5-2014

Local Zeta Functions over p-Adic Fields

Stephen P. Cameron
College of William and Mary

Local Zeta Functions over p-Adic Fields

A thesis submitted in partial fulfillment of the requirement
for the degree of Bachelor of Science in Mathematics from
The College of William & Mary

by

Stephen Philip Cameron

Accepted for _____

Professor Christopher Ryan Vinroot

Professor Vladimir Bolotnikov

Professor Shiwei Zhang

Williamsburg, VA
April 23, 2014

Acknowledgements

Thank you to Professor Vinroot, Professor Bolotnikov, and Professor Zhang for serving on my committee and giving me the time I needed to complete this work. In particular, I'd like to thank Professor Vinroot for his time, patience, and understanding throughout this whole process. Finally, thank you to everyone who supported me throughout this past year.

Abstract

A p-adic field K is a finite extension of the p-adic numbers $\mathbb{Q}_p$. The ring of integers O_K is the integral closure of the p-adic integers $\mathbb{Z}_p$, with unique maximal ideal $\pi_K O_K$. We can define a non-Archimedean absolute value $|\cdot|_K$ on K such that $O_K = \{x \in K : |x|_K \leq 1\}$ and $\pi_K O_K = \{x \in K : |x|_K < 1\}$. The field K is locally compact, and has a unique Haar measure μ_K normalized such that $\mu_K(O_K) = 1$. For any polynomial $f \in O_K[x_1, x_2, \ldots, x_n]$, we define the local zeta function of f as

$$Z(f,s) = \int_{O_K^n} |f(\mathbf{x})|_K^s d\mu_K^n(\mathbf{x}).$$

Igusa's theorem states that this is a rational function of q^{-s}, where $q = \text{card}(O_K/\pi_K O_K)$. Given a polynomial in $f \in O_K[x_1, x_2, \ldots, x_n]$, the Poincarè series of f is the infinite series

$$Q(f,t) = \sum_{m=0}^{\infty} N_m t^m,$$

where $N_m = \text{card}(\{\mathbf{x} \in (O_K/\pi_K^m O_K)^n : f(\mathbf{x}) \in \pi_K^m O_K\})$ is the number of zeroes of f mod π_K^m. These two functions are related by

$$Q(f, q^{-n}t) = \frac{tZ(f,s) - 1}{t - 1},$$

where we take $t = q^{-s}$. Thus calculating the zeta function of f allows us to count the number of zeroes of f mod π_K^m.

This thesis is broken up into two main sections. In section 1, we construct the p-adic numbers $\mathbb{Q}_p$ and prove necessary properties of p-adic fields. In section 2, we consider the Haar measure on K^n. We then define local zeta functions and state necessary theorems for the calculation of them. We then define Poincaré series, and do some basic calculations with them. For a special case, we derive a recursive relation for the coefficients of the Poincaré series using the relation between the local zeta function and the Poincaré series. In the appendix, we show how local

zeta functions may be considered on K-analytic manifolds, ending with a proof of Serre's theorem.

Contents

Chapter 1

p-Adic Background

1.1 p-Adic Absolute Value

An absolute value on a field K is a function $|\cdot|_K : K \to \mathbb{R}$ with the following properties:

1. $|x|_K \geq 0$, and $|x|_K = 0$ if and only if $x = 0$ (positive definite)
2. $|xy|_K = |x|_K|y|_K$ (multiplicative)
3. $|x + y|_K \leq |x|_K + |y|_K$ (triangle inequality)

for all $x, y \in K$. We say that $|\cdot|_K$ is a non-Archimedean absolute value if it satisfies the stronger property that

4. $|x + y|_K \leq \max\{|x|_K, |y|_K\}$ (strong triangle inequality)

for all $x, y \in K$, and we say it is Archimedean otherwise. An absolute value on K induces a metric, $d(x, y) = |x - y|_K$, which induces a topology on K.

Proposition 1.1.1. *Let K be a field, and $|\cdot|_K : K \to \mathbb{R}$ be an absolute value on K. Then K is a topological field with respect to the induced topology, i.e. the maps*

$$(x, y) \to x + y, \quad (x, y) \to xy, \quad x \to x^{-1}$$

are continuous on $K \times K$ and $K^\times = K \setminus \{0\}$ respectively.

Proof. Let $\epsilon > 0$, $z \in K$, and $x, y \in K$ be such that $x + y = z$. Then we must find a $\delta > 0$ such that $|x - x'|_K, |y - y'|_K < \delta$ implies $|z - (x' + y')|_K < \epsilon$. As $|z - (x' + y')|_K = |(x + y) - (x' + y')|_K \leq |x - x'|_K + |y - y'|_K$, by taking $\delta = \epsilon/2$ we get that $|z - (x' + y')|_K < \epsilon$. Thus the map $(x, y) \to x + y$ is continuous.

Now let $x, y \in K$ be such that $xy = z$. Then as $|z - x'y'|_K = |xy - x'y'|_K = |(xy - x'y) + (x'y - x'y')|_K \leq |x - x'|_K|y|_K + |x'|_K|y - y'|_K$. Thus by taking $\delta_x = \dfrac{\epsilon}{2|y|_K}$ and $\delta_y = \dfrac{\epsilon}{2(|x|_K + \delta_x)}$, we get that $|x - x'|_K < \delta_x$ and $|y - y'|_K < \delta_y$ implies $|z - x'y'|_K < \epsilon$. Thus the map $(x, y) \to xy$ is continuous.

Finally, let $x' \in K^\times$. Then $|x^{-1} - x'^{-1}|_K = \left|\dfrac{x' - x}{xx'}\right|_K$. Thus by taking $\delta = \dfrac{\epsilon|x|_K^2}{1 + \epsilon|x|_K}$, we get that $|x - x'|_K < \delta$ implies $|x^{-1} - x'^{-1}|_K < \epsilon$. Thus the map $x \to x^{-1}$ is continuous, and thus K is a topological field. □

We now consider absolute values on $\mathbb{Q}$, the set of rational numbers. An example of an Archimedean absolute value is the standard absolute value, defined by

$$|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$$

To get a non-Archimedean absolute value, let p be a prime number. Then any nonzero $x \in \mathbb{Q}$ can be written in the form $x = p^m \dfrac{a}{b}$ where $a, b, m \in \mathbb{Z}$ and a, b are not divisible by p. We then define the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ by $|x|_p = p^{-m}$ if $x \neq 0$ and $|0|_p = 0$.

Proposition 1.1.2. *$|\cdot|_p$ is a non-Archimedean absolute value on $\mathbb{Q}$.*

Proof. The definition is independent of our choice of a, b (provided they are not divisible by p), so $|x|_p$ is well defined. We also have by definition that $|x|_p \geq 0$ and $|x|_p = 0$ if and only if $x = 0$.

Given $x, y \in \mathbb{Q}$, without loss of generality assume $|x|_p \geq |y|_p$. If $y = 0$ then $xy = 0$, so $|xy|_p = 0$ and $|x|_p|y|_p = |x|_p \times 0 = 0$. Else, we can write $x = p^m \dfrac{a}{b}$ and $y = p^n \dfrac{c}{d}$ with $a, b, c, d, m, n \in \mathbb{Z}$ and a, b, c, d not divisible by p. Then ac, bd are also not divisible by p, so $|xy|_p = |p^{m+n}\dfrac{ac}{bd}|_p = p^{-(m+n)} = |x|_p|y|_p$. Thus $|xy|_p = |x|_p|y|_p$.

Now, if $y = 0$ then $|x + y|_p = |x|_p = \max\{|x|_p, 0\} = \max\{|x|_p, |y|_p\}$. Else, as $|x|_p \geq |y|_p$, we have that $m \leq n$. Thus $|x+y|_p = \left|\dfrac{p^m ad + p^n bc}{bd}\right|_p = |p^m ad + p^n bc|_p = |p^m(ad + p^{n-m}bc)|_p = |p^m|_p|ad + p^{n-m}bc|_p$. As $m \leq n$, we have that $(ad + p^{n-m}bc)$ is an integer and thus $|ad + p^{n-m}bc|_p \leq 1$. Thus $|x + y|_p \leq |p^m|_p = |x|_p$ whenever $|x|_p \geq |y|_p$, so $|x + y|_p \leq \max\{|x|_p, |y|_p\}$. Note that if $n > m$, then $p^{n-m}bc$ is divisible by p but ad is not, so $|x + y|_p = |x|_p|ad + p^{n-m}bc|_p = |x|_p$. □

So, $|\cdot|_p$ is a well defined non-Archimedean absolute value on $\mathbb{Q}$. We can use it to induce a metric on $\mathbb{Q}$ by $d_p(x, y) = |x - y|_p$. Moreover, as $|\cdot|_p$ is non-Archimedean, it follows that $d_p(\cdot, \cdot)$ is an ultra metric, meaning it satisfies the additional property

that $d_p(x,y) \leq \max\{d_p(x,z), d_p(z,y)\}$ for all $x, y, z \in \mathbb{Q}$. An ultrametric space is a pair (X,d) where X is a set and d is an ultrametric on X. Ultrametric spaces have several counterintuitive properties.

Proposition 1.1.3. *Let (X,d) be an ultrametric space. Then*

1. *Suppose $B, B' \subseteq X$ are open balls and $B \cap B' \neq \emptyset$. Then either $B \subseteq B'$ or $B' \subseteq B$.*
2. *Let $B \subseteq X$ be an open ball. Then any point in B is a center for B, i.e. $B(x,r) = B(y,r)$ whenever $d(x,y) < r$.*
3. *All open balls are closed, and all closed balls are open.*
4. *X is totally disconnected, i.e. the only connected subspaces of X are the single point subsets.*

Proof. 1. Let $x, y \in X$ and $r, r' > 0$ be such that $B(x,r) \cap B(y,r') \neq \emptyset$. Without loss of generality, we may assume $r \geq r'$, and then take $z \in B(x,r) \cap B(y,r')$. As $d(x,y) \leq \max\{d(x,z), d(y,z)\} < \max\{r, r'\} = r$, we have that $y \in B(x,r)$. Then for any $y' \in B(y,r')$, we have that $d(x,y') \leq \max\{d(x,y), d(y,y')\} < \max\{r, r'\} = r$, so $y' \in B(x,r)$. Thus $B(y,r') \subseteq B(x,r)$.

2. Let $x \in X$, $r > 0$, and $y \in B(x,r)$. Then as $B(x,r) \cap B(y,r) \neq \emptyset$, we have that either $B(x,r) \subseteq B(y,r)$ or $B(y,r) \subseteq B(x,r)$. But as $x \in B(y,r)$, we have that the situation is symmetric in x and y, and thus we must have $B(x,r) = B(y,r)$.

3. Let $x \in X$ and $r > 0$. Suppose that y is in the closure of $B(x,r)$. Then for any $\epsilon > 0$, we have that $B(x,r) \cap B(y,\epsilon) \neq \emptyset$. In particular, $B(x,r) \cap B(y,r/2) \neq \emptyset$, so $B(y,r/2) \subseteq B(x,r)$. Thus $y \in B(x,r)$, so $B(x,r)$ is closed.

   Now let $B[x,r] = \{y \in X : d(x,z) \leq r\}$ be the closed ball of radius r about x. Let $y \in B[x,r]$, and let $z \in B(y,r)$. Then as $d(x,z) \leq \max\{d(x,y), d(y,z)\} \leq r$, we have that $z \in B[x,r]$. Thus $B(y,r) \subseteq B[x,r]$, and as y was an arbitrary point of $B[x,r]$, we have that $B[x,r]$ is open.

4. Let $Y \subseteq X$ have more than two points. Then there are $x, y \in Y$ such that $x \neq y$. Thus $d(x,y) = r > 0$, so consider $B(x,r)$. As $x \in B(x,r)$ and $y \notin B(x,r)$, we have that $B(x,r)$ is a nonempty proper subset of Y. By (3.) we also have that $B(x,r)$ is clopen, and thus Y is disconnected. Thus X is totally disconnected.

□

In the case of $(\mathbb{Q}, |\cdot|_p)$, part (3.) of the above proposition is particularly easy to see, since the nonzero values $|\cdot|_p$ takes are a discrete subset of $\mathbb{R}_+$. Thus $\{y \in \mathbb{Q} : |x-y|_p \leq r\} = \{y \in \mathbb{Q} : |x-y|_p < r+\epsilon\}$ for sufficiently small $\epsilon > 0$, so all closed balls are open and viceversa. Suffice it to say that under $|\cdot|_p$, the topology on $\mathbb{Q}$ is very different than the standard topology that we are used to.

Example: Consider the infinite series $\sum_{i=0}^{\infty} p^i$; as for any $n \in \mathbb{N}$ we have that

$$|(1-p)\sum_{i=0}^{n} p^i - 1|_p = |-p^{n+1}|_p = p^{-(n+1)} \to 0$$

as $n \to \infty$. Thus $\lim_{n\to\infty}(1-p)\sum_{i=0}^{n} p^i = (1-p)\sum_{i=0}^{\infty} p^i = 1$, and thus $\sum_{i=0}^{\infty} p^i = \frac{1}{1-p}$. The same argument shows that $\sum_{i=0}^{\infty} p^{ir} = \frac{1}{1-p^r}$. We also get that

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

We now show that any rational number has a "Laurent series expansion base p," that is for any $x \in \mathbb{Q}$, $x = \sum_{i=m}^{\infty} c_i p^i$, where $c_i \in \{0, 1, \ldots, p-1\}$ and $m \in \mathbb{Z}$ is such that $c_m \neq 0$. As $|\sum_{i=m}^{n} c_i p^i|_p = |c_m p^m|_p = p^{-m}$ for every $n \geq m$, it follows that $|x|_p = |\sum_{i=m}^{\infty} c_i p^i|_p = p^{-m}$. Furthermore, as $\sum_{i=m}^{\infty} |c_i p^i|_p \leq \sum_{i=m}^{\infty} p^{-i} = \frac{p^{m+1}}{p-1} < \infty$, we have that the Laurent expansion is absolutely convergent, so these expansions can be manipulated in the same way that absolutely convergent series in the real and complex numbers can. In particular, the order in which we sum terms is irrelevant.

Proposition 1.1.4. *Let x be a rational number. Then x has Laurent expansion base p.*

Proof. To show the existence, we must first show that if x and y have expansions, then so does $x+y$. So, let $x = \sum_{i=m}^{\infty} c_i p^i$ and $y = \sum_{i=k}^{\infty} d_i p^i$, and let us denote the partial sums $\sum_{i=m}^{n} c_i p^i, \sum_{i=k}^{n} d_i p^i$ by x_n, y_n respectively for all $n \geq \max\{m,k\}$. Without loss of generality, let $m \leq k$. Then as both x_n, y_n can be written as

finite sums, it is clear that $x_n + y_n = \sum_{i=m}^{n+1} e_{i,n}p^i$ for some $e_{i,n} \in \{0, \ldots, p-1\}$. As $c_i, d_i \geq 0$, it follows that $e_{i,N} = e_{i,M}$ for all $i \leq \min\{N, M\}$. Thus taking $e_i = e_{i,i+1}$, we may write $x_n + y_n = \sum_{i=m}^{n} e_i p^i + e_{n+1,n}p^{n+1}$, where $e_{n+1,n} = 0$ or 1. Thus $|x + y - \sum_{i=m}^{n} e_i p^i|_p = |(x - x_n) + (y - y_n) + e_{n+1,n}p^{n+1}|_p \leq p^{-(n+1)} \to 0$ as $n \to \infty$. Thus $x + y = \sum_{i=m}^{\infty} e_i p^i$, so it has an expansion as well.

It is clear that a rational number x can be written as $x = \sum_{i=m}^{n} c_i p^i$ for some $n \geq m \geq 0$ if and only if x is a nonnegative integer. Given a positive integer $k = \sum_{i=m}^{\infty} c_i p^i$ (where $m \geq 0$, $c_m \neq 0$, and $c_i = 0$ for all but finitely many i), it follows that $-k = (p - c_m)p^m + \sum_{i=m+1}^{\infty} (p - c_i - 1)p^i$. Thus there exists an expansion for any integer. Now let $x \in \mathbb{Q} \setminus \mathbb{Z}$. Then $x = \frac{a}{b}$ for some $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ with $b > 1$. Without loss of generality, was may assume that b is not divisible by p, as else $b = p^k b'$ for some b' relatively prime to p. It then follows that if $x' = \frac{a}{b'} = \sum_{i=m}^{\infty} c_i p^i$, then $x = p^{-k}x' = \sum_{i=m-k}^{\infty} c_{i+k}p^i$. Furthermore, as we have shown that any integer has an expansion and that having an expansion is preserved under addition, we can shift x by integer values so that without loss of generality, we may assume that $x < 0$.

