(b_i) > 0$ for all i.

Now fix some $\varepsilon > 0$ and choose $n \in \mathbb{N}$ so that if $i > n$ then $v_p(a_i) > \varepsilon$ (we can always do this since $v_p(a_i) \to \infty$). Define

$$\delta = \min_{1 \leq i \leq m} \{v_p(a_i)\}$$

We shall show, by induction on m, that $i > mn$ implies $v_p(b_i) > \min\{\varepsilon, m\delta\}$. The claim is clearly true for $m = 0$ so suppose it is true for arbitrary $m - 1$ and that $i > mn$. Again, we have

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

If $j > n$, we have that $v_p(b_{i-j}a_j) \geq v_p(a_j) > \varepsilon$. Conversely if $j \leq n$ then $v_p(b_{i-j}a_j) \geq v_p(b_{i-j}) + \delta$. Now, $i - j > (m-1)n$ and thus, by the induction hypothesis, we have $v_p(b_{i-j}a_j) \geq \min\{\varepsilon, (m-1)\delta\} + \delta$. Expanding this out, we see that all terms in the expression for b_i have p-adic valuation greater than $\min\{\varepsilon, m\delta\}$ as required. Now, taking $m \to \infty$, we see that $v_p(b_i) \to \infty$ and thus the theorem is true for $N = 0$.

Suppose that the theorem is true for arbitrary $N-1$. Let $\lambda_1 \leq \lambda$ denote the first slope of the Newton polygon of $f(X)$. Lemma 3.3.7 guarantees the existence of a root of $f(X)$, say α, such that $v_p(\alpha) = -\lambda_1$. Define

$$f_\alpha(X) = f(X)\left(1 + \frac{X}{\alpha} + \frac{X^2}{\alpha^2} + \dots\right)$$

Lemma 3.3.8 implies that $f_\alpha(X)$ converges on $D[p^{\lambda_1}]$. Denote $c = 1/\alpha$ so as to write $f(X) = (1 -$

$cX)f_\alpha(X)$. Let λ_1' be the first slope of the Newton polygon of $f_\alpha(X)$. If $\lambda_1' < \lambda_1$ then Lemma 3.3.7 would imply that $f_\alpha(X)$ would have a root with p-adic valuation $-\lambda_1'$. But then so would $f(X)$ which is a contradiction. Hence $\lambda_1' \geq \lambda_1$. Now, Lemma 3.3.6 implies that $f_\alpha(X)$ has the same Newton polygon as $f(X)$ except for the segment joining $(0,0)$ to $(1,\lambda_1)$. Now, since $f(X)$ converges on $D[p^\lambda]$, this lemma also implies that $f_\alpha(X)$ converges on the same disc.

We can now apply the induction hypothesis to $f_\alpha(X)$ to find a polynomial $h_\alpha(X) \in 1 + X\mathbb{C}_p[[X]]$ of degree $N-1$ and a power series $g(X) \in 1 + X\mathbb{C}_p[[X]]$ which converges and is nonzero on $D[p^\lambda]$ such that

$$h_\alpha(X) = f_\alpha(X)g(X)$$

Multiplying both sides by $1 - cX$ and denoting $h(X) = (1-cX)h_\alpha(X)$ we have

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

as required.

To prove the uniqueness of $h(X)$, suppose that $h'(X) \in 1 + X\mathbb{C}_p[X]$ is another polynomial of degree N such that $h'(X) = f(X)g'(X)$ where $g'(X)$ converges and is non-zero on $D[p^\lambda]$. We have

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

It therefore suffices to prove that $h'(X)g(X) = h(X)g'(X)$ implies that $h'(X)$ and $h(X)$ have the same roots with the same multiplicities. We prove the claim by induction on N. If $N = 1$, then $h(X)$ and $h'(X)$ are linear and hence $h(x) = 0$ if and only if $h'(x) = 0$ for some $x \in D[p^\lambda]$. Suppose that $N > 1$. We may assume that $v_p(\alpha) = -\lambda$ for some root α of $h(X)$. α must also be a root of $h'(X)$ so we may divide both sides of $h'(X)g(X) = h(X)g'(X)$ by $1 - X/\alpha$. Appealing to Lemma 3.3.8, the two sides converge on $D[|\alpha|_p]$ and thus we may apply the induction hypothesis to reduce to the case $N-1$ and we are done. □

Corollary 3.3.10. *Let $f(X) \in 1 + X\mathbb{C}_p[[X]]$ be a power series. If the Newton polygon of $f(X)$ has a finite slope λ of length N then there exists N (not necessarily distinct) $x \in \mathbb{C}_p$ such that $f(x) = 0$ and $v_p(x) = -\lambda$.*

Corollary 3.3.11. *Let $f(X) \in \mathbb{C}_p[[X]]$ with $f(0) = a$ where a is non-zero. If $f(X)$ converges everywhere in $\mathbb{C}_p$ then we can write*

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

where the α_i form a countable set which we may refer to as the ***roots*** *of $f(X)$.*

Proof. Clearly the result holds if $f(X)$ is a polynomial. Hence we may assume that f is a power series that has infinitely many non-zero terms. Let $\overline{f(X)} = f(x)/a$. Since $\overline{f}(X)$ converges everywhere, Lemma 3.3.4

implies that the slopes of the Newton polygons are unbounded from above. Hence for any slope λ, we can apply the Weierstrass Preparation Theorem and write $\overline{f}(X) = h_\lambda(X)g_\lambda(X)$ with $g_\lambda(X)$ convergent and non-vanishing on $D[p^\lambda]$. We claim that the coefficients of $h_\lambda(X)$ converge to the coefficients of $\overline{f}(X)$ as $\lambda \to \infty$. Equivalently, it suffices to show that $g_\lambda(X) \to 1$ as $\lambda \to \infty$. First write

$$g_\lambda(X) = 1 + \sum_{i=1} b_i^\lambda X^i$$

Let λ_g be the first slope of the Newton polygon of $g(X)$. Suppose that the Newton polygon of $g_\lambda(X)$ contains a point $(i, v_p(b_i^\lambda))$. Since $g_\lambda(X)$ does not vanish on $D[p^\lambda]$, Lemma 3.3.7 implies that $\lambda_g > \lambda$. If there are only finitely many λ such that the Newton polygon of $g_\lambda(X)$ does not touch a point then we can pass to the limit $\lambda \to \infty$ and we see that $b_i^\lambda \to 0$ for all i.

If there are infinitely many λ for which the Newton polygon of $g_\lambda(X)$ does not contain a point then all the points (i, b_i^λ) lie above the first slope λ_g. Since $g_\lambda(X)$ converges on $D[p^\lambda]$, Lemma 3.3.4 implies that the slope of the Newton polygon is at least λ. We thus see that, in this case, the coefficients b_i^λ also go to 0. □

This is a rather remarkable result of independent interest. Entire power series over $\mathbb{C}$ do not enjoy such a property - such power series may have an exponential factor in their factorisation.

Chapter 4

Dwork's proof of the rationality of the zeta-function

We are finally ready to tackle Dwork's proof. Dwork first shows that the zeta-function defines a p-adic meromorphic function on $\mathbb{C}_p$. To this end, he proves a trace formula for certain endomorphisms of $\mathbb{C}_p[[X_1, \ldots, X_n]]$. One particular endomorphism to which this trace formula applies is obtained from a so-called 'lifting' of a character to a function on $\mathbb{C}_p$. Armed with these tools, Dwork then applies a criterion for rationality of a power series due to Borel in order to conclude that the zeta-function is rational.

Before we start this program, we state and prove a few useful and interesting properties of the zeta-function itself.

4.1 Properties of the zeta-function

Lemma 4.1.1. *Let H_f be an affine hypersurface defined over the finite field $\mathbb{F}_q$. Then the zeta-function $Z(H_f/\mathbb{F}_q; T)$ has integral coefficients; in particular, its constant term is 1.*

Proof. Let $X = (x_1, \ldots, x_n)$ be a $\mathbb{F}_{q^{s_0}}$-point of H_f (where s_0 is the least such s where all the x_i lie in $\mathbb{F}_{q^{s_0}}$). Let $x_{1j}, \ldots, x_{ij}$ be the conjugates of the x_i over $\mathbb{F}_q$ for $1 \leq j \leq s_0$. Let $P_j = (x_{1j}, \ldots, x_{nj})$ be the conjugates of X. Then, clearly, the X_j must be distinct. Indeed, if they weren't, then all the x_i would be fixed by an $\mathbb{F}_q$-automorphism σ of $\mathbb{F}_{q^{s_0}}$ they would thus be in a smaller finite field, contradiciting the minimality of s_0.