As p and b are relatively prime, there must be a positive integer r such that $p^r \equiv 1 \mod b$. Thus there is an integer $c \in \mathbb{N}$ such that $bc = p^r - 1$. Thus $x = \frac{a}{b} = \frac{ac}{bc} = \frac{-ac}{1-p^r}$. As $x < 0$, we have that $a < 0$, so $-ac$ is a positive integer. Thus $x = -ac\frac{1}{1-p^r} = (-ac)\sum_{j=0}^{\infty} p^{jr} = \underbrace{(1+1+1+\ldots+1)}_{-ac \text{ times}}\sum_{j=0}^{\infty} p^{jr}$ is a finite sum of Laurent expansions, so $x = \sum_{i=0}^{\infty} c_i p^i$ for some $c_i \in \{0, \ldots, p-1\}$.

□

With the latter proposition out of the way, we now get to the main point. Consider a $|\cdot|_p$-Cauchy sequence $(r_k)_{k=1}^{\infty}$ of rational numbers, where $r_k = \sum_{i=-\infty}^{\infty} c_{i,k}p^i$

($c_i \neq 0$ for only finitely many $i < 0$). As it is a Cauchy sequence, for any $N \in \mathbb{Z}$, there is an $M_N \in \mathbb{N}$ such that for all $k, l > M_N$, we have that $|r_k - r_l|_p = |\sum_{i=-\infty}^{\infty} c_{i,k}p^i - \sum_{i=-\infty}^{\infty} c_{i,l}p^i|_p < p^{-N}$. But $r_k - r_l = \sum_{i=m}^{\infty} c'_i p^i$ for some $m \in \mathbb{Z}$ with $c'_i \in \{0, \ldots, p-1\}$ and $c'_m \neq 0$. This means that $|r_k - r_l|_p = p^{-m} < p^{-N}$, so $m > N$ and thus $c_{i,k} = c_{i,l}$ for all $i < m$. So, that means each term in our expansion stabilizes eventually, so we can take $c_i = \lim_{k\to\infty} c_{i,k}$ for each $i \in \mathbb{Z}$. It is clear then that if $r = \sum_{i=-\infty}^{\infty} c_i p^i \in \mathbb{Q}$, then $r_k \to r$. The only problem is that there is no reason that $\sum_{i=1}^{\infty} c_i p^i$ converges in $\mathbb{Q}$, but this is easily fixed.

1.2 *p*-Adic Numbers

Definition 1.2.1. We define the p-adic numbers $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ with respect to the metric $d_p(\cdot, \cdot)$, i.e. as the space of equivalence classes of Cauchy sequences in $\mathbb{Q}$ under d_p.

We can identify $\mathbb{Q}$ with a dense subspace of $\mathbb{Q}_p$ by identifying each $r \in \mathbb{Q}$ with $[(r)_{k=1}^{\infty}]$, the equivalence class of the constant sequence $(r)_{k=1}^{\infty}$. Let $x, y \in \mathbb{Q}_p$ and $(x_k)_{k=1}^{\infty}, (y_k)_{k=1}^{\infty}$ be Cauchy sequences of rational numbers converging to x, y respectively in $\mathbb{Q}_p$. Then the algebraic operations on $\mathbb{Q}$ are extended to $\mathbb{Q}_p$ by taking $x + y = \lim_{k\to\infty} x_k + y_k$, $xy = \lim_{k\to\infty} x_k y_k$, and $x^{-1} = \lim_{k\to\infty} x_k^{-1}$.

Similarly, the p-absolute value is extended to $\mathbb{Q}_p$ by taking $|x|_p = \lim_{k\to\infty} |x_k|_p$. We now show that $|\cdot|_p$ is a non-Archimedean absolute value on $\mathbb{Q}_p$. It follows from the definition that $|x|_p \geq 0$ for all $x \in \mathbb{Q}_p$, and $|x|_p = 0$ implies that there is a sequence of rational numbers $(x_k)_{k=1}^{\infty}$ such that $x_k \to x$ and $|x_k|_p \to 0$. But $|x_k|_p \to 0$ implies that $x_k \to 0$, so $x = 0$. Thus $|\cdot|_p$ is positive definite on $\mathbb{Q}_p$. As for any $x, y \in \mathbb{Q}_p$, we have that $|xy|_p = \lim_{k\to\infty} |x_k y_k|_p = (\lim_{k\to\infty} |x_k|_p)(\lim_{k\to\infty} |y_k|_p) = |x|_p |y|_p$. Thus $|\cdot|_p$ is still multiplicative. Finally, $|x + y|_p = \lim_{k\to\infty} |x_k + y_k|_p \leq \lim_{k\to\infty} \max\{|x_k|_p, |y_k|_p\} = \max\{\lim_{k\to\infty} |x_k|_p, \lim_{k\to\infty} |x_k|_p\} = \max\{|x|_p, |y|_p\}$. Thus $|\cdot|_p$ is still a non-Archimedean absolute value on $\mathbb{Q}_p$.

Thinking of $\mathbb{Q}_p$ as a space of equivalence classes of sequences can make it difficult to visualize, which is why the Laurent expansion for p-adic numbers is so useful.

Theorem 1.2.2. *Any $x \in \mathbb{Q}_p$ can be written uniquely as $x = \sum_{i=-\infty}^{\infty} c_i p^i$ with $c_i \in \{0, \ldots, p-1\}$ and $c_i \neq 0$ for only finitely many $i < 0$. Conversely, every series*

of that form converges in $\mathbb{Q}_p$*, with* $|\sum_{i=-\infty}^{\infty} c_i p^i|_p = p^{-m}$*, where* $m = \min\{i \in \mathbb{Z} : c_i \neq 0\}$.

Proof. Let $m \in \mathbb{Z}$ and $c_i \in \{0, \ldots, p-1\}$ for each $i \geq m$, with $c_m \neq 0$. We first show that $\sum_{i=m}^{\infty} c_i p^i \in \mathbb{Q}_p$. Let $N \geq m$, and $j \in \mathbb{N}$. Then $|\sum_{i=m}^{N+j} c_i p^i - \sum_{i=m}^{N} c_i p^i|_p = |\sum_{i=N+1}^{N+j} c_i p^i|_p \leq p^{-(N+1)}$. Thus the sequences of partial sums is a Cauchy sequence, so as $\mathbb{Q}_p$ is complete, the series converges with $\lim_{N\to\infty} \sum_{i=m}^{N} c_i p^i = \sum_{i=m}^{\infty} c_i p^i \in \mathbb{Q}_p$. Further, as $|\cdot|_p$ is continuous, we have that $|\sum_{i=m}^{\infty} c_i p^i|_p = \lim_{N\to\infty} |\sum_{i=m}^{N} c_i p^i|_p = \lim_{N\to\infty} p^{-m} = p^{-m}$.

Let $x \in \mathbb{Q}_p$. If x is rational, we've already shown that it has a Laurent series base p, so assume that x is not rational. Then let $(x_k)_{k=1}^{\infty}$ be a sequence of rational numbers converging to x, with $x_k = \sum_{i=-\infty}^{\infty} c_{i,k} p^i$. We have that $|x|_p = \lim_{k\to\infty} |x_k|_p = p^{-m}$ for some $m \in \mathbb{Z}$. As the set of nonzero values $|\cdot|_p$ can take is discrete, we must have that $|x_k|_p = p^{-m}$ for sufficiently large k, so by taking a subsequence we may assume without loss of generality that $|x_k|_p = p^{-m}$ for all $k \in \mathbb{N}$. Thus for each k, $x_k = \sum_{i=m}^{\infty} c_{i,k} p^i$, with $c_{m,k} \neq 0$. As $(x_k)_{k=1}^{\infty}$ is a Cauchy sequence, for each $N \in \mathbb{Z}$ there is an integer M_N such that for all $k, l > M_N$, we have that $|x_k - x_l|_p < p^{-N}$. Thus as $x_k - x_l = \sum_{i=m}^{\infty} (c_{i,k} - c_{i,l}) p^i$, with $(c_{i,k} - c_{i,l}) \in \{-(p-1), -(p-2), \ldots, (p-1)\}$ not divisible by p for each i, we have that $|x_k - x_l|_p = p^{-N'}$, where $N' = \min\{i : c_{i,k} \neq c_{i,l}\}$. Thus in particular, $c_{i,k} = c_{i,l}$ for all $i \leq N$ whenever $k, l > M_N$. Thus the sequence $(c_{i,k})_{k=1}^{\infty}$ converges in the discrete topology for each fixed i, so we may define $c_i = \lim_{k\to\infty} c_{i,k}$. We now show that $x = \sum_{i=m}^{\infty} c_i p^i$. It suffices to show that a subsequence $x_{k_n} \to \sum_{i=m}^{\infty} c_i p^i$. Let $k_0 \in \mathbb{N}$ be such that $c_{m,k} = c_m$ for all $k \geq k_0$, and recursively take $k_n > k_{n-1}$ such that $c_{m+n,k} = c_{m+n}$ for all $k \geq k_n$. Then $|\sum_{i=m}^{\infty} c_i p^i - x_{k_n}|_p = |\sum_{i=m+n+1}^{\infty} (c_i - c_{i,k_n}) p^i|_p \leq p^{-(m+n+1)} \to 0$ as $n \to \infty$. Thus $x_{k_n} \to \sum_{i=m}^{\infty} c_i p^i$, and as $x_k \to x$ by assumption, we have that $x = \sum_{i=m}^{\infty} c_i p^i$.

Finally, for uniqueness suppose $x = \sum_{i=m}^{\infty} c_i p^i = \sum_{i=k}^{\infty} d_i p^i$ with $c_m, d_k \neq 0$. Then we must have $|x|_p = |p^m|_p = |p^k|_p$, so $m = k$. Assume that $c_i \neq d_i$ for some $i \geq m$. Let N be such that $c_i = d_i$ for all $i < N$, and $c_N \neq d_N$. Then $|\sum_{i=m}^{\infty} c_i p^i - \sum_{i=m}^{\infty} d_i p^i|_p = |(c_N - d_N)p^N + \sum_{i=N+1}^{\infty} (c_i - d_i)p^i|_p$. As $|(c_i - d_i)p^i|_p = |p^i|_p = p^{-i} < p^{-N} = |(c_N - d_N)p^N|_p$ for all $i > N$, it follows that $|\sum_{i=m}^{\infty} c_i p^i - \sum_{i=m}^{\infty} d_i p^i|_p = p^{-N}$. But $\sum_{i=m}^{\infty} c_i p^i = \sum_{i=k}^{\infty} d_i p^i = x$ so $|\sum_{i=m}^{\infty} c_i p^i - \sum_{i=m}^{\infty} d_i p^i|_p = |x - x|_p = 0$, a contradiction. Thus the expansion is unique.

□

In most cases, using the Laurent expansion is the easiest way to work with p-adic numbers. Of particular importance are the series with no Laurent-part, i.e. of the form $\sum_{i=0}^{\infty} c_i p^i$.

Definition 1.2.3. We define the p-adic integers $\mathbb{Z}_p$ to be the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$

Theorem 1.2.4.

1. $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \{\sum_{i=0}^{\infty} c_i p^i : c_i \in \{0, \ldots, p-1\}\}$
2. $p^n\mathbb{Z}_p = \{\sum_{i=n}^{\infty} c_i p^i : c_i \in \{0, \ldots, p-1\}\} = \{x \in \mathbb{Q}_p : |x|_p \leq p^{-n}\}$ *is a compact, open subring of* $\mathbb{Q}_p$ *for each* $n \geq 0$.
3. $\mathbb{Q}_p$ *is locally compact, i.e. for every* $x \in \mathbb{Q}_p$, *there is a compact set* $C \subset \mathbb{Q}_p$ *such that* x *is contained in the interior of* C.
4. $\mathbb{Z}_p$ *has a unique maximal ideal,* $p\mathbb{Z}_p$.
5. $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$, *the finite field with* p *elements.*

Proof.

1. Let $x \in \mathbb{Z}_p$. Then by definition of $\mathbb{Z}_p$, there is a sequence of integers $(x_k)_{k=1}^{\infty}$ converging to x. Thus as $|x_k|_p \leq 1$ for all $k \in \mathbb{N}$, $|x|_p = \lim_{k\to\infty} |x_k|_p \leq 1$, so $\mathbb{Z}_p \subseteq \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. Conversely, suppose $x \in \mathbb{Q}_p$ with $|x|_p \leq 1$.

Then $x = \sum_{i=-\infty}^{\infty} c_i p^i$ for some $c_i \in \{0, \ldots, p-1\}$. As $|x|_p = p^{-m}$, where $m = \min\{i \in \mathbb{Z} : c_i \neq 0\}$, and $|x|_p \leq 1$, we have that $m \geq 0$. Thus $c_i = 0$ for all $i < 0$, so $x = \sum_{i=0}^{\infty} c_i p^i$ for some $c_i \in \{0, \ldots, p-1\}$. Thus taking $x_k = \sum_{i=0}^{k} c_i p^i$, we have that $(x_k)_{k=0}^{\infty}$ is a sequence of integers with $\lim_{k\to\infty} x_k = \lim_{k\to\infty} \sum_{i=0}^{k} c_i p^i = \sum_{i=0}^{\infty} c_i p^i = x$, and thus $x \in \mathbb{Z}_p$. Thus $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \{\sum_{i=0}^{\infty} c_i p^i : c_i \in \{0, \ldots, p-1\}\}$.

2. Let $n \geq 0$. We first show that $p^n\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. As $|0|_p = 0$, we have that $0 \in p^n\mathbb{Z}_p$ so $p^n\mathbb{Z}_p$ is nonempty with an additive identity. For any $x, y \in p^n\mathbb{Z}_p$, we have that $|x - y|_p \leq \max\{|x|_p, |-y|_p\} = \max\{|x|_p, |y|_p\} \leq p^{-n}$, so $x - y \in p^n\mathbb{Z}_p$. Finally, $|xy|_p = |x|_p|y|_p \leq p^{-n} \times p^{-n} \leq p^{-n}$, so $xy \in p^n\mathbb{Z}_p$ and thus $p^n\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.

   As the map $x \to p^n x$ is a homeomorphism of $\mathbb{Q}_p$, it suffices to show that $\mathbb{Z}_p$ is compact and open. As $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, we have that $\mathbb{Z}_p$ is the closed ball of radius 1 around 0. Thus as $\mathbb{Q}_p$ is an ultra metric space, we have that $\mathbb{Z}_p$ is both open and closed. To prove that $\mathbb{Z}_p$ is compact, we show that it is complete and totally bounded (see Theorem 2 in Section 11 of [3]). As $\mathbb{Z}_p$ is a closed subset of a complete space, it is complete. Totally bounded means that for any $\epsilon > 0$, there are finitely many open balls of radius at most ϵ which cover $\mathbb{Z}_p$. So, let $\epsilon > 0$, $N \in \mathbb{N}$ be such that $p^{-N} < \epsilon$, and $C_N = \{\sum_{i=0}^{N-1} c_i p^i : c_i \in \{0, \ldots, p-1\}\}$. Then $\{x + p^N\mathbb{Z}_p : x \in C_N\}$ is a finite collection of open balls of radius less than ϵ with $\bigcup_{x\in C} x + p^N\mathbb{Z}_p = \mathbb{Z}_p$. Thus $\mathbb{Z}_p$ is compact.

3. As $\mathbb{Z}_p$ is a compact open set and $\mathbb{Q}_p$ is a topological field, $x + \mathbb{Z}_p = \{x + y : y \in \mathbb{Z}_p\}$ is a compact neighborhood of x.