Now, each X_j is an $\mathbb{F}_{q^s}$-point whenever $s_0|s$ and thus X_j contributes s_0 to $N_{s_0}, N_{2s_0}, N_{3s_0}, \ldots$. We can thus write down their contributions to the zeta-function as follows:

$$\exp\left(\sum_{i=1}^{\infty} \frac{s_0 T^{is_0}}{is_0}\right) = \exp(-\log(1 - T^{s_0})) = \frac{1}{1 - T^{s_0}} = \sum_{i=0}^{\infty} T^{is_0}$$

The series on the right hand side clearly has positive integer coefficients. The zeta-function is now a product of similar series meaning the zeta-function itself must have positive integer coefficients. It also follows that the constant term of $Z(H_f/\mathbb{F}_q; T)$ is 1. □

Lemma 4.1.2. *Let H_f be an affine hypersurface defined over a finite field $\mathbb{F}_q$. Then the coefficient of T^i in the zeta-function $Z(H_f/\mathbb{F}_q; T)$ is bounded above by q^{ni} where n is the dimension of the affine space.*

In particular, $Z(H_f/\mathbb{F}_q;T)$ defines a holomorphic function on the disc of radius q^{-n} in $\mathbb{C}$.

Proof. The maximum possible value for N_s is the cardinality of n-dimensional affine space defined over $\mathbb{F}_{q^s}$, namely q^{ns}. Hence,

$$\exp\left(\sum_{s=1}^{\infty}\frac{N_sT^s}{s}\right)\leq\exp\left(\sum_{s=1}^{\infty}\frac{q^{ns}T^s}{s}\right)=\exp(-\log(1-q^nT))=\frac{1}{1-q^nT}=\sum_{i=0}^{\infty}q^{ni}T^i$$

□

We end this short section with a result that makes it clear why we chose the zeta-function in the form that it is.[1]

A useful construction is the notion of a global zeta-function. Consider a polynomial $f(x_1,\dots,x_n)\in\mathbb{Z}[X_1,\dots,X_n]$. Reducing the coefficients modulo p, we may obtain affine hypersurfaces $H_{f,p}$ for all primes p. We then define the global zeta-function of f to be

$$Z(f,x)=\prod_p Z(H_{f,p},p^{-x})$$

Now reduce to the case of 0-dimensional affine space and let f be the zero polynomial. Then

$$\begin{aligned}Z(0,x)=\prod_p Z(H_{0,p},p^{-x})=\prod_p\left[\exp\left(\sum_{s=1}^{\infty}\frac{(p^{-x})^s}{s}\right)\right]&=\prod_p\exp(-\log(1-p^{-x}))\\&=\prod_p\frac{1}{1-p^{-x}}\end{aligned}$$

and we recover the Euler product for the Riemann zeta-function. It is thus clear that our choice for the zeta-function of an affine hypersurface is natural.

4.2 Borel's Theorem

Theorem 4.2.1. *Let K be a field and $F(T)=\sum_{i=0}^{\infty}a_iT^i\in K[[T]]$ be a power series. Given $m,s\geq 0$ define the matrix $A_{s,m}=(a_{s+i+j})_{0\leq i,j\leq m}$. In other words,*

$$A_{s,m}=\begin{pmatrix}a_s & a_{s+1} & a_{s+2} & \cdots & a_{s+m}\\ a_{s+1} & a_{s+2} & a_{s+3} & \cdots & a_{s+m+1}\\ a_{s+2} & a_{s+3} & a_{s+4} & \cdots & a_{s+m+2}\\ \vdots & \vdots & \vdots & \cdots & \vdots\\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m}\end{pmatrix}$$

Let $N_{s,m}=\det A_{s,m}$. Then $F(T)$ is a quotient of two polynomials $P(T),Q(T)\in K[T]$ if and only if there exist integers $m,S\geq 0$ such that $N_{S,m}=0$ for all $s\geq S$.

Proof. First suppose that $F(T)$ is a quotient of two polynomials $P(T),Q(T)\in K[T]$. Denote $P(T)=$

[1] although this is certainly not the only reason

$\sum_{i=0}^{M} b_i T^i$ and $Q(T) = \sum_{i=0}^{N} c_i T^i$. By hypothesis, we have $F(T)Q(T) = P(T)$. Equating coefficients of T^i with $i > \max\{M, N\}$ in this equation yields

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

Hence if s is taken to be sufficiently large, we have the following equations for $i = s+N, s+N+1, \dots, s+2N$:

$$\begin{aligned} a_s c_N + a_{s+1} c_{M-1} + \cdots + a_{s+N} c_0 &= 0 \\ a_{s+1} c_N + a_{s+2} c_{N-1} + \cdots + a_{s+N+1} c_0 &= 0 \\ &\vdots \\ a_{s+N} c_N + a_{s+N+1} c_{N-1} + \cdots + a_{s+2N} c_0 &= 0 \end{aligned}$$

We can rewrite this as a matrix equation: $A_{s,N}(c_N, \dots, c_0)^T = \vec{0}$. This clearly implies that $N_{s,N} = 0$ for s sufficiently large.

For the opposite implication, assume that there exists S and m such that $N_{s,m} = 0$ for all $s \geq S$ and m is the minimal such integer that this holds. We claim that $N_{s,m-1} \neq 0$ for all $s \geq S$.

To arrive at a contradiction, suppose that $N_{s,m-1} = 0$ for all $s \geq S$. This implies that there exists a linear combination of the first m rows of $A_{s,m}$ that vanishes in all but possibly the last column. Label the rows $r_1, \dots, r_{m-1}$. Let $i_0 \in \mathbb{N}$ be such that r_{i_0} is the first row in the above linear combination with non-zero coefficient. Then we may write

$$r_{i_0} = \alpha_1 r_{i_0+1} + \alpha_2 r_{i_0+2} + \cdots + \alpha_{m-i_0-1} r_{m-1}$$

except for possibly in the last column. Replacing r_{i_0} by $r_{i_0} - (\alpha_1 r_{i_0+1} + \cdots + \alpha_{m-i_0-1} r_{m-1})$ we have two cases, $i_0 = 0$ and $i_0 > 0$.

In the first case $A_{s,m}$ takes the form

$$\left(\begin{array}{ccc|c} a_s & a_{s+1} & \cdots & \multicolumn{1}{c}{a_{s+m}} \\ \cline{1-3} a_{s+1} & a_{s+2} & \cdots & a_{s+m+1} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \alpha \\ \vdots & \vdots & \cdots & \vdots \\ a_{s+m} & a_{s+m+1} & \cdots & a_{s+2m} \end{array}\right)$$

for some $\alpha \in K$. The inner block has determinant $N_{s+1,m-1} = 0$.

In the latter case, $A_{s,m}$ takes the form

$$\left(\begin{array}{c|ccc|c} 0 & 0 & \cdots & & \alpha \\ \hline a_{s+1} & a_{s+2} & \cdots & & a_{s+m+1} \\ \vdots & \vdots & \cdots & & \vdots \\ \hline a_{s+m} & a_{s+m+1} & \cdots & & a_{s+2m} \end{array}\right)$$

It is clear that both inner blocks have determinant $N_{s+1,m-1}$. By hypothesis, $N_{s,m} = 0$ so either the bottom left block has determinant 0 or either $\alpha = 0$ in which case we also have $N_{s+1,m-1} = 0$. By induction, we see that $N_{t,m-1} = 0$ for all $t \geq s$. But this contradicts the minimality of m. Hence we must have that $N_{s,m-1} \neq 0$ for all $s \geq S$.

This implies that there exists a vanishing linear combination of the rows of $A_{s,m}$ where the coefficient of the last row is non-zero. Hence, the last row of $A_{s,m}$ is a linear combination of all the previous m rows. Therefore if $\gamma_0, \dots, \gamma_m \in K$ satisfy

$$\begin{pmatrix} a_s & a_{s+1} & \cdots & a_{s+m} \\ \vdots & \vdots & \cdots & \vdots \\ a_{s+m+1} & a_{s+m} & \cdots & a_{s+2m-1} \end{pmatrix} \begin{pmatrix} \gamma_m \\ \vdots \\ \gamma_0 \end{pmatrix} = \vec{0}$$

then we also have $a_s\gamma_m + \dots a_{s+m}\gamma_0 = 0$. By induction, this applies to all $s \geq S$. But this implies that

$$\left(\sum_{i=0}^{m} \gamma_i X^i\right)\left(\sum_{i=1}^{\infty} a_i X^i\right)$$

is a polynomial and we are done. □

In order to apply Borel's Theorem to the zeta-function, we need to show that the zeta-function defines a meromorphic function on $\mathbb{C}_p$. The next two sections will be concerned with the proof of this fact.

4.3 Endomorphisms of $\mathbb{C}_p[[X_1, \dots, X_n]]$

The goal of this section is to prove the so-called Dwork's Trace Formula which is the first of two results that we need in order to prove the p-adic meromorphicity of the zeta-function.

Throughout this section, we shall set $R = \mathbb{C}_p[[X_1, \dots, X_n]]$. Let

$$U = \{ (x_1, \dots, x_n) \mid x_i \in \mathbb{Z}, x_i \geq 0 \}$$

If $X_1^{u_1} \dots X_n^{u_n} \in R$ is a monomial then, for brevity, we shall write it in the compact form X^u where $u = (u_1, \dots, u_n)$. The standard arithmetic operations on $u \in U$, such as multiplication or exponentiation by an integer, shall be given by applying the operation component-wise. If u is an index (for a summation for example) and it is acted upon by an operation that sends it outside U then we set the indexed object to zero.

Let $G \in R$ be a power series. By μ_G we shall mean the endomorphism of R given by multiplication of G:

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

Let q be a positive integer. By ϕ_q we shall mean the endomorphism of R given by

$$\begin{aligned} \phi_q : R &\to R \\ \sum_{u \in U} a_u X^u &\mapsto \sum_{u \in U} a_{qu} X^u \end{aligned}$$

In other words, if $u \in U$ is not divisible by q then the corresponding term of the power series $a_u X^u$ vanishes under the action of ϕ_q. If u is divisible by q then ϕ_q replaces X^u by $X^{u/q}$.

Finally, we denote the composition of these two endomorphisms by $\Psi_{q,G} = \phi_q \circ \mu_G$. Suppose that $G = \sum_{w \in U} \gamma_w X^w$. Then $\Psi_{q,G}$ acts on a monomial X^u as follows:

$$\Psi_{q,G}(X^u) = \phi_q \left(\sum_{w \in U} \gamma_w X^{w+u} \right) = \sum_{w \in U} \gamma_{qw-u} X^w$$

Lemma 4.3.1. *Let $G = \sum_{w \in U} \gamma_w X^w \in R$. If $G_q(X) = G(X^q)$ then*

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

Proof. We have that

$$\mu_G \circ \phi_q(X^u) = \begin{cases} 0 & \text{if } q \not| u \\ GX^{u/q} & \text{if } q|u \end{cases}$$

In the case where $q|u$, this is the same as

$$\sum_{w \in U} \gamma_w X^{w+u/q} = \sum_{w \in U} \gamma_{w-u/q} X^w \tag{4.1}$$

On the other hand, we have

$$\phi_q \circ \mu_{G_q}(X^u) = \phi_q \left(\sum_{w \in U} \gamma_{w \in U} X^{qw+u} \right) = \sum_{w \in U} \gamma_{qw} X^{qw+u} = \sum_{w \in U} \gamma_{w-u/q} X^w$$

If $q \not| u$ then this is simply 0. If not then we retrieve Equation 4.1. Finally,

$$\Psi_{q,G_q}(X^u) = \phi_q \circ \mu_{G_q}(X^u) = \phi_q \left(\sum_{w \in U} \gamma_w X^{qw+u} \right) = \sum_{w \in U} \gamma_{qw} X^{qw+u} = \sum_{w \in U} \gamma_{w-u/q} X^w$$

as desired. □

Definition 4.3.2. We define the set of **overconvergent power series** to be

$$R_0 = \left\{ G = \sum_{w \in U} \gamma_w X^w \in R \;\middle|\; \exists\, \varepsilon > 0 \text{ such that } v_p(\gamma_w) \geq \varepsilon |w| \ \forall w \in U \right\}$$

where $|w|$ is understood to be the sum of the components of w.

Lemma 4.3.3. *R_0 is closed under multiplication and the map $G \mapsto G_q$.*

Proof. Let $f(X) = \sum_{v \in U} \beta_v X^v$ and $g(X) = \sum_{w \in U} \gamma_w X^w$ be power series in R_0. Then

$$f(X)g(X) = \sum_{z \in U} a_z X^z$$

where $a_z = \sum_{m+n=z} \beta_m \gamma_n$. Now

$$v_p(a_z) \geq \min_{m+n=z} v_p(\beta_m \gamma_n) = \min_{m+n=z} [v_p(\beta_m) + v_p(\gamma_n)]$$

By hypothesis, there exist $\varepsilon, \delta > 0$ such that for all $m, n \in U$ we have $v_p(\beta_m) \geq \varepsilon|m|$ and $v_p(\gamma_n) \geq \delta|n|$. Furthermore if $m + n = z$ then $|m| + |n| = |z|$. Hence

$$v_p(a_z) \geq \min_{m+n=z} [\varepsilon|m| + \delta|n|] \geq \min\{\delta, \varepsilon\}|z|$$

It therefore follows that $f(X)g(X) \in R_0$.

For the second part of the lemma, let $G(X) = \sum_{w \in U} \gamma_u X^u$. We have

$$G_q(X) = \sum_{z \in U} \gamma_z X^{qz}$$

If $\gamma'_z X^z$ is a term in G_q then γ'_z is 0 unless $q|z$. In that case, we have $z = qw$ where w is the power of X in a monomial of the expansion of $g(X)$. Then there exists a $\varepsilon > 0$ such that

$$v_p(\gamma'_z) = v_p(\gamma_w) \geq \varepsilon|w| = \frac{\varepsilon}{q}|qw| = \frac{\varepsilon}{q}|z|$$

and thus $G_q \in R_0$. □

Lemma 4.3.4. *If $\mu_n(\mathbb{C}_p)$ is the set of all n^{th} roots of unity in $\mathbb{C}_p$ then*

$$\sum_{\zeta \in \mu_n(\mathbb{C}_p)} \zeta^a = \begin{cases} n & \text{if } n|a \\ 0 & \text{if } n \not| a \end{cases}$$

Proof. Suppose first that n divides a. Then any n^{th} root of unity to the power of a is 1. Since there are exactly n n^{th} roots of unity, the formula follows.

Now assume that $n \not| a$ and that n and a are coprime. Then the map $\zeta \mapsto \zeta^a$ is an automorphism of $\mu_n(\mathbb{C}_p)$ whence

$$\sum_{\zeta \in \mu_n(\mathbb{C}_p)} \zeta^a = \sum_{\zeta \in \mu_n(\mathbb{C}_p)} \zeta$$

Recall that the n^{th} roots of unity are the roots of the polynomial $X^n - 1$. Clearly, this factors as $X^n - 1 = \prod_{\zeta \in \mu_n(\mathbb{C}_p)} X - \zeta$. Now, the coefficient of the X^{n-1} term on the left hand side is 0 and on the right hand side it is simply the negative of the sum of the elements of $\mu_n(\mathbb{C}_p)$. Hence, in this case, the original sum is 0.

Finally, suppose that $1 < d = \gcd(n, a) < n$. Then we obtain d sums of n/d roots of unity which also sum to 0 and we are done. □

Recall that given an n-dimensional vector space V and a linear map $A : V \to V$, we define the **trace** of A to be

$$\mathrm{Tr}(A) = \sum_{i=1}^{n} A_{ii}$$

Now if V is an infinite dimensional vector space over a field equipped with an absolute value $|\cdot|$ and A is an endomorphism of V then we can also define the trace of A provided that the sum

$$\mathrm{Tr}(A) = \sum_{i=1}^{\infty} A_{ii}$$

converges with respect to $|\cdot|$.[2]

Proposition 4.3.5 (Dwork's Trace Formula). *Let $G \in R_0$ be an overconvergent power series, q a positive integer and $\Psi = \Psi_{q,G}$. Let μ_{q^s-1} denote the set of all $\mathbb{C}_p$ n-tuples consisting of $(q^s-1)^{th}$ roots of unity. Then $\mathrm{Tr}(\Psi^s)$ converges for all $s \geq 1$ and*

$$(q^s-1)^n \mathrm{Tr}(\Psi^s) = \sum_{x \in \mu_{q^s-1}} G(x)G(x^q)G(x^{q^2})\ldots \tag{4.2}$$

Proof. We prove the lemma by induction on s. Suppose that $s = 1$ and $G(X) = \sum_{w \in U} \gamma_w X^w$. By definition we have $\Psi(X^u) = \sum_{w \in U} \gamma_{qw-u}$. The elements that contribute to the trace are those when $v = u$ and so

$$\mathrm{Tr}(\Psi) = \sum_{u \in U} \gamma_{(q-1)u}$$

Since $G \in R_0$, the above sum is convergent and thus the trace is well-defined.