4. Let $x \in \mathbb{Z}_p \setminus \{0\}$. Then as $|x^{-1}|_p = |x|_p^{-1}$, we have that $x^{-1} \in \mathbb{Z}_p$ if and only if $|x|_p = 1$. Thus x is a unit of $\mathbb{Z}_p$ if and only if $|x|_p = 1$. So, $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}$ is the collection of all non-units of $\mathbb{Z}_p$. No proper ideal I of $\mathbb{Z}_p$, can contain any units, so $I \subseteq \mathbb{Z}_p \setminus \{x \in \mathbb{Z}_p : |x|_p = 1\} = p\mathbb{Z}_p$. Thus if we show that $p\mathbb{Z}_p$ is an ideal, it must be the unique maximal ideal. We have

that $p\mathbb{Z}_p$ is a subring of $\mathbb{Z}_p$. As for any $x \in p\mathbb{Z}_p$ and $y \in \mathbb{Z}_p$, we have that $|xy|_p = |x|_p|y|_p \leq p^{-1} \times 1 < 1$, so $xy \in p\mathbb{Z}_p$. Thus $p\mathbb{Z}_p$ is an ideal of $\mathbb{Z}_p$, and thus it is the unique maximal ideal.

5. As $p\mathbb{Z}_p$ is a maximal ideal, we have that $\mathbb{Z}_p/p\mathbb{Z}_p$ must be a field. Now let $x = \sum_{i=0}^{\infty} c_i p^i$. Then $x + p\mathbb{Z}_p = c_0 + p\mathbb{Z}_p$. As there are p choices for c_0, we have that $|\mathbb{Z}_p/p\mathbb{Z}_p| = p$. Thus $\mathbb{Z}_p/p\mathbb{Z}_p$ is a finite field with p elements, so $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$.

□

Remark: We will frequently use the notation $x \equiv y \mod p^n$, meaning $|x - y|_p \leq p^{-n}$, which is equivalent to $x + p^n\mathbb{Z}_p = y + p^n\mathbb{Z}_p$ (where the equality can either be taken as the equality of subsets of $\mathbb{Z}_p$ or as equality in $\mathbb{Z}_p/p^n\mathbb{Z}_p$). We will use these three different notations interchangeably, primarily based on context they arise.

The p-adic integers are a useful space in order to formulate and solve certain number theoretic questions. One of the most useful tools in answering those questions is Hensel's lemma

Theorem 1.2.5. *(Hensel's Lemma): Let* $f(x) = \sum_{j=0}^{n} a_j x^j$ *be a polynomial in* $\mathbb{Z}_p[x]$ *with formal derivative* $f'(x) = \sum_{j=0}^{n} j a_j x^{j-1}$. *Let* $c \in \mathbb{Z}_p$ *be such that* $f(c) \equiv 0 \mod p$ *and* $f'(c) \not\equiv 0 \mod p$. *Then there is a unique* $b \in \mathbb{Z}_p$ *such that* $b \equiv c \mod p$ *and* $f(b) = 0$.

Proof. We prove there is a unique zero by constructing a unique sequence $(c_i)_{i=0}^{\infty} \subset \{0, \ldots, p-1\}^{\infty}$ such that $c_0 \equiv c \mod p$, and each for $n \geq 0$, $b_n = \sum_{i=0}^{n} c_i p^i$ satisfies $f(b_n) \equiv 0 \mod p^{n+1}$. Given that, taking $b = \lim_{n\to\infty} b_n = \sum_{i=0}^{\infty} c_i p^i$, we would then have $|f(b)|_p = \lim_{n\to\infty} |f(b_n)|_p \leq \lim_{n\to\infty} p^{-(n+1)} = 0$. We would then have that b is unique by the uniqueness of our sequence $(c_n)_{n=0}^{\infty}$, completing the proof.

So, let $c_0 \in \{0, \ldots, p-1\}$ be such that $c_0 \equiv c \mod p$. Then as f is a polynomial, we then have that $f(c_0) \equiv f(c) \equiv 0 \mod p$. Taking $b_0 = c_0$, we have our base case. Now suppose that we have chosen $c_0, \ldots, c_{n-1}$ such that $f(b_{n-1}) \equiv 0 \mod p^n$ for some $n \geq 1$. Let $x \in \{0, \ldots, p-1\}$ be indeterminate. Then

$$\begin{aligned} f(b_{n-1}+xp^n) &= \sum_{j=0}^{n} a_j(b_{n-1}+xp^n)^j = \sum_{j=0}^{n} a_j \sum_{k=0}^{j} \binom{j}{k} b_{n-1}^{j-k}(xp^n)^k \\ &\equiv \sum_{j=0}^{n} a_j(b_{n-1}^j + jb_{n-1}^{j-1}xp^n) \mod p^{n+1} = \sum_{j=0}^{n} a_j b_{n-1}^j + \sum_{j=0}^{n} j a_j b_{n-1}^{j-1} xp^n \\ &= f(b_{n-1}) + f'(b_{n-1})xp^n \end{aligned}$$

By induction hypothesis $f(b_{n-1}) \equiv 0 \mod p^n$, so $f(b_{n-1}) \equiv \alpha_n p^n \mod p^{n+1}$ for some $\alpha_n \in \{0, \ldots, p-1\}$. Now, $\alpha_n p^n + f'(b_{n-1})xp^n \equiv 0 \mod p^{n+1}$ if and only if $\alpha_n + f'(b_{n-1})x \equiv 0 \mod p$. As $b_{n-1} \equiv c_0 \equiv c \mod p$, we have that $f'(b_{n-1}) \equiv f'(c) \not\equiv 0 \mod p$. Thus there is a unique $c_n \in \{0, \ldots, p-1\}$ such that $c_n \equiv \dfrac{-\alpha_n}{f'(c)} \mod p$. Fixing this unique value of c_n and taking $b_n = b_{n-1} + c_n p^n = \displaystyle\sum_{i=0}^{n} c_i p^i$ satisfies $f(b_n) \equiv 0 \mod p^{n+1}$ and $b_n \equiv b_{n-1} \mod p^n$. Thus by induction there is a unique sequence $(c_i)_{i=0}^{\infty} \subset \{0, \ldots, p-1\}^{\infty}$, so $b = \displaystyle\sum_{i=0}^{\infty} c_i p^i$ is the unique zero of f with $b \equiv c \mod p$.

□

A nice application of the latter lemma is to the study of permutation polynomials. We say that a polynomial $f \in \mathbb{Z}[x]$ is a permutation polynomial $\mod m$ if for every $\eta \in \{0, \ldots, m-1\}$, there is an integer $\xi \in \{0, \ldots, m-1\}$ such that $f(\xi) \equiv \eta \mod m$ (that is, if f induces a bijection from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$).

A natural question is when is a polynomial f a permutation polynomial $\mod m$? The case when m is a prime can be solved explicitly, and if $m = m_1 m_2$ where $\gcd(m_1, m_2) = 1$, then by the Chinese Remainder Theorem f is a permutation polynomial $\mod m$ if and only if it is a permutation polynomial $\mod m_1$ and $\mod m_2$. The remaining case when m is a power of a prime can be settled using Hensel's Lemma.

Corollary 1.2.6. *A polynomial $f \in \mathbb{Z}[x]$ is a permutation polynomial* $\mod p^n$ *for some $n > 1$ if and only if f is a permutation polynomial* $\mod p$ *and $f'(x) \not\equiv 0 \mod p$ for all $x \in \{0, \ldots, p-1\}$.*

Proof. Suppose f is a permutation polynomial $\mod p$ and $f'(x) \not\equiv 0 \mod p$ for all $x \in \{0, \ldots, p-1\}$, and let $\eta \in \{0, \ldots, p^n - 1\}$. Then we need to show that there is some $\xi \in \{0, \ldots, p^n - 1\}$ such that $f(\xi) = \eta \mod p^n$. Taking $g(x) = f(x) - \eta$, this is equivalent to $g(\xi) = 0$. As f is a permutation polynomial $\mod p$, g is as

well. Thus we have that there is a $c \in \{0, \ldots, p-1\}$ such that $g(c) \equiv 0 \mod p$. As $g'(c) = f'(c) \not\equiv 0 \mod p$, by Hensel's lemma we have that there is a unique p-adic integer b such that $b \equiv c \mod p$ and $g(b) = 0$. Thus taking $\xi \in \{0, \ldots, p^n - 1\}$ such that $\xi \equiv b \mod p^n$, we get that $g(\xi) \equiv 0 \mod p^n$, and thus $f(\xi) \equiv \eta \mod p^n$. Thus as η was arbitrary, we get that f is a permutation polynomial $\mod p^n$.

Now, suppose that f is not a permutation polynomial $\mod p$. Then there is some $\eta \in \{0, \ldots, p-1\}$ such that $f(x) \not\equiv \eta \mod p$ for all $x \in \{0, \ldots, p-1\}$, which is equivalent to $f(x) \not\equiv \eta \mod p$ for any integer x. Thus $f(x) \not\equiv \eta \mod p^n$ for any integer x, so f is not a permutation polynomial $\mod p^n$. Finally, suppose that $f'(\xi) \equiv 0 \mod p$ for some $\xi \in \{0, \ldots, p-1\}$. Then $f(\xi + p^{n-1}) \equiv f(\xi) + f'(\xi)p^{n-1} \mod p^n \equiv f(\xi)$. Thus the map f induces on $\mathbb{Z}/p^n\mathbb{Z}$ isn't injective, so cannot be bijective. Thus f is not a permutation polynomial $\mod p^n$. Thus f is a permutation polynomial $\mod p^n$ for some $n > 1$ if and only if f is a permutation polynomial $\mod p$ and $f'(x) \not\equiv 0 \mod p$ for all $x \in \{0, \ldots, p-1\}$. □

We can also go in the reverse direction to address certain questions about the p-adic integers using elementary number theory. Let p be an odd prime, and consider the polynomial $f(x) = x^2 - a$, for some $a \in \mathbb{Z}_p$. Then as $f'(x) = 2x$, we have that $f'(x) \not\equiv 0 \mod p$ for all $x \not\equiv 0 \mod p$. Thus if $a \not\equiv 0 \mod p$, we have that there is a square root of a in $\mathbb{Z}_p$ if and only if there is a solution to the congruence $x^2 \equiv a \mod p$. That is, if and only if a is a quadratic residue $\mod p$.

Thus since $3^2 \equiv 2 \mod 7$, we have that there is a 7-adic integer $\sqrt{2} \in \mathbb{Z}_7$ with $(\sqrt{2})^2 = 2$ and $\sqrt{2} \equiv 3 \mod 7$. Using algorithm outlined in Hensel's lemma, we can calculate the 7-adic expansion of $\sqrt{2}$. We're given that $c_0 = 3$. Then as $f(3) = 7 = 1 \times 7$, we have that $\alpha_1 = 1$. Thus since $f'(3) \equiv 6 \mod 7$, we have that $c_i \equiv \dfrac{-1}{6} \mod 7 \equiv 1 \mod 7$. Thus $3 + 1 \times 7 = 10 \equiv \sqrt{2} \mod 7^2$. As we then have $f(10) = 98 = 2 \times 7^2$, we get that $c_2 \equiv \dfrac{-2}{6} \mod 7 \equiv 2 \mod 7$ and thus $3 + 1 \times 7 + 2 \times 7^2 = 108 \equiv \sqrt{2} \mod 7$. In this particular example, we see that $b_n = b_{n-1} + f(b_{n-1})$. Thus we can easily iterate this process and calculate the expansion of $\sqrt{2}$ to arbitrary accuracy.

Of course not all integers are quadratic residues $\mod p$, so not all will have square roots in $\mathbb{Z}_p$. Due to Gauss, we have -1 is a quadratic residue $\mod p$ if and only if $p \not\equiv 3 \mod 4$. Thus in particular there is no square root of -1 in $\mathbb{Q}_7$. This isn't too much of a problem however, as we can simply consider the extension field $\mathbb{Q}_7(\sqrt{-1}) = \{a + b\sqrt{-1} : a, b \in \mathbb{Q}_7\}$.

1.3 p-Adic Fields

In general, as $\mathbb{Q}_p$ has characteristic 0, it follows that if K is a finite degree field extension of $\mathbb{Q}_p$ then by the primitive element theorem $K = \mathbb{Q}_p(\alpha)$ for some element $\alpha \in K$. These finite field extensions have many of the properties that $\mathbb{Q}_p$ has and are an object of intense study, motivating the following definition.

Definition 1.3.1. We say that a field K is a p-adic field if K is a finite extension of $\mathbb{Q}_p$.

Since any finite degree field extension is an algebraic field extension, it follows that for an $\alpha \in K$ there is a monic, irreducible polynomial $f_\alpha(x) \in \mathbb{Q}_p[x]$ such that $f_\alpha(\alpha) = 0$. We call $f_\alpha(x)$ the minimal polynomial of α over $\mathbb{Q}_p$. This fact in turn motivates the natural extension of $\mathbb{Z}_p$.

Definition 1.3.2. Let K be a p-adic field. Define the ring of integers $O_K = \{\alpha \in K : f_\alpha(x) \in \mathbb{Z}_p[x]\}$.

The majority of $\mathbb{Q}_p$'s interesting properties arise from its non-Archimedean absolute value $|\cdot|_p$. In order to show that an arbitrary p-adic field K inherits these interesting properties, we will construct a non-Archimedean absolute value $|\cdot|_K : K \to \mathbb{R}$. In order to construct this non-Archimedean absolute value, we need a couple of useful lemmas.

Lemma 1.3.3. *Let $A \in M_n(\mathbb{Z}_p)$, and denote its image in $M_n(\mathbb{Z}_p/p\mathbb{Z}_p) \cong M_n(\mathbb{F}_p)$ by $\overline{A}$. Then the system of linear equations $Ax = y$ is has a solution $x \in \mathbb{Z}_p^n$ for every $y \in \mathbb{Z}_p^n$ if and only $\overline{A}\overline{x} = \overline{y}$ has a solution $\overline{x} \in (\mathbb{Z}_p/p\mathbb{Z}_p)^n \cong \mathbb{F}_p^n$ for every $\overline{y} \in (\mathbb{Z}_p/p\mathbb{Z}_p)^n \cong \mathbb{F}_p^n$.*

Proof. Given $A \in M_N(\mathbb{Z}_p)$, we have that A has a multiplicative inverse in $M_n(\mathbb{Z}_p)$ if and only if $\det(A)$ is a unit of $\mathbb{Z}_p$. Thus the system of equations $Ax = y$ has a solution for every y if and only if $|\det(A)|_p = 1$. Similarly, the system of equations $\overline{A}\overline{x} = \overline{y}$ is solvable for every $\overline{y}$ if and only if $\det(\overline{A}) \neq 0$. As $\det(A) \equiv \det(\overline{A}) \mod p$, and $\det(A) \not\equiv 0 \mod p$ if and only if $|\det(A)|_p = 1$, we're done. □

Using this lemma, we can now prove a version of Hensel's Lemma for polynomials. For any polynomial $f(x) \in \mathbb{Z}_p[x]$, we denote it's image in $\mathbb{Z}_p/p\mathbb{Z}_p[x] \cong \mathbb{F}_p[x]$ by $\overline{f}(x)$. Then

Theorem 1.3.4. *(Hensel's Lemma for Polynomials): Let $f(x) \in \mathbb{Z}_p[x]$ be a non-constant polynomial such that its image $\overline{f}(x)$ splits in $\mathbb{F}_p[x]$ as $\overline{f}(x) = \overline{g}_0(x)\overline{h}_0(x)$ for some relatively prime $\overline{g}_0(x), \overline{h}_0(x)$ in $\mathbb{F}_p[x]$. Then there exist $g(x), h(x) \in \mathbb{Z}_p[x]$ such that $\overline{g}(x) = \overline{g}_0(x)$, $\overline{h}(x) = \overline{h}_0(x)$, $\deg(g) = \deg(\overline{g}_0)$, and*

$$f(x) = g(x)h(x).$$

Proof. By assumption we have that $\overline{f}(x) \neq 0$, as the product of any two relatively prime polynomials in $\mathbb{F}_p[x]$ is nonzero. Now, let $\overline{g}_0, \overline{h}_0$ be as stated in the theorem, and $g_0(x), h_0(x) \in \mathbb{Z}_p[x]$ be such that there images in $\mathbb{F}_p[x]$ are $\overline{g}_0, \overline{h}_0$ and with $\deg(g_0) = \deg(\overline{g}_0)$, $\deg(h_0) = \deg(\overline{h}_0)$. Then we must have that $d = \deg(f) \geq \deg(\overline{f}) = \deg(\overline{g}_0\overline{h}_0) = \deg(g_0h_0)$.