We now shift our attention to the right hand side of Equation 4.2. If $x, w \in U$, let x_i and w_i denote their i^{th} coordinates respectively. Then by Lemma 4.3.4 we have

$$\sum_{x_i^{q-1}=1} x_i^{w_i} = \begin{cases} q-1 & \text{if } (q-1)|w_i \\ 0 & \text{if } (q-1)\not| w_i \end{cases}$$

whence it follows that

$$\sum_{x \in \mu_{q^s-1}} x^w = \prod_{i=1}^{n} \left(\sum_{x_i^{q-1}=1} x_i^{w_i} \right) = \begin{cases} (q-1)^n & \text{if } (q-1)|w \\ 0 & \text{if } (q-1)\not| w \end{cases}$$

We now see that

$$\sum_{x \in \mu_{q^s-1}} G(x) = \sum_{w \in U} \gamma_w \sum_{x \in \mu_{q^s-1}} x^w = (q-1)^n \sum_{u \in U} g_{(q-1)u} = (q-1)^n \mathrm{Tr}(\Psi)$$

which proves the lemma in the case $s = 1$.

[2] one must be careful to make sure that such a construction is independent of the choice of basis for V. Indeed, the trace is independent of such a choice for the finite case by elementary linear algebra. For the infinite dimensional case, we may simply pass to the limit on the finite dimensional case.

Now assume that $s > 1$. By the definition of Ψ and Lemma 4.3.1 we have

$$\begin{aligned} \Psi^s &= \phi_q \circ \mu_G \circ \phi_q \circ \mu_G \circ \Psi^{s-2} \\ &= \phi_q \circ \phi_q \circ \mu_{G_q} \circ \mu_G \circ \Psi^{s-2} \\ &= \phi_{q^2} \circ \mu_{GG_q} \circ \Psi^{s-2} \\ &\vdots \\ &= \phi_{q^s} \circ \mu_{GG_q \ldots G_{q^{s-1}}} = \Psi_{q^s, GG_q \ldots G_{q^{s-1}}} \end{aligned}$$

By Lemma 4.3.3, the power series $GG_q \ldots G_{q^{s-1}}$ is in R_0. Hence the case where $s > 1$ reduces to the basis case and we are done. □

Dwork's Trace Formula is essentially the result that will allow us to 'lift' the problem of the zeta-function over finite fields to a problem of p-adic analysis. This, along with the character lifting introduced in the next section, are the most fundamental parts of Dwork's proof.

Proposition 4.3.6. *Let $G \in R_0$ be an overconvergent power series, q a positive integer and $\Psi = \Psi_{q,G}$. Then the power series* $\det(1 - \Psi T) \in \mathbb{C}_p[[T]]$ *is a well-defined entire power series and*

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

Proof. Let $G(X) = \sum_{w \in U} \gamma_w X^w \in R_0$. We first recall the definition of the determinant in terms of permutations:

$$\det(1 - \Psi T) = \sum_{b=0}^{\infty} b_n T^n$$

where

$$b_n = (-1)^n \sum_{\substack{u_1 \ldots u_n \in U \\ \sigma \in S_n}} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} \Psi_{u_1, u_{\sigma(i)}}$$

Here $\Psi_{u,w}$ means the $(u, w)^{th}$ entry of the (infinite) matrix for the endomorphism Ψ. We can read such entries off from the definition $\Psi(X^u) = \sum_{w \in U} \gamma_{qw-u} X^w$.

Since $G \in R_0$, we can always find an $\varepsilon > 0$ such that $v_p(\gamma_w) \geq \varepsilon |w|$ for all $w \in U$. Thus

$$\begin{aligned} v_p(\gamma_{qu_{\sigma(1)}-u_1} \cdots \gamma_{qu_{\sigma(j)}-u_n}) &\geq \varepsilon(|qu_{\sigma(1)} - u_1| + \cdots + |qu_{\sigma(n)} - u_n|) \\ &\geq \varepsilon \left(\sum_{i=1}^{n} q|u_{\sigma(i)}| - \sum_{i=1}^{n} |u_i| \right) \\ &= \varepsilon(q-1) \sum_{i=1}^{n} |u_i| \end{aligned}$$

From this we clearly see that $v_p(b_n) \to \infty$ as $n \to \infty$ whence the determinant is well-defined. Furthermore, $(1/n)v_p(b_n) \to \infty$ as $n \to \infty$. This implies that, as $n \to \infty$,

$$\lim_{n\to\infty} |b_n|_p^{1/n} \to 0$$

Hence the determinant has an infinite radius of convergence.

To prove the equation given in the proposition, we first consider the case where A is an endomorphism of an n-dimensional vector space over $\mathbb{C}_p$. From elementary linear algebra, we know that the determinant and the trace of such a mapping is invariant under a change of basis. Since $\mathbb{C}_p$ is algebraically closed, we can always find a change of basis so that A, with respect to the new basis, is upper triangular. Hence, without loss of generality, we may assume that A is upper triangular. Then

$$\det(1 - AT) = \prod_{i=1}^{n}(1 - A_{i,i}T)$$

On the other hand, we have

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

Hence

$$\begin{aligned}\exp_p\left(-\sum_{s=1}^{\infty}\sum_{i=1}^{n}\frac{(A_{i,i})^sT^s}{s}\right) &= \prod_{i=1}^{n}\exp_p\left(-\sum_{s=1}^{\infty}\frac{(A_{i,i}T)}{s}\right)\\ &= \prod_{i=1}^{n}\exp_p\left(\log_p(1 - A_{i,i}T\right)\\ &= \prod_{i=1}^{n}(1 - A_{i,i}T) = \det(1 - AT)\end{aligned}$$

Now if Ψ is an endomorphism acting on an infinite dimensional vector space over $\mathbb{C}_p$, we can easily pass to the limit $n \to \infty$ in the above to arrive at the same identity for Ψ. □

4.4 Lifting of $\mathbb{C}_p$-valued characters

Having proved Dwork's Trace Formula for the endomorphism Ψ and discovered some of its properties, we now look towards finding an overconvergent power series with which we can use these results. This power series will be the second key result we need in order to prove that the zeta-function is p-adic meromorphic.

Definition 4.4.1. Let G be a finite group and K a field. A **K-valued character** of G is a homomorphism $\varphi : G \mapsto K^\times$.

It is immediate from Lagrange's Theorem and the definition of a character that the image of φ is necessarily a subset of the roots of unity in $K^\times$.

Let L/K be a field extension and $\alpha \in L$ with $[K(\alpha) : K] = m$ and $[L : K(\alpha)] = n$. Recall that we define the **trace** of α from L to K to be

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

where the $\alpha = \alpha_1, \dots, \alpha_m$ are the conjugates of α over K. Furthermore, if L/K is Galois and $G = \mathrm{Gal}(L/K)$ then

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

Proposition 4.4.2. *Let $\omega \in \mathbb{C}_p$ be a p^{th} root of unity. Then*

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

is a well-defined $\mathbb{C}_p$-valued character of the additive group of $\mathbb{F}_q$. Here, exponentiation by $t = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)$ is to be understood as exponentiation by the least positive residue of t.

Proof. It is an elementary result of the theory of finite fields that $\mathbb{F}_q/\mathbb{F}_p$ is Galois. Let $G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Then G is generated by the $\mathbb{F}_p$-automorphism $x \mapsto x^p$ - the so-called Frobenius automorphism. We have

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

Since each $\sigma \in G$ is a power of the Frobenius automorphism, we see that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)$ is fixed by all elements of G. Hence $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) \in \mathbb{F}_p$.

It is easy to see that the trace is additive. Indeed,

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

where we have used the fact that the Frobenius automorphism and all its powers are additive in characteristic p. φ is therefore a character of the additive group of $\mathbb{F}_q$. □

Let $a \in \mathbb{F}_q$ for some prime power $q = p^s$. Recall that there exists a unique Teichmüller representative of a given by $\tau_s(a)$ (the Teichmüller lift) in an unramified extension K of $\mathbb{Q}_p$ generated by a primitive $(p^s-1)^{th}$ root of unity. $\tau_s(a)$ satisfies $\tau_s(a)^{p^s} = \tau_s(a)$ and $\tau_s(a) \equiv a \pmod{p\mathcal{O}_K}$. $K/\mathbb{Q}_p$ is Galois since K is the splitting field for the q^{th} cyclotomic polynomial over $\mathbb{Q}_p$. Letting $G = \mathrm{Gal}(K/\mathbb{Q}_p)$ we have

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

It then follows that

$$\mathrm{Tr}_{K/\mathbb{Q}_p}(\tau_s(a)) \equiv \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(a) \pmod{p\mathcal{O}_K}$$

Hence given any p^{th} root of unity ω, we have

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

We seek a complex p-adic power series $\Theta(T) \in \mathbb{C}_p[[T]]$ satisfying $\Theta(\tau_s(a)) = \omega^a$. If we can find such a power series, then we can recover the trace character as follows:

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

We shall refer to Θ as a **lifting** of the character φ to a function on $\mathbb{C}_p$. In order to construct such a lifting, we shall use the power series we constructed after introducing Dwork's Lemma.