We inductively take $g_k, h_k \in \mathbb{Z}_p[x]$ such that $\deg(g_k) < \deg(g_0), \deg(h_k) \leq d - \deg(g_0)$, and

$$g_k(x)h_0(x) + h_k(x)g_0(x) = c_k(x)$$

where $c_1(x) = p^{-1}(f(x) - g_0(x)h_0(x))$ and $c_k(x) = -\sum_{0<i<k} g_i(x)h_{k-i}(x)$ for $k > 1$. Assuming such g_i, h_i exist, by taking $g(x) = \sum_{i=0}^{\infty} p^i g_i(x)$ and $h(x) = \sum_{i=0}^{\infty} p^i h_i(x)$ we get that

$$\begin{aligned} g(x)h(x) &= \left(\sum_{i=0}^{\infty} p^i g_i(x)\right)\left(\sum_{i=0}^{\infty} p^i h_i(x)\right) = \sum_{k=0}^{\infty} p^k \sum_{i=0}^{k} g_i(x)h_{k-i}(x) \\ &= g_0(x)h_0(x) + \sum_{k=1}^{\infty} p^k \left(g_k(x)h_0(x) + h_k(x)g_0(x) + \sum_{0<i<k} g_i(x)h_{k-i}(x)\right) \\ &= g_0(x)h_0(x) + \sum_{k=1}^{\infty} p^k \left(c_k(x) + \sum_{0<i<k} g_i(x)h_{k-i}(x)\right) \\ &= g_0(x)h_0(x) + pc_1(x) = f(x). \end{aligned}$$

As $\deg(g_i) < \deg(g_0)$ for every $i \geq 1$, we have that $\deg(g) = \deg(g_0) = \deg(\overline{g}_0)$. Thus as by construction $\overline{g} = \overline{g}_0, \overline{h} = \overline{h}_0$, if we can show that $g_i(x), h_i(x)$ exist for every i then we're done. It suffices to show that for any $c(x) \in \mathbb{Z}_p[x]$ with $\deg(c) \leq d$, we can find $a(x), b(x) \in \mathbb{Z}_p[x]$ such that

$$\deg(a) < \deg(g_0), \quad \deg(b) \leq d - \deg(g_0), \quad a(x)h_0(x) + b(x)g_0(x) = c(x).$$

As $\overline{g}_0, \overline{h}_0$ are relatively prime in $\mathbb{F}_p[x]$, we have that there are $\overline{a}(x), \overline{b}(x) \in \mathbb{F}_p[x]$ such that

$$\overline{a}(x)\overline{h}_0(x) + \overline{b}(x)\overline{g}_0(x) = \overline{c}(x).$$

By the division algorithm, we can assume that $\deg(\overline{a}) < \deg(\overline{g}_0) = \deg(g_0)$. Then as $\deg(\overline{c}) \leq d$, we must have $\deg(\overline{b}) \leq d - \deg(\overline{g}_0)$. Thus this system of linear equations is always solvable $\mod p$. Applying the previous lemma with the vector x being the $d+1$ coefficients of $a(x), b(x)$ and the vector y being the $d+1$

coefficients of $c(x)$, we then have that there are $a(x), b(x) \in \mathbb{Z}_p[x]$ with

$$\deg(a) < \deg(g_0), \quad \deg(b) \leq d - \deg(g_0), \quad a(x)h_0(x) + b(x)g_0(x) = c(x).$$

□

Corollary 1.3.5. *Let $f_0(x) \in \mathbb{Q}_p[x]$ be a monic, irreducible polynomial with $f_0(0) \in \mathbb{Z}_p$. Then $f_0(x) \in \mathbb{Z}_p[x]$.*

Proof. Let $d = \deg(f_0)$, and assume that $f_0(x) \notin \mathbb{Z}_p[x]$. Let e be the smallest integer such that $f(x) = p^e f_0(x)$ is in $\mathbb{Z}_p[x]$. As e is positive, the leading coefficient of f is p^e. By the minimality of e we must have that the coefficient of x^r is a unit of $\mathbb{Z}_p$ for some $0 < r < d$, and thus $0 < \deg(\overline{f}) < d$. Applying Hensel's Lemma with $\overline{g}_0 = \overline{f}$ and $\overline{h}_0 = 1$, we then have that there are $g(x), h(x) \in \mathbb{Z}_p[x]$ with $0 < \deg(g) < d$ and $f(x) = g(x)h(x)$. Thus we must have $\deg(h) > 0$, so f is reducible in $\mathbb{Q}_p[x]$ and hence f_0 is reducible in $\mathbb{Q}_p[x]$, a contradiction. Thus $f_0(x) \in \mathbb{Z}_p[x]$. □

With that corollary done, we can now prove that K has a non-Archimedean absolute value.

Theorem 1.3.6. *Let K be a p-adic field. Then there is a non-Archimedean absolute value $|\cdot|_K : K \to \mathbb{R}$ satisfying $|a|_K = |a|_p^n$ for every $a \in \mathbb{Q}_p$, where $n = [K : \mathbb{Q}_p]$*

Proof. We first construct our candidate function $|\cdot|_K$ and then show it satisfies the necessary properties. As K is a finite extension of degree $[K : \mathbb{Q}_p] = n$, we have that K is an n-dimensional $\mathbb{Q}_p$-vector space. Thus fix some $\mathbb{Q}_p$ basis $u_1, \ldots, u_n$ of K, and define the $\mathbb{Q}_p$-algebra homomorphism $\rho : K \to M_n(\mathbb{Q}_p)$ by $\rho(\alpha) = [a_{i,j}]_{i,j=1}^n$, where $\alpha u_j = \sum_{i=1}^{n} a_{i,j} u_i$ with $a_{i,j} \in \mathbb{Q}_p$ for $i, j = 1, \ldots, n$. Then define the norm $N : K \to \mathbb{Q}_p$ by $N(\alpha) = \det(\rho(\alpha))$. Note that N is independent of our choice of basis, as for any invertible matrix $S \in GL_n(\mathbb{Q}_p)$ (the set of $n \times n$ invertible matrices with coefficients in $\mathbb{Q}_p$), we have that $\det(S\rho(\alpha)S^{-1}) = \det(\rho(\alpha)) = N(\alpha)$.

Now to calculate the norm of α; as K is an algebraic extension, we have that α has a minimal polynomial $f_\alpha(x) \in \mathbb{Q}_p[x]$, with $\deg(f_\alpha) = d$. Then $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ forms a $\mathbb{Q}_p$ basis for $\mathbb{Q}_p(\alpha)$. With respect to this basis, the matrix corresponding to α is just the companion matrix of $f_\alpha(x)$,

$$C(f_\alpha) = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{d-1} \end{bmatrix}$$

where $f_\alpha(x) = \sum_{i=0}^{d} a_i x^i$. Thus from basic linear algebra, we have that $\det(C(f_\alpha)) = (-1)^d f_\alpha(0)$. Now let $v_1, v_2, \ldots, v_e$ be a $\mathbb{Q}_p(\alpha)$-basis for K. Then we must have $n = de$ and

$$v_1, \alpha v_1, \ldots, \alpha^{d-1} v_1, v_2, \alpha v_2, \ldots, \alpha^{d-1} v_2, \ldots, v_e, \alpha v_e, \ldots, \alpha^{d-1} v_e$$

is a $\mathbb{Q}_p$ basis for K. In the basis, we have that

$$\rho(\alpha) = \begin{bmatrix} C(f_\alpha) & 0 & 0 & \ldots & 0 \\ 0 & C(f_\alpha) & 0 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \ldots & & 0 & C(f_\alpha) \end{bmatrix}$$

is block diagonal with e copies of $C(f_\alpha)$ along the diagonal. Thus $N(\alpha) = \det(C(f_\alpha))^e = (-1)^n f_\alpha(0)^e$. Finally, we now define $|\cdot|_K : K \to \mathbb{R}$ by

$$|\alpha|_K = |N(\alpha)|_p = |f_\alpha(0)|_p^e.$$

Then as for any $a \in \mathbb{Q}_p$, we have that $f_a(x) = x - a$ and thus $|a|_K = |a|_p^n$. Now, as the range of $|\cdot|_K$ is a subset of the range of $|\cdot|_p$, we have that $|\alpha|_K \geq 0$ for every $\alpha \in K$. Furthermore, $|\alpha|_K = 0$ implies $|f_\alpha(0)|_p^e = 0$, and thus $f_\alpha(0) = 0$. Thus $\alpha = 0$, so $|\cdot|_K$ is positive definite. As ρ is a $\mathbb{Q}_p$-algebra homomorphism, we also have that for any $\alpha, \beta \in K$ that $\rho(\alpha\beta) = \rho(\alpha)\rho(\beta)$. Thus by the multiplicative properties of the determinant and $|\cdot|_p$, we get that

$$|\alpha\beta|_K = |N(\rho(\alpha\beta))|_p = |N(\rho(\alpha))|_p |N(\rho(\beta))|_p = |\alpha|_K |\beta|_K.$$

Finally, we need to prove that $|\cdot|_K$ obeys the strong triangle inequality, $|\alpha + \beta|_K \leq \max\{|\alpha|_K, |\beta|_K\}$. As we have already shown that $|\cdot|_K$ is multiplicative, this is equivalent to proving that $|\alpha + 1|_K \leq 1$ whenever $|\alpha|_K \leq 1$. As $|\alpha|_K = |f_\alpha(0)|_p^e \leq 1$, we have that $|f_\alpha(0)|_p \leq 1$. Thus $f_\alpha(0) \in \mathbb{Z}_p[x]$, and as f_α is monic and irreducible, by the previous corollary we thus have that $f_\alpha(x) \in \mathbb{Z}_p[x]$. Thus $f_{\alpha+1}(x) = f_\alpha(x-1) \in \mathbb{Z}_p[x]$, so $|\alpha + 1|_K = |f_{\alpha+1}(0)|_p^e \leq 1$. Thus $|\cdot|_K$ obeys the strong triangle inequality, and thus $|\cdot|_K$ is a non-Archimedean absolute value on K.

□

As K has a non-Archimedean absolute value, we immediately get that K is a

totally disconnected, topological field by Propositions 1.1.1 and 1.1.3. One somewhat surprising fact is that the topology on K induced by $|\cdot|_K$ is the same as the product topology on $\mathbb{Q}_p^n$, where $n = [K : \mathbb{Q}_p]$. More precisely,

Proposition 1.3.7. *Let K be a p-adic field, and $n = [K : \mathbb{Q}_p]$. Then K is homeomorphic to $\mathbb{Q}_p^n$.*

Proof. Let $u_1, u_2, \ldots, u_n$ be some fixed $\mathbb{Q}_p$-basis for K. We show that a sequence $([a_{i,j}]_{j=1}^n)_{i=1}^\infty$ converges in $\mathbb{Q}_p^n$ if and only if $(\sum_{j=1}^n a_{i,j}u_j)_{i=1}^\infty$ converges in K. So, suppose $[a_{i,j}]_{j=1}^n \to [a_j]_{j=1}^n \in \mathbb{Q}_p$, and let $M = \max\{|u_j|_K\}$. Then for any $[b_j]_{j=1}^n \in \mathbb{Q}_p$, we have that $|b_1u_1 + b_2u_2 + \ldots + b_nu_n|_p \leq \max\{|b_ju_j|_K\} = \max\{|b_j|_p^n|u_j|_K\} \leq M\max\{|b_j|_p^n\}$. Thus for any $\epsilon > 0$, let $N \in \mathbb{N}$ be such that $m > N$ implies $\max\{|a_{m,j} - a_j|_p\} < \left(\frac{\epsilon}{M}\right)^{1/n}$. Then for all $m > N$, we have that

$$|\sum_{j=1}^n a_{m,j}u_j - \sum_{j=1}^n a_ju_j|_K = |\sum_{j=1}^n (a_{m,j} - a_j)u_j|_K \leq M\max\{|a_{m,j} - a_j|_p^n\} < \epsilon,$$

so $\sum_{j=1}^n a_{i,j}u_j \to \sum_{j=1}^n a_ju_j$.

Now we suppose $\sum_{j=1}^n a_{i,j}u_j \to \sum_{j=1}^n a_ju_j \in K$, and show that $[a_{i,j}]_{j=1}^n \to [a_j]_{j=1}^n$. We prove this by induction. Suppose for all $j \neq 1$, $a_{i,j} = 0$ for all i. As $|\cdot|_K$ defines a $\mathbb{Q}_p$-vector norm on K, we have the span$\{u_1\}$ is closed. Then as $a_{i,1}u_1 = \sum_{j=1}^n a_{i,j}u_j \to \sum_{j=1}^n a_ju_j$, we have that $\sum_{j=1}^n a_ju_j \in$span$\{u_1\}$, and thus $a_j = 0$ for $j > 1$. Thus $a_{i,1}u_1 \to a_1u_1$, and as $|a_{i,1}u_1 - a_1u_1|_k = |a_{i,1} - a_1|_p^n|u_1|_K \to 0$, we have that $a_{i,1} \to a_1$. Thus $[a_{i,j}]_{j=1}^n \to [a_j]_{j=1}^n$ in $\mathbb{Q}_p^n$.

Now suppose that for some integer $1 < k \leq n$, we have that $\sum_{j=1}^{k-1} b_{i,j}u_j \to \sum_{j=1}^n b_ju_j$ implies $[b_{i,j}]_{j=1}^n \to [b_j]_{j=1}^n$, where $b_{i,j} = 0$ for $j \geq k$. Then let $\sum_{j=1}^k a_{i,j}u_j$ be such that $\sum_{j=1}^k a_{i,j}u_j \to \sum_{j=1}^n a_ju_j$. As $|\cdot|_K$ is a $\mathbb{Q}_p$ vector norm, we get that span$\{u_1, u_2, \ldots, u_k\}$ is closed. Thus $a_j = 0$ for $j > k$. Suppose that $[a_{i,j}]_{j=1}^n$ does not converge to $[a_j]_{j=1}^n$ (where $a_{i,j} = 0$ for $j > k$). Then we must have that $a_{i,j}$ does not converge to a_j for some $1 \leq j \leq k$; after reindexing, we can without loss of generality assume that $a_{i,k}$ does not converge to a_k. Then by passing to a subsequence, we can assume without loss of generality that there is an $\delta > 0$ such that $|a_{i,k} - a_k|_p > \delta$ for all i. Let $\alpha_i = \sum_{j=1}^k (a_{i,j} - a_j)u_j$. Then as $\left|\frac{\alpha_i}{a_{i,k} - a_k}\right|_K \leq \frac{1}{\delta^n}|\alpha_i|_K \to 0$, we have

that $\sum_{i=1}^{k} \frac{a_{i,j}-a_j}{a_{i,k}-a_k} u_j = u_k + \sum_{i=1}^{k-1} \frac{a_{i,j}-a_j}{a_{i,k}-a_k} u_j \to 0$. As u_k is constant, we thus have that $\sum_{i=1}^{k-1} \frac{a_{i,j}-a_j}{a_{i,k}-a_k} u_j$ is convergent, and thus $\sum_{i=1}^{k-1} \frac{a_{i,j}-a_j}{a_{i,k}-a_k} u_j \to \sum_{j=1}^{k-1} b_j u_j$, for some $b_j \in \mathbb{Q}_p$. But $\sum_{i=1}^{k-1} \frac{a_{i,j}-a_j}{a_{i,k}-a_k} u_j \to -u_k$, so $b_1u_1 + b_2u_2 + \ldots + b_{k-1}u_{k-1} + u_k = 0$. As u_j are linearly independent, we have a contradiction. Thus $[a_{i,j}]_{j=1}^n \to [a_j]_{j=1}^n$, and thus K is homeomorphic to $\mathbb{Q}_p^n$.