Lemma 4.4.3. *Let $\omega \in \mathbb{C}_p$ be a p^{th} root of unity. Then $|\omega - 1|_p = p^{-1/(p-1)}$.*

Proof. Observe that ω satisfies the p^{th} cyclotomic polynomial over $\mathbb{Q}_p$:

$$\Phi(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$$

We claim that $\Phi(X+1)$ is the minimal polynomial of $\omega - 1$ over $\mathbb{Q}_p$. Indeed, $\Phi(\omega - 1 + 1) = \Phi(\omega) = 0$ so it suffices to show that $\Phi(X+1)$ is irreducible over $\mathbb{Q}_p$. We have

$$\Phi(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(X+1)^p - 1}{X} \equiv X^{p-1} \pmod{p}$$

Hence all coefficients except the leading coefficient of $\Phi(X+1)$ is divisible by p. Furthermore, $\Phi(0+1) = \Phi(1) = p$ which is not divisible by p^2. Hence by the Eisenstein irreducibility criterion, $\Phi(X+1)$ is irreducible. Now the p-adic absolute value for ω is given in terms of the algebraic norm for ω. Calculating this, we have $\mathrm{N}_{\mathbb{Q}_p(\omega-1)/\mathbb{Q}_p}(\omega - 1) = \Phi(1) = p$. We thus see that $|\omega - 1|_p = p^{-1/(p-1)}$. □

Theorem 4.4.4. *Let ω be a p^{th} root of unity and set $\lambda = \omega - 1$. Suppose that φ is the character*

$$\varphi : \mathbb{F}_{p^s} \to (\mathbb{C}_p)^\times$$
$$a \mapsto \omega^{\mathrm{Tr}_{\mathbb{F}_{p^s}/\mathbb{F}_p}(a)}$$

Then

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

is a lifting of φ to a function on $\mathbb{C}_p$.

Proof. Recall that the function $F(X, Y)$ in the theorem's hypothesis was shown to have coefficients in $\mathbb{Z}_p$ by Dwork's Lemma. If we consider Y to be fixed we have

$$F(X, Y) = \sum_{n=0}^{\infty} X^n \left(\sum_{m=n}^{\infty} a_{m,n} Y^m \right)$$

for some constants $a_{m,n}$. Substituting T and λ we see that $F(T, \lambda) = \sum_{n=0}^{\infty} a_n T^n$ with $a_n = \sum_{m=n}^{\infty} a_{m,n} \lambda^m$.

We have that

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

where we have used Lemma 4.4.3 to calculate the p-adic valuation of $\omega - 1$. Hence if we take $\Theta(T) = F(T,\lambda)$, we see that $\Theta(T) \in \mathbb{C}_p[[T]]$ converges (at least) on the disc $D(p^{-1/(p-1)})$. We now claim that if $\tau = \tau_s(a) \in \mathbb{C}_p$ is the Teichmüller representative of $a \in \mathbb{F}_{p^s}$ in $\mathbb{C}_p$ then

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

We have

$$\prod_{i=1}^{p^{s-1}} \Theta(\tau^i) = \prod_{i=1}^{p^{s-1}} (1+\lambda)^{\tau^i}(1+\lambda^p)^{(\tau^{pi}-\tau^i)/p}\dots$$

Simplifying on the right hand side yields

$$\prod_{i=1}^{p^{s-1}} \Theta(\tau^i) = (1+\lambda)^{\tau+\tau^p+\dots\tau^{p^{s-1}}}(1+\lambda^p)^{(\tau^{p^s}-\tau)/p}(1+\lambda^{p^2})^{(\tau^{p^s+1}-\tau^p)/p^2}\dots$$

But $\tau^{p^s} = \tau$ and we are left with

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

as desired. □

Now that we have constructed the lifting, we show that it gives rise to an overconvergent power series and thus we can apply the facts from the previous section.

Proposition 4.4.5. *Let $w \in U, a \in D(1)$. Then $\Theta(aX^w)$ is an overconvergent power series.*

Proof. The proof of Theorem 4.4.4 implies that $\Theta(T) = \sum_{i=0}^{\infty} b_i T^i$ with $v_p(b_i) \geq i/(p-1)$. Now,

$$\Theta(aX_1^{w_1}\dots X_n^{w_n}) = \sum_{i=0}^{\infty} b_i a^i X_1^{iw_1}\dots X_n^{iw_n}$$

Then $v_p(b_i a^i) \geq v_p(b_i) \geq i/(p-1) = i|w|/(|w|(p-1))$. Taking $\varepsilon = 1/(|w|(p-1))$ leaves us with $v_p(b_i a^i) \geq \varepsilon|w|$ whence $\Theta(aX^w) \in R_0$. □

4.5 Meromorphicity of the zeta-function

We now put our two results together, namely Dwork's Trace Formula applied to the series Θ, to conclude that the zeta-function is p-adic meromorphic. We begin with a couple of lemmata:

Lemma 4.5.1. *Let*

$$\varphi : \mathbb{F}_q \to (\mathbb{C}_p)^\times$$

be a non-trivial $\mathbb{C}_p$-valued character of the additive group of $\mathbb{F}_q$. Then

$$\sum_{x \in \mathbb{F}_q} \varphi(x) = 0$$

Proof. Let $x_0 \in \mathbb{F}_q$ be such that $\varphi(x_0) \neq 1$. Such an x_0 exists since φ is non-trivial. Now consider the change of variables $x \mapsto x + x_0$. We have

$$\sum_{x \in \mathbb{F}_q} \varphi(x) = \sum_{x \in \mathbb{F}_q} \varphi(x + x_0) = \varphi(x_0) \sum_{x \in \mathbb{F}_q} \varphi(x)$$

but $\varphi(x_0) \neq 1$ so we must have that the summation equals 0. □

Lemma 4.5.2. *Let ω be a p^{th} root of unity in $\mathbb{C}_p$. Consider the $\mathbb{C}_p$-valued character*

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

Then

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

Proof. If $u = 0$ then the lemma is trivial. If $u \neq 0$ then we may consider the proof of the previous lemma with the change of variables $xu \mapsto xu + x_0$. □

Proposition 4.5.3. *Let H_f be an affine hypersurface defined over a finite field $\mathbb{F}_q$. Then the zeta-function $Z(H_f/\mathbb{F}_q; T)$ is p-adic meromorphic.*

Proof. We prove the proposition by induction on n, the dimension of the affine space that H_f is defined on. If $n = 0$ then any hypersurface over $\mathbb{F}_q$ consists of just a single point and its zeta function is given by

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

which is indeed a p-adic meromorphic function. Now suppose that the proposition holds true for all natural numbers less than or equal to $n - 1$. Define

$$\begin{aligned} N_s' &= |\{ (x_1, \ldots, x_n) \in \mathbb{F}_{q^s} \mid f(x_1, \ldots, x_n) = 0, \forall\, 1 \leq i \leq n,\ x_i \neq 0 \}| \\ &= |\{ (x_1, \ldots, x_n) \in \mathbb{F}_{q^s} \mid f(x_1, \ldots, x_n) = 0, \forall\, 1 \leq i \leq n,\ x_i^{q^s - 1} = 1 \}| \end{aligned}$$

We claim that the rationality of

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

implies that of $Z(H_f/\mathbb{F}_q;T)$. Indeed, we have

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

let $X_i = \{\,(x_1,\dots,x_n) \in H_f \mid x_i = 0\,\}$. Then X_i is an affine hypersurface in $\mathbb{A}_{\mathbb{F}_q}^{n-1}$. By the inclusion-exclusion principle, we then have that

$$\begin{aligned} N_s - N_s' &= \left|\bigcup_{i=1}^{n} X_i(\mathbb{F}_{q^s})\right| \\ &= \sum_{i=1}^{n} |X_i(\mathbb{F}_{q^s})| - \sum_{i<j} |X_i(\mathbb{F}_{q^s}) \cap X_j(\mathbb{F}_{q^s})| + \sum_{i<j<k} |X_i(\mathbb{F}_{q^s}) \cap X_j(\mathbb{F}_{q^s}) \cap X_k(\mathbb{F}_{q^s})| + \dots \end{aligned}$$

Note that $X_i \cap X_j$ is an affine hypersurface in $\mathbb{A}_{\mathbb{F}_q}^{n-2}$ and the same pattern is true for the more numerous intersections. Thus by the induction hypothesis,

$$\exp\left(\sum_{s=1}^{\infty} \frac{(N_s - N_s')T^s}{s}\right) = \frac{\prod_{i=1}^{n} Z(X_i/\mathbb{F}_q;T) \cdot \prod_{i<j<k} Z((X_i \cap X_j \cap X_k)/\mathbb{F}_q;T) \dots}{\prod_{i<j} Z((X_i \cap X_j)/\mathbb{F}_q;T) \dots}$$

is p-adic meromorphic. Hence it suffices to show that $Z'(H_f/\mathbb{F}_q;T)$ is p-adic meromorphic.

To this end, fix an integer $s \geq 1$ and let $q = p^r$ for some $r \geq 1$. Let $a \in \mathbb{F}_{q^s}$ and let $\tau = \tau_s(a)$ represent its Teichmüller representative in $\mathbb{C}_p$. Recall that, given a p^{th} root of unity ω, we have the following character lifting

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

By Lemma 4.5.2 we have the equality

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

Now, we may consider $u = f(X_1,\dots,X_n)$ where f is the defining polynomial of H_f. Then

$$\sum_{x_1,\dots,x_n \in (\mathbb{F}_{q^s})^\times} \sum_{x_0 \in \mathbb{F}_{q^s}} \omega^{\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(x_0 f(x_1,\dots,x_n))} = q^s N_s'$$

Hence removing the $x_0 = 0$ term leaves us with

$$\sum_{x_0,x_1,\dots,x_n \in (\mathbb{F}_{q^s})^\times} \omega^{\mathrm{Tr}_{\mathbb{F}_{q^s}/\mathbb{F}_p}(x_0 f(x_1,\dots,x_n))} = q^s N_s' - (q^s - 1)^n$$

We shall now pass to the lifting of the character to show that the zeta-function is p-adic meromorphic. To this end, let $F(X_0, X_1, \dots, X_n) \in \mathbb{C}_p[X_0, X_1, \dots, X_n]$ represent the polynomial $X_0 f(X_1,\dots,X_n)$ with its coefficients replaced by their Teichmüller representatives in $\mathbb{C}_p$. Write $F(X_0, X_1, \dots, X_n) = \sum_{i=1}^{N} a_i X^{w_i}$.

Then

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

Letting

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

we have

$$q^s N_s' = (q^s - 1)^n + \sum_{\substack{\vec{x} \in U \\ x^{q^s - 1} = 1}} G(x) G(x^q) \ldots G(x^{q^s - 1})$$

Since the a_i are the Teichmüller representatives of elements of $\mathbb{F}_{q^s}$ they are in $D(1)$. Lemma 4.4.5 then implies that $\Theta(a_i^{p^k} X^{p^k w})$ are in R_0 whence $G \in R_0$. In particular, Dwork's Trace Formula makes sense for the particular power series G and we thus have

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

Dividing through by q^s and using the binomial formula gives us

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

Using Proposition 4.3.6 we denote

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

Finally, we have that

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

Each term in this product expansion is p-adic meromorphic from which it follows that the zeta-function itself is p-adic meromorphic. □

4.6 Finishing the proof

We will now apply Borel's Theorem to the zeta-function. The following proposition is a slightly weaker statement of a result proved in Dwork's original paper, [Dwo60].

Theorem 4.6.1. *Let $\zeta(T) \in 1 + T\mathbb{Z}[[T]]$ be a power series. Suppose that ζ is holomorphic on a disk in $\mathbb{C}$ and meromorphic on $\mathbb{C}_p$. Then $\zeta(T)$ is a rational function in $\mathbb{Q}(T)$.*

Proof. Let $\zeta(T) = \alpha(T)/\beta(T)$ where $\alpha(T)$ and $\beta(T)$ are p-adic entire functions. Since $\beta(T)$ is p-adic entire, for all $r > 0$, it converges on the disk $D(r)$ in $\mathbb{C}_p$. By the p-adic Weierstrass Preparation Theorem, we may write $\beta(T) = P(T)/\beta_0(T)$ for some function $\beta_0(T) \in 1 + T\mathbb{C}_p[[T]]$ which converges on $D(r)$ and a polynomial $P(T) \in 1 + T\mathbb{C}_p[T]$. Let $F(T) = \alpha(T)\beta_0(T)$. Then $F(T) = P(T)\zeta(T)$ and is p-adically convergent on $D(r)$.

Now, write $\zeta(T) = \sum_{i=0}^{\infty} a_i T^i \in 1 + T\mathbb{Z}[[T]], F(T) = \sum_{i=0}^{\infty} b_i T^i \in 1 + T\mathbb{C}_p[[T]]$ and $P(T) = \sum_{i=0}^{e} c_i T^i \in 1 + \mathbb{C}_p[T]$. Without loss of generality, we may assume that $\zeta(T)$ converges on a disk of radius $R < 1$ in $\mathbb{C}$. Equating coefficients in $F(T) = P(T)\zeta(T)$ we have

$$b_{i+e} = a_{i+e} + c_1 a_{i+e-1} + \cdots + c_e a_i \tag{4.3}$$

Now let $A_{s,m}$ be the matrix given by $(a_{s+i+j})_{0\le i,j\le m}$ and denote $N_{s,m} = \det A_{s,m}$. We first observe that $N_{s,m}$ is necessarily an integer. Letting $m > 2e$, we see that Equation 4.3 allows us to replace all but the first e columns of $A_{s,m}$ with the corresponding columns in $(b_{s+i+j})_{0\le i,j\le m}$ without changing $N_{s,m}$. Since $|a_i|_p \le 1$, we have the following estimate for sufficiently large s

$$|N_{s,m}|_p \le \left(\max_{i\ge s+e} |b_i|_p\right)^{m+1-e} < r^{-s(m+1-e)}$$

Now write $r = 1/R^2$. We then have that

$$|N_{s,m}|_p < R^{s(m+2)}$$

Furthermore, since $\zeta(T)$ converges on the disk of radius R in the complex plane, we have that $|a_i|_\infty \le R^{-i}$. Then

$$\begin{aligned}|N_{s,m}|_\infty &= \left|\sum_{\sigma\in S_{m+1}} \operatorname{sgn}(\sigma)\prod_{i=1}^{m+1} a_{\sigma(i),i}\right|_\infty \\ &\le (m+1)!\prod_{i=1}^{m+1}\max_{0\le i,j\le m}|a_{s+i+j}|_\infty \\ &\le (m+1)!R^{-(s+2m)(m+1)}\end{aligned}$$

Then

$$|N_{s,m}|_\infty |N_{s,m}|_p \le (m+1)!R^{-(s+2m)(m+1)}R^{s(m+2)} = (m+1)!R^{s-2m(m+1)}$$

Since $R < 1$, passing to the limit $s \to \infty$ yields

$$|N_{s,m}|_\infty |N_{s,m}|_p < 1$$

for s sufficiently large. But the only integer satisfying the above is 0 so we must have that $N_{s,m} = 0$ for some $m > 2e$ and for s sufficiently large. In light of Borel's Theorem, $\zeta(T)$ is thus a rational function. □

This theorem immediately implies that the zeta-function of an affine hypersurface over $\mathbb{F}_q$ is rational. Indeed, the zeta-function is holomorphic on the disc of radius $1/q^n$ in $\mathbb{C}$, is p-adic meromorphic and has integer coefficients. Dwork's Theorem is thus proved.

Dwork's slightly more general version of Theorem 4.6.1 only requires that the power series be meromorphic on a disc of radius R in $\mathbb{C}_p$ and holomorphic on a disc of radius r in $\mathbb{C}$ where $Rr > 1$. This is proven in the same way as the proof presented above with minor changes required.

In fact, Dwork further generalised this result. In particular, if $K/\mathbb{Q}$ is a rational number field, it is possible to define a sort of p-adic absolute value on K attached to a prime ideal $\mathfrak{p} \lhd \mathcal{O}_K$, say $|\cdot|_\mathfrak{p}$. Completing K with respect to $|\cdot|_\mathfrak{p}$ yields a finite extension of $\mathbb{Q}_p$. This is a generalisation of p-adic completions to arbitrary number fields. Dwork then proves the following theorem:

Theorem 4.6.2. *Let K be a number field and $F(T) = \sum_{i=0}^\infty a_i T^i \in K[[T]]$ a power series. Then $F \in K(T)$ if and only if there exists a finite set S of primes*[3] *of K such that*

1. *For all $\mathfrak{p} \notin S$, $|a_i|_\mathfrak{p} \leq 1$ for all i*
2. *For all $\mathfrak{p} \in S$, $F(T)$ is meromorphic on the disk of radius $R_\mathfrak{p}$ where $\{ R_\mathfrak{p} \}$ is a set of positive real numbers satisfying*

$$\prod_{\mathfrak{p} \in S} R_\mathfrak{p} > 1$$

The interested reader is invited to read Dwork's paper, [Dwo60] for a proof of this theorem. We end this chapter by extending the reach of Dwork's proof of the rationality of the zeta-function to so-called affine varieties.