□

Corollary 1.3.8. *Let K be a p-adic field. Then K is locally compact, and thus complete.*

Proof. As $\mathbb{Z}_p$ is a compact subset of $\mathbb{Q}_p$, we have that for any $a = [a_j]_{j=1}^n \in \mathbb{Q}_p$ that $\prod_{i=1}^{n}(a_i + \mathbb{Z}_p)$ is a compact neighborhood of a. Thus $\mathbb{Q}_p^n$ is locally compact. As K is homeomorphic to $\mathbb{Q}_p^n$, we then have that K is locally compact. As any locally compact metric space is complete, we then have that K is complete. □

As in the case of the p-adic numbers, the ring of integers O_K is typically more important than the field K itself. Recall $O_K = \{\alpha \in K : f_\alpha(x) \in \mathbb{Z}_p[x]\}$. Using $|\cdot|_K$, we can get a number of useful properties of O_K.

Theorem 1.3.9.

1. *The ring of integers $O_K = \{x \in K : |x|_K \leq 1\}$.*
2. *O_K is a subring of K with unique maximal ideal $\pi_K O_K = \{x\pi_K : x \in O_K\} = \{x \in O_K : |x|_K < 1\}$ for some $\pi_K \in O_K$. Furthermore, for any $x \in K, |x|_K = |\pi_K|_K^m$ for some integer $m \in \mathbb{Z}$.*
3. *The residue field of O_K, $O_K/\pi_K O_K$, is isomorphic to the finite field with q elements $\mathbb{F}_q$, where $q = p^r$ for some integer $1 \leq r \leq n = [K : \mathbb{Q}_p]$.*
4. *Let $S \subset O_K$ be a system of representatives of $O_K/\pi_K O_K$, i.e., a subset such that $0 \in S$, card(S) = card($O_K/\pi_K O_K$) = q, and $\{s + \pi_K O_K : s \in S\} = O_K/\pi_K O_K$. Then every element $x \in K$ can be written uniquely in the form $x = \sum_{i=m}^{\infty} a_i \pi_K^i$, where $m \in \mathbb{Z}$, $a_i \in S$ for all i, and $a_m \neq 0$. Conversely, every such series converges in K with $\sum_{i=m}^{\infty} a_i \pi_K^i = |\pi_K|_K^m$.*

5. *O_K is a compact open set.*

6. *$[K : \mathbb{Q}_p] = re$, where $r = [O_K/\pi_K O_K : \mathbb{F}_p]$ and $e \in \mathbb{N}$ is such that $\pi_K^e O_K = pO_K$. Furthermore, $|\pi_K|_K = p^{-r} = q^{-1}$ and thus for any $x \in K$, $|x|_K = q^{-m}$ for some integer m.*

Proof. 1. Suppose $\alpha \in O_K$. Then by the definition of O_K, we have that $f_\alpha(x) \in \mathbb{Z}_p[x]$. Thus $f_\alpha(0) \in \mathbb{Z}_p$, so $|\alpha|_K = |f_\alpha(0)|_p^e \leq 1$, so $O_K \subseteq \{x \in K : |x|_K \leq 1\}$. Now let $\alpha \in K$ be such that $|\alpha|_K \leq 1$. Then necessarily $|f_\alpha(0)|_p \leq 1$, so $f_\alpha(0) \in \mathbb{Z}_p$. As $f_\alpha(x)$ is a monic, irreducible polynomial, we thus have that $f_\alpha(x) \in \mathbb{Z}_p[x]$, so $\alpha \in O_K$. Thus $O_K = \{x \in K : |x|_K \leq 1\}$.

2. $\mathbb{Z}_p \subseteq O_K$, so O_K is nonempty. As $|\cdot|_K$ is a non-Archimedean norm, we have that for any $x, y \in O_K$ that $|x - y|_K \leq \max\{|x|_K, |y|_K\} \leq 1$ and $|xy|_K = |x|_K|y|_K \leq 1$. Thus $x - y, xy \in O_K$, so O_K is a subring of K.

   By the same reasoning as in Theorem 1.2.4 (4.), we have that x is a unit of O_K if and only if $|x|_K = 1$. Thus any proper ideal I of O_K necessarily has $I \subseteq O_K \setminus \{x : |x|_K = 1\} = \{x \in O_K : |x|_K < 1\}$. As the set of non-units $\{x \in O_K : |x|_K < 1\}$ is an ideal of O_K (again, by the same reasoning as in theorem 1.2.4), we have that it is the unique maximal ideal.

   As the range of nonzero values $|\cdot|_K$ takes is a discrete set, we have that there is some element $\pi_K \in O_K$ such that $|\pi_K|_K = \max\{|x|_K : |x|_K < 1\}$, and thus $\pi_K O_K = \{x\pi_K : x \in O_K\} = \{x \in O_K : |x|_K < 1\}$. As the range of nonzero values $|\cdot|_K$ takes is a discrete subgroup of $\mathbb{R}_+^\times$, it is a cyclic subgroup and thus we have that it is generated by $|\pi_K|_K$. Thus as $|\pi_K|_K^m = |\pi_K^m|_K$, we then have that for any $x \in K$, $|x|_K = |\pi_K^m|_K$ for some integer $m \in \mathbb{Z}$.

3. As $\pi_K O_K$ is a maximal ideal of O_K, we have that $O_K/\pi_K O_K$ is a field. As $|p|_K = |p|_p^n < 1$, we have that $p + \pi_K O_K = 0 + \pi_K O_K$, so $\mathrm{char}(O_K/\pi_K O_K) = p$. Thus $O_K/\pi_K O_K$ contains $\mathbb{F}_p$ as a subfield, so $O_K/\pi_K O_K$ is an $\mathbb{F}_p$ vector space. We now show that it is a finite dimensional $\mathbb{F}_p$ vector space by proving $n = [K : \mathbb{Q}_p] \geq [O_K/\pi_K O_K : \mathbb{F}_p]$, thus forcing $O_K/\pi_K O_K$ to be a finite field of characteristic p. Hence, we get $O_K/\pi_K O_K \cong \mathbb{F}_q$, the finite field with q elements where $q = p^r$ for some integer $1 \leq r \leq n$.

   Now let $w_1, w_2, \ldots, w_m \in O_K$. If $w_1, \ldots, w_m$ are linearly dependent over $\mathbb{Q}_p$, then there is a nontrivial linear combination $a_1 w_1 + a_2 w_2 + \ldots + a_n w_n = 0$ for some $a_i \in \mathbb{Q}_p$ not all equal to 0. By scaling both sides of this equation by an appropriate power of p, we can assume that $a_i \in \mathbb{Z}_p$ for all i and $a_j \in \mathbb{Z}_p^\times$

for some $j \in \{1, \ldots, m\}$. Then as $0 = \sum_{i=1}^{m} a_i w_i$ in O_K, we have that

$$\begin{aligned} 0 + \pi_K O_K &= \left(\sum_{i=1}^{m} a_i w_i \right) + \pi_K O_K = \sum_{i=1}^{m} (a_i w_i + \pi_K O_K) \\ &= \sum_{i=1}^{m} a_i \cdot (w_i + \pi_K O_K) \end{aligned}$$

in $O_K/\pi_K O_K$, where we now consider $a_i \in \mathbb{F}_p$ by the canonical projection map $\rho : \mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. Then as $|a_j|_p = 1$ for some $j \in \{1, \ldots, m\}$, we have that not all a_i are zero in $\mathbb{F}_p$. Thus this is a nontrivial linear combination, so the set $\{w_1 + \pi_K O_K, w_2 + \pi_K O_K, \ldots, w_m + \pi_K O_K\}$ is linearly dependent in $O_K/\pi_K O_K$. Thus $n = [K : \mathbb{Q}_p] \geq [O_K/\pi_K O_K : \mathbb{F}_p]$, so $O_K/\pi_K O_K$ is a finite extension of $\mathbb{F}_p$. Thus $O_K/\pi_K O_K \cong \mathbb{F}_q$, the finite field with q elements, with $q = p^r$ for some integer $1 \leq r \leq n$.

4. Let $S \subset O_K$ be a fixed system of representatives of $O_K/\pi_K O_K$. As $0 = 0 + 0\pi_k + 0\pi_K^2 + \ldots$, it suffices to show that for any x with $|x|_K = 1$, that $x = \sum_{i=0}^{\infty} a_i \pi_K^i$ with $a_i \in S$ and $a_0 \neq 0$. Else, $|\pi_K^{-m} x|_K = 1$ for some $m \in \mathbb{Z}$, so $\pi_K^{-m} x = \sum_{i=0}^{\infty} a_i \pi_K^i$ implies $x = \sum_{i=m}^{\infty} a_{i-m} \pi_K^i$.

   Now, $|x|_K = 1$ implies $x \notin \pi_K O_K$. As S is a system of representatives, we have that $x + \pi_K O_K = a_0 + \pi_K O_K$ for some $a_0 \in S$ with $a_0 \neq 0$ as $x \notin \pi_K O_K$. Thus $(x - a_0) + \pi_K O_K = 0 + \pi_K O_K$, so $x - a_0 \in \pi_K O_K$. Now assume that $a_0, a_1, \ldots, a_{n-1} \in S$ are such that $x - \sum_{i=0}^{n-1} a_i \pi_K^i \in \pi_K^n O_K$. Then as the map $y + \pi_K O_K \to y\pi_K^n + \pi_K^{n+1} O_K$ is an isomorphism of abelian groups, we have that there is some $a_n \in S$ such that $\left(x - \sum_{i=0}^{n-1} a_i \pi_K^i \right) + \pi_K^{n+1} O_K = a_n \pi_K^n + \pi_K^{n+1} O_K$. Thus $x - \sum_{i=0}^{n} a_i \pi_k^i \in \pi_K^{n+1} O_K$. Thus by induction, we have that there are $a_i \in S$ for all $i \geq 0$ such that for any $N \in \mathbb{N}$, $x - \sum_{i=0}^{N} a_i \pi_K^i \in \pi_K^{N+1} O_K$. Thus $\lim_{N \to \infty} |x - \sum_{i=0}^{N} a_i \pi_K^i|_K \leq \lim_{N \to \infty} |\pi_K^{N+1}|_K = \lim_{N \to \infty} |\pi_K|_K^{N+1} = 0$. Thus $x =$

$\sum_{i=0}^{\infty} a_i \pi_K^i$.

Now consider the infinite series $\sum_{i=m}^{\infty} a_i \pi_K^i$, where $a_i \in S$ and $a_m \neq 0$. For any integers $N \geq m$ and $j \in \mathbb{N}$, we have that $|\sum_{i=m}^{N+j} a_i \pi_K^i - \sum_{i=m}^{N} a_i \pi_K^i|_K = |\sum_{i=N+1}^{N+j} a_i \pi_K^i|_K \leq |\pi_K|_K^{N+1} \to 0$ as $N \to \infty$. Thus as K is complete, we have that $\sum_{i=m}^{\infty} a_i \pi_K^i \in K$. Finally, by continuity we have that $|\sum_{i=m}^{\infty} a_i \pi_K^i|_K = \lim_{N\to\infty} |\sum_{i=m}^{N} a_i \pi_K^i|_K = \lim_{N\to\infty} |\pi_K|_K^m = |\pi_K|_K^m$.

Finally, for uniqueness suppose $x = \sum_{i=m}^{\infty} a_i \pi_K^i = \sum_{i=k}^{\infty} b_i \pi_K^i$ with $a_i, b_i \in S$ for all i and $a_m, b_k \neq 0$. Then we must have $|x|_K = |\pi_K^m|_K = |\pi_K^k|_K$, so $m = k$. Assume that $a_i \neq b_i$ for some $i \geq m$. Let N be such that $a_i = b_i$ for all $i < N$, and $a_N \neq b_N$. Then

$$|\sum_{i=m}^{\infty} a_i \pi_K^i - \sum_{i=m}^{\infty} b_i \pi_K^i|_K = |(a_N - b_N)\pi_K^N + \sum_{i=N+1}^{\infty} (a_i - b_i)\pi_K^i|_K.$$

As $a_N \neq b_N$, and S is a system of representatives, we have that $a_N - b_N \notin \pi_K O_K$, so $|a_N - b_N|_K = 1$. Thus

$$|(a_i - b_i)\pi_K^i|_K \leq |\pi_K^i|_K < |\pi_K^N|_K = |(a_N - b_N)\pi_K^N|_K$$

for all $i > N$, so $|\sum_{i=m}^{\infty} a_i \pi_K^i - \sum_{i=m}^{\infty} b_i \pi_K^i|_K = |\pi_K^N|_K$. But $\sum_{i=m}^{\infty} a_i \pi_K^i = \sum_{i=k}^{\infty} b_i \pi_K^i = x$ so $|\sum_{i=m}^{\infty} a_i \pi_K^i - \sum_{i=m}^{\infty} b_i \pi_K^i|_K = |x - x|_K = 0$, a contradiction. Thus the expansion is unique.

5. As $O_K = \{x \in K : |x|_K \leq 1\}$, we have that O_K closed ball in an ultrametric space and thus is both open and closed. As K is complete and O_K is closed, we have that O_K is complete. Thus we just need to show that O_K is totally bounded to prove that O_K is compact. So, let $\epsilon > 0$, $N \in \mathbb{N}$ be such that

$|\pi_K^N|_K < \epsilon$, and $C_N = \{\sum_{i=0}^{N-1} a_i \pi_K^i : a_i \in S\}$ for some set of representatives S. Then $\{x + \pi_K^N O_K : x \in C_N\}$ is a finite collection of open balls of radius less than ϵ with $\bigcup_{x \in C} x + \pi_k^N O_K = O_K$. Thus O_K is compact.

6. Let $r = [O_K/\pi_K O_K : \mathbb{F}_p]$ and $e \in \mathbb{N}$ be such that $\pi_K^e O_K = pO_K$. Let $w_1, w_2, \ldots, w_r \in O_K$ be such that $\{w_i + \pi_K O_K\}$ is a $\mathbb{F}_p$ basis for $O_K/\pi_K O_K$. We prove that $re = n$ by showing that

$$\{w_i \pi_K^j : i = 1, \ldots, r, j = 0, \ldots, e-1\}$$

is a $\mathbb{Q}_p$ basis for K. Let $S = \{\sum_{i=1}^{r} c_i w_i : c_i \in \{0, \ldots, p-1\} \text{ for } i = 1, \ldots, r\}$ Then as $\{w_i + \pi_K O_K\}$ is a $\mathbb{F}_p$ basis for $O_K/\pi_K O_K$, we have that S is a system of representatives for $O_K/\pi_K O_K$. By part (4.), we have that for any $x \in O_K$, we can write x uniquely as $x = \sum_{i=0}^{\infty} a_i \pi_K^i$. As $\pi_K^e O_K = pO_K$, we could have by the same argument expanded x in terms of

$$1, \pi_K, \ldots, \pi_K^{e-1}, p, \pi_K p, \pi_K^2 p, \ldots, \pi_K^{e-1} p, p^2, \pi_K p^2, \ldots$$

Thus we can write x uniquely as

$$x = \sum_{j=0}^{e-1} \sum_{k=0}^{\infty} a_{j,k} \pi_K^j p^k$$

with $a_{j,k} \in S$. But $S = \{\sum_{i=1}^{r} c_i w_i : c_i \in \{0, \ldots, p-1\}\}$, so we can write x as

$$\begin{aligned} x &= \sum_{j=0}^{e-1} \sum_{k=0}^{\infty} \left(\sum_{i=1}^{r} c_{i,j,k} w_i \right) \pi_K^j p^k \\ &= \sum_{i=1}^{r} \sum_{j=0}^{e-1} \left(\sum_{k=0}^{\infty} c_{i,j,k} p^k \right) w_i \pi_K^j \\ &= \sum_{i=1}^{r} \sum_{j=0}^{e-1} b_{i,j} w_i \pi_K^j \end{aligned}$$

where $b_{i,j} = \sum_{k=0}^{\infty} c_{i,j,k} p^k \in \mathbb{Z}_p$. As the collection $\{b_{i,j}\}$ is uniquely determined by the collection $\{a_{j,k}\}$, it follows that our final expression is unique. Thus by scaling by an appropriate power of p, it follows that we can write any $x \in K$ uniquely as $x = \sum_{i=1}^{r} \sum_{j=0}^{e-1} b_{i,j} w_i \pi_K^j$ for some $b_{i,j} \in \mathbb{Q}_p$. Thus $\{w_i \pi_K^j : 1 \leq i \leq r, 0 \leq j \leq e-1\}$ is a basis for K, and thus $re = n$.