Definition 4.6.3. Let K be a field and $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ a polynomial. We define the **affine variety** defined by $f_1, \ldots, f_n$ in $\mathbb{A}^n_K$ to be

$$H_{f_1,\ldots,f_n} = \{ (x_1, \ldots, x_n) \in \mathbb{A}^n_K \mid f_i(x_1, \ldots, x_n) = 0 \, \forall \, 1 \leq i \leq n \}$$

If $H_{f_1,\ldots,f_m}$ is an affine variety over $\mathbb{F}_q$ then we may define $N_s = |H_{f_1,\ldots,f_m}(\mathbb{F}_{q^s})|$ and the zeta-function for $H_{f_1,\ldots,f_m}$ in exactly the same way as we did for affine hypersurfaces.

Proposition 4.6.4. *Let $H_{f_1,\ldots,f_n}$ be an affine variety over $\mathbb{F}_q$. Then the zeta-function for this variety is rational.*

[3] here we include the possibility of the so-called **prime at infinity**, ∞. This corresponds to the absolute value $|\cdot|_\infty$

Proof. We shall prove the proposition by induction on the number of polynomials f_i. If $n = 1$ then H_{f_1} is simply a hypersurface and its zeta-function is rational by Dwork's Theorem. Suppose the proposition holds for all $1 \leq i \leq n-1$. We have that

$$H_{f_1,\ldots,f_{n-1}} = H_{f_1} \cap \cdots \cap H_{f_{n-1}}$$

By the inclusion-exclusion principle we have, for any $s \geq 1$,

$$\begin{aligned} \left| \bigcup_{i=1}^{n} H_{f_i}(\mathbb{F}_{q^s}) \right| &= \sum_{i=1}^{n} |H_{f_i}(\mathbb{F}_{q^s})| - \sum_{i<j} |H_{f_i}(\mathbb{F}_{q^s}) \cap H_{f_j}(\mathbb{F}_{q^s})| \\ &+ \sum_{i<j<k} |H_{f_i}(\mathbb{F}_{q^s}) \cap H_{f_j}(\mathbb{F}_{q^s}) \cap H_{f_k}(\mathbb{F}_{q^s})| \\ &\vdots \\ &+ (-1)^{n-1} |H_{f_1}(\mathbb{F}_{q^s}) \cap \cdots \cap H_{f_n}(\mathbb{F}_{q^s})| \end{aligned}$$

Note that $\cup_{i=1}^{n} H_{f_i}$ is simply the hypersurface $H_{f_1 \cdots f_n}$. We thus see that we can describe the number of points of $H_{f_1,\ldots,f_n}$ in terms of the number of points of hypersurfaces and varieties of dimension strictly less than n. By the induction hypothesis and Dwork's Theorem, the zeta-function of $H_{f_1,\ldots,f_n}$ can be expressed as products of rational zeta functions of such hypersurfaces and lower dimensional varieties. Therefore, the zeta-function of $H_{f_1,\ldots,f_n}$ is itself rational. □

Chapter 5

The Weil Conjectures

Dwork's Theorem fits into a larger framework of now-proven results concerning the zeta-function of varieties. They were introduced by André Weil in 1949 in his influential paper [Wei49]. In order to state the conjectures in full generality, we shall generalise our idea of varieties to projective space.

Definition 5.1. Let K be a field. Define an equivalence relation $\sim$ on $\mathbb{A}_K^{n+1} \setminus \{ 0 \}$ where $(a_1, \ldots, a_{n+1}) \sim (b_1, \ldots, b_{n+1})$ if and only if there exists $\lambda \in K^\times$ such that $a_i = \lambda b_i$ for all $1 \leq i \leq n+1$. We define **n-dimensional projective space**, denoted $\mathbb{P}_K^n$, to be the set of all equivalence classes of this equivalence relation.

Intuitively, we see that $\mathbb{P}_K^n$ is the set of all lines through the origin in $\mathbb{A}_K^{n+1}$. $\mathbb{A}_K^n$ embeds in $\mathbb{P}_K^n$ by the inclusion mapping $(a_1, \ldots, a_n) \mapsto [(1, a_1, \ldots, a_n)]$. The image of $\mathbb{A}_K^n$ is clearly all of $\mathbb{P}_K^n$ except for the equivalence classes of ordered pairs with zero x_0 coordinates. We shall refer to such equivalence classes as the **points at infinity** of $\mathbb{P}_K^n$. It is easy to see that the set of all points at infinity of $\mathbb{P}_K^n$ are 'isomorphic' to $\mathbb{P}_K^{n-1}$. Indeed, there is a bijection between the equivalence classes of $(0, x_1, \ldots, x_n)$ in $\mathbb{P}_K^n$ and the equivalence classes of $(x_1, \ldots, x_n)$ in $\mathbb{P}_K^{n-1}$. We can repeat this process to see that $\mathbb{P}_K^n$ is the following disjoint union: $\mathbb{P}_K^n = \mathbb{A}_K^n \cup \mathbb{A}_K^{n-1} \cdots \cup \mathbb{A}_K^1 \cup (\text{point at infinity})$

Definition 5.2. Let K be a field and $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ a polynomial. The **homogeneous completion** of f is the polynomial $\overline{f}(X_0, \ldots, X_n) = X_0^{\deg f} f(X_1/X_0, \ldots, X_n/X_0)$.

The homogeneous completion of a polynomial is naturally a homogenous polynomial in the degree of f. Now, if $\overline{f}(X_0, X_1, \ldots, X_n) \in K[X_0, X_1, \ldots, X_n]$ is a homogeneous polynomial and $\overline{f}(x_0, x_1, \ldots, x_n) = 0$ then clearly $\overline{f}(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = 0$ for any $\lambda \in K^\times$. Hence it makes sense to consider the points (equivalence classes) of $\mathbb{P}_K^n$ where $\overline{f}$ vanishes. This motivates the following definition:

Definition 5.3. Let K be a field and $\overline{f}_1, \ldots, \overline{f}_m \in K[X_0, X_1, \ldots, X_n]$ a homogeneous polynomial. We define the **projective variety** defined by the $\overline{f}_i$, denoted $H_{\overline{f}_1, \ldots, \overline{f}_m}$ to be the set of points in $\mathbb{P}_K^n$ at which each of the $\overline{f}_i$ simultaneously vanish.

Example 5.4. Consider the projective hypersurface $H_{\overline{f}}$ over $\mathbb{P}_{\mathbb{F}_q}^1$ defined by the homogeneous polynomial $\overline{f}(X_0, X_1) = X_0$. Then, using the fact that $\mathbb{P}_{\mathbb{F}_q}^1 = \mathbb{A}_{\mathbb{F}_q}^1 \cup (\text{point at infinity})$, we have $N_s = |H_{\overline{f}}(\mathbb{F}_{q^s})| = q^s + 1$. We can then define the zeta-function for this hypersurface in exactly the same way as for affine hypersurfaces:

$$Z(H_{\overline{f}}/\mathbb{F}_q; T) = \exp\left(\sum_{s=1}^{\infty} \frac{(q^s+1)T^s}{s}\right) = \frac{1}{(1-T)(1-qT)}$$

Definition 5.5. Let K be a field and $H_{\overline{f}_1,\ldots,\overline{f}_m}$ a projective variety defined by homogeneous polynomials $\overline{f}_1,\ldots,\overline{f}_m \in K[X_0,X_1,\ldots,X_n]$. We say that $H_{\overline{f}_1,\ldots,\overline{f}_m}$ is **smooth** if the partial derivatives of each $\overline{f}_i$ with respect to all indeterminates do not vanish simultaneously.

We can now state the Weil conjectures. Let H be a smooth projective variety defined over $\mathbb{P}^n_{\mathbb{F}_q}$. Then the zeta-function of H enjoys the following properties:

1. **Rationality**

   $$Z(H/\mathbb{F}_q;T) = \frac{P_1(T)\ldots P_{2n-1}(T)}{P_0(T)\ldots P_{2n}(T)}$$

   where $P_0(T) = 1-T, P_{2n}(T) = 1-q^nT$ and each $P_i(T)$ factors over $\mathbb{C}$ as

   $$P_i(T) = \prod_j (1-\alpha_{ij}T)$$

   for some algebraic numbers α_{ij}.

2. **Functional equation**

   $$Z(H/\mathbb{F}_q;1/(q^nT)) = \pm q^{n\varepsilon/2}T^{\varepsilon}Z(H/\mathbb{F}_q;T)$$

   where $\varepsilon \in \mathbb{Z}$ is the **Euler characteristic** of H.