Finally, as $|\pi_K^e|_K = |p|_K = |p|_p^n = p^{-n}$, we have that $|\pi_K|_K = p^{-n/e} = p^{-r} = q^{-1}$. Thus for any $x \in K$, we have that $|x|_K = |\pi_K|_K^m = q^{-m}$ for some integer $m \in \mathbb{Z}$.

□

Remark: In the case that $e = 1$, we say the extension field K is unramified and else that it is ramified. The standard notation for the degree of the residue field $[O_K/\pi_K O_K]$ is f, but we elected to call this r in order to avoid confusing this with a polynomial $f(x)$.

Now with these theorems done, we've shown that any p-adic field has essentially all of the same properties that the p-adic numbers $\mathbb{Q}_p$ have. More precisely, we've shown that any p-adic field K is a complete, locally compact, totally disconnected, topological field with a non-Archimedean absolute value $|\cdot|_K$. K has a ring of integers $O_K = \{x \in K : |x|_K \leq 1\}$ which is compact, open subring of K. There is an element $\pi_K \in O_K$ such that $\pi_K O_K$ is the unique maximal ideal of O_K, and $O_K/\pi_K O_K \cong \mathbb{F}_q$, the finite field with q elements. Given a set of representatives $S \subset O_K$ of $O_K/\pi_K O_K$, we have that any element $x \in K$ can be written uniquely in the form $x = \sum_{i=m}^{\infty} a_i \pi_K^i$ with $m \in \mathbb{Z}$, $a_i \in S$ for all i, $a_m \neq 0$, and $|x|_K = |\pi_K^m|_K = q^{-m}$. With all of these properties now proven, we can now move on and construct the local zeta function $Z(f, s)$.

Chapter 2

Local Zeta Functions

2.1 Haar Measure

In order to define the local zeta function, we first need a translation invariant measure μ_K on a p-adic field K, known as the Haar measure on K. But in order to properly define the Haar measure, we first recall several basic definitions from measure theory.

Definition 2.1.1. Let X be a set, and $\mathcal{M}$ be a collection of subsets of X. We say that $\mathcal{M}$ is a σ-algebra, and the pair $(X, \mathcal{M})$ is a measurable space if

1. $X \in \mathcal{M}$
2. If $A \in \mathcal{M}$, then $X \setminus A \in \mathcal{M}$.
3. If $\{A_i : i \in \mathbb{N}\} \subseteq \mathcal{M}$, then $\bigcup_{i=1}^{\infty} A_i \in \mathcal{M}$

Given a subset $A \subseteq X$, we say that A is measurable if $A \in \mathcal{M}$ and that A is nonmeasurable otherwise.

As $X \setminus X = \emptyset$, it follows that if $\mathcal{M}$ is σ-algebra then $\emptyset \in \mathcal{M}$. Similarly, as $\bigcap_{i=1}^{\infty} A_i = X \setminus \bigcup_{i=1}^{\infty} (X \setminus A_i)$, we also have that any σ-algebra is closed under countable intersections as well. Finally, we get that $\mathcal{M}$ is closed under finite unions and intersections by taking $A_i = \emptyset$ or X respectively for all but finitely many i.

Definition 2.1.2. Let $(X, \mathcal{M})$ be a measurable space. Then a measure μ on $(X, \mathcal{M})$ is a countably additive function $\mu : \mathcal{M} \to [0, \infty]$. That is, for any $\{A_i : i \in \mathbb{N}\} \subseteq \mathcal{M}$ with $A_i \cap A_j = \emptyset$ for $i \neq j$, we have $\mu(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \mu(A_i)$. We call the triple $(X, \mathcal{M}, \mu)$ a measure space.

So, for any measurable set $A \in \mathcal{M}$, a measure μ assigns some nonnegative, possibly infinite value $\mu(A)$ to it which represents "the size" of A. In order for this measure to fit with our intuitive notion of size, we would like it to have nice regulatory properties.

Definition 2.1.3. We say that a measure space $(X, \mathcal{M}, \mu)$ is complete if for any measurable set $Z \in \mathcal{M}$ with $\mu(Z) = 0$ and subset $E \subseteq Z$ is measurable.

Similarly to how we define the completion of a metric space, we can define the completion of a measure space by adding in subsets of measure 0 sets. Formally,

Definition 2.1.4. Let $(X, \mathcal{M}, \mu)$ be a measure space. We say that two sets $A, B \subseteq X$ are μ-equivalent if $A \triangle B = (A \setminus B) \cup (B \setminus A) \subseteq Z$, for some measurable set $Z \in \mathcal{M}$ with $\mu(Z) = 0$.

Proposition 2.1.5. *Let $(X, \mathcal{M}, \mu)$ be a (possibly incomplete) measure space, and let*

$$\mathcal{M}' = \{A' \subseteq X : A' \text{ is } \mu - \text{equivalent to some } A \in \mathcal{M}\}$$

Extend μ to $\mathcal{M}'$ by taking $\mu(A') = \mu(A)$ if A' is μ-equivalent to $A \in \mathcal{M}$. Then $(X, \mathcal{M}', \mu)$ is a complete measure space, called the completion of $(X, \mathcal{M}, \mu)$.

See [4] for proof.

We need a bit more structure than an arbitrary notion of size for our purpose, so let's add some structure.

Definition 2.1.6. Let X be a topological space, and $\mathcal{T}$ be the collection of open sets of X. Then the Borel Sets $\mathcal{B}_X$ of X are the smallest σ-algebra of X containing $\mathcal{T}$. That is,

$$\mathcal{B}_X = \bigcap_{\mathcal{T} \subseteq \mathcal{A}} \mathcal{A},$$

where $\mathcal{A}$ are σ-algebras of X containing $\mathcal{T}$. We say that a measure μ is a Borel measure on X if it is defined on a σ-algebra $\mathcal{M}$ containing the Borel sets $\mathcal{B}_X$ of X.

It can easily be checked that an arbitrary intersection of σ-algebras of X is a σ-algebra of X. Thus as $\mathcal{T} \subseteq \mathcal{P}(X)$, the power set of X, and the power set is a σ-algebra, it follows that the Borel Sets exist for any topological space X.

If μ is a Borel measure on X, then we have that μ is defined for the open sets of X. It doesn't, however, impose any nice conditions on how the measure of those sets is calculated, which motivates more definitions.

Definition 2.1.7. Let X be a topological space, μ a Borel measure on X, and $E \in \mathcal{M}$ a measurable set. We say that μ is outer regular on E if

$$\mu(E) = \inf\{\mu(U) : E \subseteq U, U \text{ open } \}$$

and we say that μ is inner regular on E if

$$\mu(E) = \sup\{\mu(C) : C \subseteq E, C \text{ compact }\}.$$

The last piece of structure we need to add to our set X in order to define the Haar measure is a continuous group operation,

Definition 2.1.8. We say that X is an abelian topological group if X is an abelian group with the topology defined on it such that the maps

$$(x, y) \to x + y, \quad x \to -x$$

from $X \times X \to X$ and $X \to X$ are continuous. We say that a measure μ defined on a σ-algebra $\mathcal{M}$ of X is translation invariant if for any $A \in \mathcal{M}$ and $x \in X$, we have that

$$\mu(x + A) = \mu(A).$$

With all of these definitions in hand, we can finally define the Haar measure:

Theorem 2.1.9. *Let X be a locally compact, Hausdorff, abelian topological group. Then up to a positive scalar multiple, there is a unique, nontrivial, translation invariant measure μ on the Borel sets, called the Haar measure, such that μ is finite on all compact sets, outer regular on all Borel sets, and inner regular on all open sets.*

See [2] for proof of existence and uniqueness. For convenience, we always consider the Haar measure on the completion of $(X, \mathcal{B}_x, \mu)$. In the case of the real numbers $\mathbb{R}$, the Haar measure is just the normal Lebesgue measure, defined by $\mu([a, b]) = b - a$ on closed intervals, and then extended by regularity to all measurable subsets of $\mathbb{R}$. In the case of any group G with the discrete topology, the Haar measure is simply the counting measure, $\mu(A) =$card(A) for all $A \subseteq G$. But in this paper, we are interested in the case when our topological group K is a p-adic field.

Theorem 2.1.10. *Let K be a p-adic field with ring of integers O_K. Then there is a unique Haar measure μ_K defined on K such that $\mu_K(O_K) = 1$.*

Proof. As K has a non-Archimedean absolute value, by Proposition 1.1.1 we have that K is a topological field, and thus a topological group under addition. As K is a metric space we have that any two distinct points $x, y \in K$ have disjoint neighborhoods so K is necessarily Hausdorff, and by Corollary 1.3.8 we have that K is locally compact. Thus there is a Haar measure ν_K defined on K, which is unique up to a positive scalar multiple. By Theorem 1.3.9 (5.) we have that O_K is compact, and thus we must have that $\nu_K(O_K)$ is finite. If $\nu_K(O_K) > 0$, then

by taking $\mu_K(\cdot) = \dfrac{\nu_K(\cdot)}{\nu_K(O_K)}$, we have that μ_K is the unique Haar measure with $\mu_K(O_K) = 1$.

So suppose $\nu_K(O_K) = 0$, and let S be a system of representatives of $O_K/\pi_K O_K$. Let $A = \{\sum_{i=-\infty}^{-1} a_i \pi_K^i : a_i \in S, a_i = 0 \text{ for all but finitely many } i\}$. Then $\{x + O_K : x \in A\}$ is a countable collection of disjoint subsets of K, with $\bigcup_{x\in A}(x + O_K) = K$. Thus

$$\nu_K(K) = \nu_K(\bigcup_{x\in A} x + O_K) = \sum_{x\in A} \nu_K(x + O_K) = \sum_{x\in A} \nu_K(O_K) = 0$$

as $\nu_K(O_K) = 0$. But by definition of the Haar measure, ν_K is nontrivial and thus $\nu_K(K) \neq 0$, a contradiction. Thus $\nu_K(O_K) > 0$, and thus there is a unique Haar measure defined on K with $\mu_K(O_K) = 1$. □

For the rest of this thesis, let K be a fixed p-adic field with ring of integers O_K, residue field $O_K/\pi_K O_K \cong \mathbb{F}_q$ with fixed set of representatives S, and normalized Haar measure μ_K.

So we have that μ_K is uniquely defined with $\mu_K(O_K) = 1$. In order to explicitly calculate the measure of any other subset however, we need to be clever.

Proposition 2.1.11. *Let $m \in \mathbb{Z}$. Then $\mu_K(\pi_K^m O_K) = q^{-m}$, and $\mu_K(\pi_K^m O_K \setminus \pi_K^{m+1} O_K) = \dfrac{q-1}{q^{m+1}}$.*

Proof. As $\mu_K(O_K) = 1$, we have that the first statement is true for $m = 0$. For $m > 0$, let $A_m = \{\sum_{i=0}^{m-1} a_i \pi_K^i : a_i \in S\}$. Then we can write O_K as a disjoint union $O_K = \bigcup_{x\in A_m} (x + \pi_K^m O_K)$, so by additivity and translation invariance we get that

$$\begin{aligned}\mu_K(O_K) = \mu_K(\bigcup_{x\in A_m} (x + \pi_K^m O_K)) &= \sum_{x\in A_m} \mu_K(x + \pi_K^m O_K) \\ &= \sum_{x\in A_m} \mu_K(\pi_K^m O_K) = q^m \mu_K(\pi_K^m O_K).\end{aligned}$$

Thus as $\mu_K(O_K) = 1$, we get that $\mu_K(\pi_K^m O_K) = q^{-m}$ for all $m > 0$.

For $m < 0$, take $B_m = \{\sum_{i=m}^{-1} a_i \pi_K^i : a_i \in S\}$. Then we can represent $\pi_K^m O_K$ as a disjoint union of q^{-m} translates of O_K, $\pi_K^m O_K = \bigcup_{x\in B_m} (x + O_K)$. Thus by additivity

and translation invariance, $\mu_K(\pi_K^m O_K) = q^{-m}\mu_K(O_K) = q^{-m}$.

Finally, for any $m \in \mathbb{Z}$ we have that

$$\begin{aligned}\mu_K(\pi_K^m O_K \setminus \pi_K^{m+1} O_K) &= \mu_K(\pi_K^m O_K) - \mu_K(\pi_K^{m+1} O_K) = q^{-m} - q^{-(m+1)} \\ &= \frac{q-1}{q^{m+1}}.\end{aligned}$$

□

2.2 Local Zeta Functions

For the purposes of this paper, these are essentially the only cases we will need to consider. The main purpose of developing a measure is to be able to properly define the notion of an integral, so

Definition 2.2.1. Let $(X, \mathcal{M}, \mu)$ be a measure space. We say that a function $f : X \to \mathbb{C}$ is a simple function if

$$f(x) = \sum_{i=0}^{\infty} c_i \chi_{A_i}(x)$$

where $c_i \in \mathbb{C}$, $\chi_{A_i}(x) = \begin{cases} 1, & x \in A_i \\ 0, & x \notin A_i \end{cases}$ is the characteristic function of A_i, and $A_i \in \mathcal{M}$ is measurable for all i. For any measurable set $A \in \mathcal{M}$, we say that a simple function is μ-integrable on A if the series $\sum_{i=0}^{\infty} c_i \mu(A_i \cap A)$ is absolutely convergent. We then define the integral of f on A as

$$\int_A f(x) d\mu(x) = \sum_{i=0}^{\infty} c_i \mu(A_i \cap A).$$

Example: For some fixed $s \geq 0$, consider the function $|x|_K^s$. As $|x|_K^s = q^{-ms}$ if and only if $x \in \pi_K^m O_K \setminus \pi_K^{m+1} O_K$, we have that $|x|_K^s = \sum_{m=0}^{\infty} q^{-ms} \chi_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K}(x)$ for any $x \in O_K$. Thus

$$\begin{aligned}\int_{O_K} |x|_K^s d\mu_K(x) &= \sum_{m=0}^{\infty} q^{-ms} \mu_K(\pi_K^m O_K \setminus \pi_K^{m+1} O_K) = \sum_{m=0}^{\infty} \frac{q-1}{q^{m(s+1)+1}} \\ &= \frac{q-1}{q} \sum_{m=0}^{\infty} \left(q^{-(s+1)}\right)^m = \frac{q-1}{q} \frac{1}{1-q^{-(s+1)}} = \frac{q-1}{q-q^{-s}}.\end{aligned}$$

The above series is absolutely convergent for any $s > -1$, so in fact we can define the integral for any $s \in \mathbb{C}$ with $\Re(s) > -1$. In general, if $f(x) \in O_K[x]$, then $A_m = \{x \in O_K : |f(x)|_K^s = q^{-ms}\}$ is a closed set as $|f(x)|_K^s$ is a continuous function of x. Hence each A_m is measurable, $|f(x)|_K^s = \sum_{m=0}^{\infty} q^{-ms}\chi_{A_m}(x)$ for all $x \in O_K$. As $\sum_{m=0}^{\infty} |q^{-ms}|\mu_K(A_m) \leq \sum_{m=0}^{\infty} \mu_K(A_m) = 1$ whenever $\Re(s) \geq 0$, we have that the series $\sum_{m=0}^{\infty} q^{-ms}\mu_K(A_m)$ converges absolutely, and thus the integral of $|f(x)|_K^s$ is defined for all $s \in \mathbb{C}$ with $\Re(s) \geq 0$,

Definition 2.2.2. Let $f(x) \in O_K[x]$. Then we define the local zeta function of f as

$$Z(f,s) = \int_{O_K} |f(x)|_K^s d\mu_K(x)$$

for all $s \in \mathbb{C}$ with $\Re(s) \geq 0$.

Thus we showed that $Z(x,s) = \int_{O_K} |x|_K d\mu_K(x) = \dfrac{q-1}{q-q^{-s}}$. For another good illustrative example, consider

Example: Take $f(x) = (x-1)^2$. Then by definition,

$$Z(f,s) = \int_{O_K} |(x-1)^2|_K^s d\mu_K(x)$$

As for each $x \in O_K$ we have that $|(x-1)^2|_K^s = |x-1|_K^{2s}$, we then get that

$$\begin{aligned} Z(f,s) &= \int_{O_K} |x-1|_K^{2s} d\mu_K(x) = \sum_{m=0}^{\infty} q^{-2ms}\mu_K(\{x \in O_K : (x-1) \in \pi_K^m O_K \setminus \pi_K^{m+1} O_K\}) \\ &= \sum_{m=0}^{\infty} q^{-2ms}\mu_K(1 + \pi_K^m O_K \setminus \pi_K^{m+1} O_K). \end{aligned}$$

By the translation invariance of the Haar measure, we have that

$$\mu_K(1 + \pi_K^m O_K \setminus \pi_K^{m+1} O_K) = \mu_K(\pi_K^m O_K \setminus \pi_K^{m+1} O_K)$$

so

$$Z(f,s) = \sum_{m=0}^{\infty} q^{-2ms}\mu_K(1+\pi_K^m O_K \setminus \pi_K^{m+1}O_K) = \sum_{m=0}^{\infty} q^{-m(2s)}\mu_K(\pi_K^m O_K \setminus \pi_K^{m+1}O_K)$$
$$= \int_{O_K} |x|_K^{2s} d\mu_K(x) = Z(x,2s) = \frac{q-1}{q-q^{-2s}}.$$

By the same argument, one can show that for any $a \in O_K$ and integer $d \in \mathbb{N}$,

$$Z((x-a)^d, s) = Z(x, ds) = \frac{q-1}{q-q^{-ds}}$$

illustrating

Theorem 2.2.3. *Let X be a locally compact, Hausdorff, abelian topological group. Then up to positive scalar multiple, the Haar measure μ is uniquely characterized by the properties that any nonnegative, continuous function $f : X \to \mathbb{R}_+$ with compact support is μ-integrable on X, and for any integrable function ϕ on X and $y \in X$,*

$$\int_X \phi(x+y)d\mu(x) = \int_X \phi(x)d\mu(x).$$

Thus the translation invariance of the Haar measure implies the translation invariance of the integral. See [2] for proof. The above theorem says that the function ϕ must be μ-integrable, which so far we have only defined in the case that ϕ is a simple function. So,

Definition 2.2.4. Let $(X, \mathcal{M}, \mu)$ be a measure space. We say that X is σ-finite if $\mu(X) = \infty$, but there is a countable collection of measurable subsets $\{X_i :\in \mathbb{N}\} \subset \mathcal{M}$ such that $\mu(X_i) < \infty$ for all i, and $\bigcup_{i=1}^{\infty} X_i = X$.

Definition 2.2.5. Let $(X, \mathcal{M}, \mu)$ be a measure space, and $f : X \to \mathbb{C}$. If $A \in \mathcal{M}$ has finite measure, then we say that f is μ-integrable on A if there is a sequence of μ-integrable simple functions $(f_k)_{k=1}^{\infty}$ on A converging uniformly to f almost everywhere on A. That is, $(f_k)_{k=1}^{\infty}$ converges uniformly to f on a set $B \in \mathcal{M}$ such that $B \subseteq A$ and $\mu(A \setminus B) = 0$. We then define the integral of f with respect to μ on A by

$$\int_A f(x)d\mu(x) = \lim_{k\to\infty} \int_A f_k(x)d\mu(x)$$

If X is a σ-finite measure space and $A \in \mathcal{M}$ has infinite measure, then we say that f is integrable on A if for any countable collection of measurable subsets

$\{X_i :\in \mathbb{N}\} \subset \mathcal{M}$ such that $\mu(X_i) < \infty$ for all i, and $\bigcup_{i=1}^{\infty} X_i = X$, f is integrable on $X_i \cap A$ for each i and the limit

$$\lim_{i\to\infty} \int_{X_i\cap A} f(x)d\mu(x)$$

exists. We then define the integral of f with respect to μ on A by

$$\int_A f(x)d\mu(x) = \lim_{i\to\infty} \int_{X_i\cap A} f(x)d\mu(x).$$

See sections 29 and 30 of [3] for proof that these definitions are consistent.

As we can write $K = \bigcup_{m=1}^{\infty} \pi_K^{-m} O_K$, we have that K is σ-finite and thus these definitions are good enough for our purposes. Now that our integral is properly defined, a couple of useful properties are:

1. For any $f(x), g(x)$ integrable on A and scalars $\alpha, \beta \in \mathbb{C}$,

$$\int_A (\alpha f(x) + \beta g(x))d\mu(x) = \alpha \int_A f(x)d\mu(x) + \beta \int_A g(x)d\mu(x).$$

2. Let $\{A_i : i \in \mathbb{N}\}$ be a collection of measurable, disjoint subsets with $\bigcup_{i=1}^{\infty} A_i = A$. Then if $f(x)$ is integrable on A, then $f(x)$ is integrable on each A_i and

$$\int_A f(x)d\mu(x) = \sum_{i=1}^{\infty} \int_{A_i} f(x)d\mu(x).$$

See section 29 of [3] for proof.

At this point, we would like to extend the definition of the local zeta function $Z(f, s)$. The range of nonzero values $|\cdot|_K^s$ takes is a countable discrete set, and $|\cdot|_K^s$ is continuous for all $s \in \mathbb{C}$ with $\Re(s) \geq 0$. Thus for any continuous function $f : X \to K$, we can write $|f(x)|_K^s$ as a countable sum of characteristic functions of closed subsets of X. In particular, we can do this for any polynomial $f(\mathbf{x}) \in O_K[x_1, x_2, \ldots, x_n]$. In order to extend our local zeta function to multivariate polynomials however, we first need to define a measure on K^n.

Definition 2.2.6. Let $(X, \mathcal{M}, \mu)$ and $(Y, \mathcal{N}, \nu)$ be complete measure spaces, and let $\mathcal{R} = \{A \times B : A \in \mathcal{M}, B \in \mathcal{N}\}$ be the collection of measurable rectangles in

$X \times Y$. Then we define the product measure space as $(X \times Y, \mathcal{M} \otimes \mathcal{N}, \mu \otimes \nu)$, where

$$\mathcal{M} \otimes \mathcal{N} = \bigcap_{\mathcal{R} \subseteq \mathcal{A}} \mathcal{A}$$

is the intersection of all σ-algebras $\mathcal{A}$ in $X \times Y$ containing $\mathcal{R}$, and for each measurable set $E \in \mathcal{M} \otimes \mathcal{N}$, we have

$$(\mu \otimes \nu)(E) = \int_X \nu(E_x) d\mu(x) = \int_Y \mu(E^y) d\nu(y)$$

where $E_x = \{y \in Y : (x, y) \in E\}$ and $E^y = \{x \in X : (x, y) \in E\}$.

It is implicitly stated in the above definition that those functions and integrals are sufficiently well defined, though in this case we do allow integrals diverge to infinity when E has infinite measure. See [5] or Section 35 of [3]. In the case that $E = A \times B$ for some $A \in \mathcal{M}$ and $B \in \mathcal{N}$ with $\mu(A), \nu(B) < \infty$, its straightforward to see that $\mu(E^y) = \mu(A)\chi_B(y)$, and thus

$$(\mu \otimes \nu)(A \times B) = \int_Y \mu(A)\chi_B(y) d\nu(y) = \mu(A)\nu(B),$$

so the term "measurable rectangle" makes sense. Note that if both X and Y are σ-finite, then so is the product space $X \times Y$, as $\{X_i\} \subset \mathcal{M}$,$\{Y_j\} \subset \mathcal{N}$ with $\bigcup_i X_i = X$ and $\bigcup_j Y_j = Y$ implies $\{X_i \times Y_j\} \subset \mathcal{R} \subset \mathcal{M} \otimes \mathcal{N}$ with $\bigcup_{i,j}(X_i \times Y_j) = X \times Y$.

Our most powerful tool working over any product space is Fubini's theorem, which allows us to turn an integral over the product space $X \times Y$ into integrals over the original spaces X and Y.

Theorem 2.2.7. *Fubini's Theorem: Let $(X, \mathcal{M}, \mu)$ and $(Y, \mathcal{N}, \nu)$ be complete measure spaces, and $f(x, y)$ be integrable on the product space $X \times Y$. Then the integral of f over the product space $X \times Y$ is equal to the iterated integrals over X and Y. That is,*

$$\int_Y \left(\int_X f(x, y) d\mu(x) \right) d\nu(y) = \int_{X \times Y} f(x, y) d(\mu \otimes \nu)(x, y) = \int_X \left(\int_Y f(x, y) d\nu(y) \right) d\mu(x).$$

See [5] and section 35 of [3] for proof.

In the special case that the function f is separable, i.e. $f(x, y) = g(x)h(y)$ for

integrable functions g, h, by linearity the above equation simplifies to

$$\int_{X\times Y} f(x,y)d(\mu\otimes\nu)(x,y) = \int_X \left(\int_Y g(x)h(y)d\nu(y)\right) d\mu(x) = \int_X g(x)\left(\int_Y h(y)d\nu(y)\right) d\mu(x)$$
$$= \left(\int_X g(x)d\mu(x)\right)\left(\int_Y h(y)d\nu(y)\right).$$

Thus in this case the integral of the product is just the product of integrals.

Observe that taking the product of measure spaces is associative, i.e. if $(X_i, \mathcal{M}_i, \mu_i)$ for $i = 1, 2, 3$ are measure spaces, then $(\mathcal{M}_1 \otimes \mathcal{M}_2) \otimes \mathcal{M}_3 = \mathcal{M}_1 \otimes (\mathcal{M}_2 \otimes \mathcal{M}_3)$ and $(\mu_1 \otimes \mu_2) \otimes \mu_3 = \mu_1 \otimes (\mu_2 \otimes \mu_3)$ (see section 35 [3]). Thus we may unambiguously define the product of the n spaces as $(\prod_{i=1}^{n} X_i, \bigotimes_{i=1}^{n} \mathcal{M}_i, \bigotimes_{i=1}^{n} \mu_i)$. In the special case that all $(X_i, \mathcal{M}_i, \mu_i)$ are equal, we denote the product measure $\mu \otimes \mu \otimes \ldots \otimes \mu =: \mu^n$. Thus in particular, we define μ_K^n to be the product measure on K^n.

We would like to extend our definition of the local zeta function to include any polynomial $f(\mathbf{x}) \in O_K[x_1, \ldots, x_n]$. We've defined an appropriate measure μ_K^n on K^n, but unfortunately we still don't have that those polynomials are integrable. We prove this by proving that μ_K^n is in fact the Haar measure on K^n, thus getting that any continuous function is integrable over any compact subset of K^n. But first, a lemma:

Lemma 2.2.8. *Let X, Y be Hausdorff spaces with respective Borel measures μ, ν. If Y have a countable basis (e.g., Y is a separable metric space), then the product measure $\mu \otimes \nu$ is a Borel measure.*

See section 6.4 of [6] for proof.

In proposition 1.3.7, we showed that K is homeomorphic to $\mathbb{Q}_p^d$, where $d = [K : \mathbb{Q}_p]$. Thus as $\mathbb{Q}_p$ has $\mathbb{Q}$ as a dense subspace, we have that $\mathbb{Q}_p^d$ is a separable metric space. Thus K has a countable (topological) basis, so the product measure $\mu_K \otimes \mu_K = \mu_K^2$ on $K \times K = K^2$ is a Borel measure. By induction, if μ_K^{n-1} is a Borel measure, then we get that $\mu_K^{n-1} \otimes \mu_K = \mu_K^n$ is a Borel measure on $K^{n-1} \times K = K^n$. Thus every Borel set of K^n is measurable. We are now ready prove:

Proposition 2.2.9. *The Haar measure on K^n is the product measure μ_K^n.*

Proof. In light of Theorem 2.2.3, we prove this by showing that any continuous, nonnegative function with compact support is μ_K^n-integrable, and that integration with respect to μ_K^n is translation invariant. So, let $f : K^n \to \mathbb{R}_+$ be a continuous,

nonnegative function with compact support. Then there is a compact set $C \subset K^n$ such that $f(\mathbf{x}) = 0$ for all $\mathbf{x} \notin C$, and thus it suffices to show that f is integrable on C. We first construct a sequence of simple functions $(f_k)_{k=1}^{\infty}$ that converges uniformly to f. As f is continuous and C is compact, we have that f is bounded and thus there is a positive integer $M \in \mathbb{N}$ such that $f(\mathbf{x}) \leq M$ for all $\mathbf{x} \in K^n$. For each $k \in \mathbb{N}$ and $i = 1, \ldots, kM$, let $A_{i,k} = f^{-1}((\frac{i-1}{k}, \frac{i}{k}])$. Then as f is continuous, $A_{i,k} = f^{-1}((\frac{i-1}{k}, \frac{i}{k})) \cup f^{-1}(\{\frac{i}{k}\})$ is the union of an open set and a closed set, and thus is a Borel set of K^n. Hence $A_{i,k}$ is measurable for each i, k, so define $f_k(\mathbf{x}) = \sum_{i=1}^{kM} \frac{i}{k} \chi_{A_{i,k}}(\mathbf{x})$. Then for each k, f_k is a simple function with $|f_k(\mathbf{x}) - f(\mathbf{x})| < \frac{1}{k}$ for all $\mathbf{x}$. Thus $(f_k)_{k=1}^{\infty}$ converges uniformly to f on C. As C is compact, it is bounded and thus $C \subseteq \pi_K^{-m} O_K^n$ for some $m \in \mathbb{N}$. Thus $\mu_K^n(C) \leq \mu_K^n(\pi_K^{-m} O_K^n) = \big(\mu_K(\pi_K^{-m} O_K)\big)^n = q^{mn}$, and hence $\mu_K^n(C)$ is finite. As

$$\sum_{i=1}^{kM} \frac{i}{k} \mu_K^n(A_{i,k}) \leq M \sum_{i=1}^{kM} \mu_K^n(A_{i,k}) = M \mu_K^n(C) < \infty,$$

we have that $\sum_{i=0}^{\infty} \frac{i}{k} \mu_K^n(A_{i,k})$ converges, and thus f_k is integrable. Thus f is integrable, with

$$\int_{K^n} f(\mathbf{x}) d\mu_K^n(\mathbf{x}) = \lim_{k \to \infty} \int_{K^n} f_k(\mathbf{x}) d\mu_K^n(\mathbf{x}).$$

Now for any μ_K^n integrable function $\phi : K^n \to \mathbb{C}$ and any $y = [y_j]_{j=1}^n \in K^n$, consider

$$\int_{K^n} \phi(\mathbf{x} + \mathbf{y}) d\mu_K(\mathbf{x}).$$

By Fubini's theorem we can replace the integral over K^n as an n-fold iterated integral

$$\int_{K^n} \phi(\mathbf{x} + \mathbf{y}) d\mu_K^n(\mathbf{x}) =$$
$$\int_K \left(\int_K \ldots \left(\int_K \phi(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) d\mu_K(x_n) \right) \ldots d\mu_K(x_2) \right) d\mu_K(x_1).$$

As μ_K is the Haar measure on K, the inner integral is translation invariant and thus

$$\int_K \phi(x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) d\mu_K(x_n) = \int_K \phi(x_1 + y_1, x_2 + y_2, \ldots, x_n) d\mu_K(x_n)$$

and hence

$$\int_{K^n} \phi(\mathbf{x} + \mathbf{y}) d\mu_K^n(\mathbf{x}) =$$
$$\int_K \left(\int_K \ldots \left(\int_K \phi(x_1 + y_1, x_2 + y_2, \ldots, x_n) d\mu_K(x_n) \right) \ldots d\mu_K(x_2) \right) d\mu_K(x_1).$$

Again by Fubini's theorem, we can rearrange the order of integration in any way we like. Thus by repeating this argument for each x_j, $j = 1, \ldots, n-1$, we get that

$$\begin{aligned} &\int_{K^n} \phi(\mathbf{x} + \mathbf{y}) d\mu_K^n(\mathbf{x}) = \\ &\int_K \left(\int_K \ldots \left(\int_K \phi(x_1, x_2, \ldots, x_n) d\mu_K(x_n) \right) \ldots d\mu_K(x_2) \right) d\mu_K(x_1) \\ =&\int_{K^n} \phi(\mathbf{x}) \mu_K^n(\mathbf{x}). \end{aligned}$$

Thus integration with respect to the product measure μ_K^n is translation invariant, and thus μ_K^n is the Haar measure on K^n. □

Definition 2.2.10. Let $f(\mathbf{x}) \in O_K[x_1, x_2, \ldots, x_n]$. Then we define the local zeta function of f as

$$Z(f, s) = \int_{O_K^n} |f(\mathbf{x})|_K^s d\mu_K^n(\mathbf{x})$$

for all $s \in \mathbb{C}$ with $\Re(s) \geq 0$.