3. **Riemann Hypothesis** - Each α_{ij} for $1 \le i \le 2n-1$ in the expansion above satisfies $|\alpha_{ij}|_\infty = q^{i/2}$.

In light of the above, we can see that Dwork's proof of the rationality of zeta-function was quite remarkable in that it was far more general than Weil conjectured. Indeed, Dwork's proof was targeted at affine hypersurfaces regardless of their smoothness. This result then implies the rationality for smooth projective varieties. In addition to this, Weil originally hypothesised that the proof of the conjectures would depend on a suitable so-called Weil cohomology theory[1]. However, Dwork's proof relied solely on p-adic analysis which certainly came as a surprise to his contemporaries. The functional equation and rationality were proven together by Alexander Grothendieck in 1965 after the development of étale cohomology. Pierre Deligne then built upon his efforts and proved the Riemann hypothesis component of the conjectures in 1974.

The Weil conjectures found many uses in pure mathematics - especially in number theory. They are also highly applicable in areas such as coding theory and cryptography. Despite Dwork's proof being superseded by Grothendieck's, it is not only of historical interest. Indeed, Lauder and Wan [LW08] recently used Dwork's proof to construct a deterministic, polynomial time algorithm for computing the zeta-function of varieties over finite fields of small characteristic.

[1] The details of this is outside the scope of this dissertation. We shall simply state that, given an algebraically closed field k and a coefficient field K, then a Weil cohomology is a contravariant functor (satisfying certain properties) between the category of smooth projective varieties defined over k and the category of graded K-algebras

Chapter 6

Conclusion

In retrospect, we have given a rigorous exposition of Dwork's Theorem through the application of p-adic analysis. In order to achieve this goal, we discussed the p-adic numbers $\mathbb{Q}_p$ which are obtained as a completion of the rational numbers with respect to a non-Archimedean absolute value $|\cdot|_p$. The properties of the extensions of $\mathbb{Q}_p$ were analysed and this allowed us to construct a unique multiplicative homomorphism from finite fields to p-adic roots of unity, the Teichmüller lift τ_f. Furthermore, we sought out a p-adic analogue to $\mathbb{C}$, namely the complex p-adic numbers $\mathbb{C}_p$. This field is algebraically closed and complete with respect to the extended $|\cdot|_p$ and it is the domain in which we proved Dwork's Theorem.

After the construction of $\mathbb{C}_p$, we turned our sights towards analysis in this field. We constructed p-adic analogues of the exponential, logarithm and binomial expansions functions and discussed their convergence and continuity. In particular, we used Dwork's Lemma to construct a p-adic power series which is at the heart of Dwork's proof. In addition, we discussed Newton polygons and their role in proving the p-adic analogue of the Weierstrass Preparation Theorem.

To prove Dwork's Theorem, we first gave a necessary and sufficient condition for a power series with coefficients in a field to be a rational function - Borel's Theorem. In order to apply this result, we had to show that the zeta-function of any affine hypersurface is necessarily p-adic meromorphic. To this end, we discussed particular endomorphisms of $\mathbb{C}_p[[X_1, \ldots, X_n]]$ and proved Dwork's Trace Formula. We then applied this trace formula to a so-called lifting of a trace character to a function on $\mathbb{C}_p$. This allowed us to express the zeta-function in terms of alternating products of p-adic meromorphic functions. Dwork's Theorem then followed by proving a result found in Dwork's original paper which combined the fact that the zeta-function is holomorphic on a disc in $\mathbb{C}$ and p-adic meromorphic.

Thanks to Dwork's Theorem, the original problem of determining the number of solutions to polynomial equations over finite fields was solved. Since the zeta-function is rational, we are able to completely determine the number of solutions in each extension of a finite field through a recursive sequence.

Dwork's Theorem led us naturally on to the more general framework of the Weil conjectures. In particular, we examined smooth projective varieties and discussed the properties that their zeta-functions satisfy. These were rationality, a functional equation and an analogue of the Riemann Hypothesis.

Notation Index

Symbol	**Meaning**	**Page**
$\mathbb{A}^n_K$	n-dimensional affine space over the field K	2
$\mathbb{F}_q$	Finite field of order q	2
$\overline{K}$	Algebraic closure of the field K	2
$Z(H/K;T)$	Zeta-function of the variety H defined over the field K in T	3
v_p	p-adic valuation for some prime p	5
$\mathbb{Q}_p$	p-adic numbers for some prime p	6
$\mathbb{Z}_p$	p-adic integers for some prime p	6
$\lvert \cdot \rvert_\infty$	Euclidean absolute value	6
$\lvert \cdot \rvert_p$	p-adic absolute value for some prime p	6
$\mathrm{Gal}(L/K)$	Galois group of the Galois extension L/K	10
$\mathrm{N}_{L/K}(\alpha)$	Algebraic norm of α from L to K	10
$\mathcal{O}_K$	Ring of integers of the (p-adic) number field K	13
$\mathfrak{p}_K$	Unique maximal ideal of $\mathcal{O}_K$	13
$\mu_n(\mathcal{O}_K)$	Cyclic group of n^{th} roots of unity in $\mathcal{O}_K$	16
$\tau(x)$	Teichmüller lift	16
$\mathbb{C}_p$	Complex p-adic numbers for some prime p	18
$D_c(r)$	Open disc of radius r about c in $\mathbb{C}_p$	20
$D_c[r]$	Closed disc of radius r about c in $\mathbb{C}_p$	20
$\log_p(X)$	p-adic logarithm for some prime p	21
$\exp_p(X)$	p-adic exponential for some prime p	22
$B_{a,p}(X)$	p-adic binomial expansion for some $a \in \mathbb{C}_p$ and prime p	23
U	Set of all positive $\mathbb{Z}$ n-tuples	37
R_0	Set of overconvergent power series	38
Ψ	Dwork's endomorphism of $\mathbb{C}_p[[X_1, \ldots, X_n]]$	40
$\mathrm{Tr}_{L/K}(\alpha)$	Algebraic trace of α from L to K	43
Θ	Trace character lifting power series	45
$\mathbb{P}^n_K$	n-dimensional projective space over the field K	52

Bibliography

[Wei49] André Weil. "Numbers of solutions of equations in finite fields". In: *Bull. Amer. Math. Soc.* 55 (1949), pp. 497–508. ISSN: 0002-9904.

[Dwo60] Bernard Dwork. "On the Rationality of the Zeta Function of an Algebraic Variety". In: *American Journal of Mathematics* 82.3 (1960), pp. 631–648. ISSN: 00029327, 10806377.

[Mon70] Paul Monsky. *p-adic analysis and Zeta functions.* Lectures in Mathematics. Kinkokuniya bookstore, 1970.

[Kob84] Neal Koblitz. *p-adic Numbers, p-adic analysis and Zeta-functions.* 2nd ed. Graduate Texts in Mathematics. Springer, 1984. ISBN: 9787510004537.

[Ste89] Ian Stewart. *Galois Theory.* 2nd ed. Champion and Hall, 1989. ISBN: 0412345404.

[Gou93] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction.* Universitext. Springer, 1993. ISBN: 9783540568445.

[Rob00] Alain M. Robert. *A Course in p-adic Analysis.* 1st ed. Graduate Texts in Mathematics. Springer, 2000. ISBN: 9780387986692.

[Mur02] M. Ram Murty. *An introduction to p-adic Analytic Number Theory.* American Mathematical Society, 2002. ISBN: 9780821832622.

[LW08] Alan G.B. Lauder and Daqing Wan. "Counting points on varieties over finite fields of small characteristic." In: *Algorithmic number theory. Lattices, number fields, curves and cryptography.* Cambridge: Cambridge University Press, 2008, pp. 579–612. ISBN: 9780521808545.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* 2nd ed. Graduate Texts in Mathematics 106. Springer-Verlag New York, 2009. ISBN: 9780387094939.

[Tho10] Jack Thorne. *p-adic analysis, p-adic arithmetic.* 2010. URL: `http://www.math.harvard.edu/~thorne/all.pdf` (Retrieved 21/03/2016).

[Mus11] Mircea Mustaţă. *Zeta functions in algebraic geometry.* 2011. URL: `http://www.math.lsa.umich.edu/~mmustata/zeta_book.pdf` (Retrieved 21/03/2016).

[Tao14] Terence Tao. *Dworks proof of rationality of the zeta function over finite fields.* 2014. URL: `https://terrytao.wordpress.com/2014/05/13/dworks-proof-of-rationality-of-the-zeta-function-over-finite-fields/` (Retrieved 21/03/2016).