With the local zeta function finally defined, we can move on to a couple more examples.

Example: Consider $f(\mathbf{x}) = \sum_{i=1}^{n} x_i = x_1 + x_2 + \ldots + x_n$. Then by Fubini's theorem, we get that

$$Z(f,s) = \int\limits_{O_K^n} |\sum_{i=1}^{n} x_i|_K^s d\mu_K^n(\mathbf{x}) = \int\limits_{O_K^{n-1}} \left(\int\limits_{O_K} |\sum_{i=1}^{n} x_i|_K^s d\mu_K(x_n) \right) d\mu_K^{n-1}(\mathbf{x})$$
$$= \int\limits_{O_K^{n-1}} \left(\int\limits_{O_K} |x_n + \sum_{i=1}^{n-1} x_i|_K^s d\mu_K(x_n) \right) d\mu_K^{n-1}(\mathbf{x}).$$

Now in the inner integral, x_i is just a fixed constant with $x_i \in O_K$ for $i = 1, \ldots, n-1$. Thus $\sum_{i=1}^{n-1} x_i \in O_K$ is a constant, so by the translation invariance of the Haar measure

$$\int\limits_{O_K} |x_n + \sum_{i=1}^{n-1} x_i|_K^s d\mu_K(x_n) = \int\limits_{O_K} |x_n|_K^s d\mu_K(x_n) = Z(x,s) = \frac{q-1}{q-q^{-s}}.$$

Thus we have

$$Z(f,s) = \int\limits_{O_K^{n-1}} \left(\int\limits_{O_K} |x_n + \sum_{i=1}^{n-1} x_i|_K^s d\mu_K(x_n) \right) d\mu_K^{n-1}(\mathbf{x}) = \int\limits_{O_K^{n-1}} \frac{q-1}{q-q^{-s}} d\mu_K^{n-1}(\mathbf{x})$$
$$= \frac{q-1}{q-q^{-s}} \int\limits_{O_K^{n-1}} d\mu_K^{n-1}(\mathbf{x}) = \frac{q-1}{q-q^{-s}}.$$

Example: Take $f(\mathbf{x}) = \prod_{i=1}^{n} x_i$. Since f is separable and $|\cdot|_K^s$ is multiplicative,

$$Z(f,s) = \int\limits_{O_K^n} |\prod_{i=1}^{n} x_i|_K^s d\mu_K^n(\mathbf{x}) = \int\limits_{O_K^n} \prod_{i=1}^{n} |x_i|_K^s d\mu_K^n(\mathbf{x})$$
$$= \prod_{i=1}^{n} \left(\int\limits_{O_K} |x_i|_K^s d\mu_K(x_i) \right) = \prod_{i=1}^{n} Z(x,s) = \left(\frac{q-1}{q-q^{-s}} \right)^n.$$

So far all the integrals we've computed have been rather simple. As our polynomials become more complicated though, the calculations drastically become more difficult. So before we introduce a less trivial example, we need one more tool for calculating these integrals. And as what seems to be the theme of this paper, before

we can say anything useful we need more definitions.

Definition 2.2.11. Let U be an open subset of K^n, and $f : U \to K$. Then we say f is a K-analytic function if f can expanded locally as a power series about any point $\mathbf{a} \in U$. That is, if for any $\mathbf{a} \in U$, there is a neighborhood U' of $\mathbf{a}$ such that for all $\mathbf{x} \in U'$, we have

$$f(\mathbf{x}) = f(\mathbf{a}) + \sum_{\mathbf{i} \in \mathbb{N}^n} c_{\mathbf{i}} (\mathbf{x} - \mathbf{a})^{\mathbf{i}}$$

where $c_{\mathbf{i}} \in K$ and $(\mathbf{x} - \mathbf{a})^{\mathbf{i}} := \prod_{k=1}^{n} (x_k - a_k)^{i_k}$ for all $\mathbf{i} \in \mathbb{N}^n$.

If $f = [f_j]_{j=1}^m : U \to K^m$, then we say that f is a K-analytic map if each f_j is a K-analytic function for $j = 1, \ldots, m$. If V is also an open subset of K^n and $f : U \to V$ is a bijection such that both f, f^{-1} are K-analytic maps, then we say that f is a K-bianalytic map.

Finally, if $f : U \to V$ is a K-analytic map, then we define the function $\dfrac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)} : U \to K$ by

$$\frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)}(\mathbf{a}) := \det \left[\left. \frac{\partial f_j}{\partial x_i} \right|_{\mathbf{x}=\mathbf{a}} \right]_{i,j=1}^{n}$$

Theorem 2.2.12. *Change of Variables Formula: Let U, V be open sets of K^n and $f : U \to V$ be a K-analytic map such that $\dfrac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)}(\boldsymbol{a}) \neq 0$ for all $\boldsymbol{a} \in U$. Then f is a K-bianalytic map, and for any function ϕ integrable on a measurable set $f(A)$ for some $A \subseteq U$,*

$$\int_{f(A)} \phi(\boldsymbol{y}) d\mu_K^n(\boldsymbol{y}) = \int_A \phi(f(\boldsymbol{x})) \left| \frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)}(\boldsymbol{x}) \right|_K d\mu_K^n(\boldsymbol{x}).$$

Proof. We prove this in the special case that $f(\mathbf{x}) = D\mathbf{x}$ for some diagonal matrix $D \in GL_n(K)$, as this is the only case we will use in the paper. See 7.4 of [1] for full proof.

In our case, $\dfrac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)}(\mathbf{x}) = \det(D)$, and thus we need to show that

$$\int_{DA} \phi(\mathbf{y}) d\mu_K^n(\mathbf{y}) = \int_A \phi(D\mathbf{x}) |\det(D)|_K d\mu_K^n(\mathbf{x}).$$

We do this by showing that $\nu_D(\cdot) = \mu_K^n(D\cdot)$ is a Haar measure, from which it

follows that $\nu_D = |\det(D)|_K \mu_K^n$. As $D \in GL_n(K)$, it follows that $f(\mathbf{x}) = D\mathbf{x}$ is a homeomorphism on K^n. Thus a set $A \subseteq K^n$ is a Borel set if and only if $DA = \{D\mathbf{x} : \mathbf{x} \in A\}$ is a Borel set. For any Borel set $A \subseteq K^n$ and $\mathbf{y} \in K^n$, we have that

$$\nu_D(y + A) = \mu_K^n(D(y + A)) = \mu_K^n(Dy + DA) = \mu_K^n(DA) = \nu_D(A).$$

Thus ν_D is a translation invariant Borel measure. As D sends compacts sets to compact sets, we have that for any compact set $C \subset K^n$ that $\nu_D(C) = \mu_K^n(DC) < \infty$. Thus ν_D is finite on compact sets.

Now let U be a fixed open set, and consider $\nu_D(U)$. As μ_K^n is inner regular, if $\mu_K^n(DU) < \infty$, then for any $\epsilon > 0$, there is a compact set $C_\epsilon \subseteq DU$ such that $\mu_K^n(C_\epsilon) > \mu_K^n(DU) - \epsilon$. Thus $D^{-1}C_\epsilon \subset U$ with $\nu_D(D^{-1}C) > \nu_D(U) - \epsilon$. If $\mu_K^n(DU) = \infty$, then for any $M > 0$ there is a compact set $C_M \subset DU$ such that $\mu_K(C_M) > M$. Thus $D^{-1}C_M \subset U$ with $\nu_D(D^{-1}C) > M$. Thus ν_D is inner regular on open sets. The proof that ν_D is outer regular on Borel sets follows the same form, so we have that ν_D is a Haar measure on K^n.

Thus as the Haar measure is unique up to a positive scalar, we have that $\nu_D = \alpha\mu_K^n$ for some $\alpha > 0$. Let d_i denote the i'th diagonal entry of D. Then as D is invertible, $d_i = u_i\pi_k^{m_i}$ for some $u_i \in O_K \setminus \pi_K O_K$ and $m_i \in \mathbb{Z}$ for $i = 1, \ldots, n$. Thus $DO_K^n = \prod_{i=1}^n u_i\pi_K^{m_i} O_K = \prod_{i=1}^n \pi_K^{m_i} O_K$, and thus

$$\alpha = \nu_D(O_K^n) = \mu_K^n(\prod_{i=1}^n \pi_K^{m_i} O_K) = q^{-\sum_i m_i}.$$

As $|\det(D)|_K = |\prod_{i=1}^n u_i\pi_K^{m_i}|_K = \prod_{i=1}^n |\pi_K^{m_i}|_K = q^{-\sum_i m_i}$, we thus have that $\nu_D = |\det(D)|_K \mu_K^n$.

Now let $A \subset K^n$ be a measurable set, and ϕ be an integrable simple function on DA. Then $\phi(\mathbf{y}) = \sum_{m=0}^{\infty} c_m \chi_{DA_m}(\mathbf{y})$ for some measurable sets $A_m \subseteq A$ and all

$\mathbf{y} \in DA$. Then $\phi(D\mathbf{x}) = \sum_{m=0}^{\infty} c_m \chi_{A_m}(\mathbf{x})$ for all $\mathbf{x} \in A$, and thus we have that

$$\begin{aligned}\int_{DA} \phi(\mathbf{y}) d\mu_K^n(\mathbf{y}) &= \sum_{m=0}^{\infty} c_m \mu_K^n(DA_m) = \sum_{m=0}^{\infty} c_m |\det(D)|_K \mu_K^n(A_m) \\ &= \int_A \phi(D\mathbf{x}) |\det(D)|_K \mu_K^n(\mathbf{x}).\end{aligned}$$

Thus the equality holds for simple functions. As $\phi_k \to \phi$ uniformly implies $\phi_K |\det(D)|_K \to \phi |\det(D)|_K$ uniformly, by taking limits we get that equality holds for all integrable functions ϕ.

□

With the proof of the change of variables formula now done, we can finally move on to a more complicated local zeta function.

Proposition 2.2.13. *Let $f(x,y) = xy(x+y)$. Then the local zeta function of f is*

$$Z(f,s) = \int_{O_K^2} |xy(x+y)|_K^s d\mu_K^2(x,y) = \frac{(q-1)((2q-1)q^{-s} + q^2 - 2q)}{(q-q^{-s})(q^2 - q^{-3s})}.$$

Proof. For any $x, y \in O_K$, there are three basic scenarios: either $|x|_K > |y|_K$, $|x|_K < |y|_K$, or $|x|_K = |y|_K$. Thus we can break up our integral into three parts,

$$\begin{aligned}\int_{O_K^2} |f|_K^s d\mu_K^2(x,y) = &\int_{|x|_K > |y|_K} |x|_K^s |y|_K^s |x+y|_K^s d\mu_K^2(x,y) + \int_{|x|_K < |y|_K} |x|_K^s |y|_K^s |x+y|_K^s d\mu_K^2(x,y) \\ &+ \int_{|x|_K = |y|_K} |x|_K^s |y|_K^s |x+y|_K^s d\mu_K^2(x,y).\end{aligned}$$

By the symmetry of x and y, we have that the first two parts are the same. Furthermore, $|x|_K > |y|_K$ implies $|x+y|_K = |x|_K$. Thus we get that

$$\int_{O_K^2} |f|_K^s d\mu_K^2(x,y) = 2 \int_{|x|_K > |y|_K} |x|_K^{2s} |y|_K^s d\mu_K^2(x,y) + \int_{|x|_K = |y|_K} |x|_K^s |y|_K^s |x+y|_K^s d\mu_K^2(x,y).$$

Finally, there are two distinct cases when $|x|_K = |y|_K$; either $|x+y|_K = |x|_K = |y|_K$, or $|x+y|_K < |x|_K, |y|_K$. Thus we have that

$$\int_{O_K^2} |f|_K^s d\mu_K^2(x,y) = 2 \int_{|x|_K>|y|_K} |x|_K^{2s}|y|_K^s d\mu_K^2(x,y) + \int_{|x+y|_K=|x|_K=|y|_K} |x|^{3s} d\mu_K^2(x,y)$$
$$+ \int_{|x+y|_K<|x|_K=|y|_K} |x|_K^{2s}|x+y|_K^s d\mu_K^2(x,y).$$

Using Fubini's theorem, we then have that our first integral

$$\int_{|x|_K>|y|_K} |x|_K^{2s}|y|_K^s d\mu_K^2(x,y) = \int_{O_K} |x|_K^{2s} \left(\int_{|x|_K>|y|_K} |y|_K^s d\mu_K(y) \right) d\mu_K(x).$$

Breaking down the x integral into the different level sets $\pi_K^m O_K \setminus \pi_K^{m+1} O_K$ and summing them up, we get that

$$\begin{aligned}\int_{|x|_K>|y|_K} |x|_K^{2s}|y|_K^s d\mu_K^2(x,y) &= \sum_{m=0}^{\infty} \int_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} |x|_K^{2s} \left(\int_{\pi_K^{m+1} O_K} |y|_K^s d\mu_K(y) \right) d\mu_K(x) \\ &= \sum_{m=0}^{\infty} q^{-2ms} \mu_K(\pi_K^m O_K \setminus \pi_K^{m+1} O_K) \int_{\pi_K^{m+1} O_K} |y|_K^s d\mu_K(y) \\ &= \sum_{m=0}^{\infty} q^{-2ms} \frac{q-1}{q^{m+1}} \int_{\pi_K^{m+1} O_K} |y|_K^s d\mu_K(y).\end{aligned}$$

By making the change of variables $y' = \pi_K^{-(m+1)} y$, we get that the inner integral is

$$\begin{aligned}\int_{\pi_K^{m+1} O_K} |y|_K^s d\mu_K(y) &= \int_{O_K} |\pi_K^{m+1} y'|_K^s d\mu_K(\pi_K^{m+1} y') = \int_{O_K} |\pi_K^{m+1} y'|_K^s |\pi_K^{m+1}|_K d\mu_K(y') \\ &= q^{-(m+1)(s+1)} \int_{O_K} |y'|_K^s d\mu_K(y') = q^{-(m+1)(s+1)} \frac{q-1}{q-q^{-s}}.\end{aligned}$$

Thus we get that

$$\begin{aligned}\int\limits_{|x|_K>|y|_K} |x|_K^{2s}|y|_K^s d\mu_K^2(x,y) &= \sum_{m=0}^{\infty} q^{-2ms}\frac{q-1}{q^{m+1}} \int\limits_{\pi_K^{m+1}O_K} |y|_K^s d\mu_K(y) \\ &= \sum_{m=0}^{\infty} q^{-2ms}\frac{q-1}{q^{m+1}}\left(q^{-(m+1)(s+1)}\frac{q-1}{q-q^{-s}}\right) \\ &= \frac{q^{-s}(q-1)^2}{q^2(q-q^{-s})}\sum_{m=0}^{\infty}(q^{-(3s+2)})^m = \frac{q^{-s}(q-1)^2}{q^2(q-q^{-s})(1-q^{-(3s+2)})} \\ &= \frac{q^{-s}(q-1)^2}{(q-q^{-s})(q^2-q^{-3s})}.\end{aligned}$$

Now for the second integral where $|x|_K = |y|_K = |x+y|_K$, we see that

$$\begin{aligned}\int\limits_{|x+y|_K=|x|_K=|y|_K} |x|_K^{3s} d\mu_K^2(x,y) &= \int\limits_{O_K} |x|_K^{3s}\left(\int\limits_{|y|_K=|x+y|_K=|x|_K} d\mu_K(y)\right) d\mu_K(x) \\ &= \int\limits_{O_K} |x|_K^{3s}\mu_K(\{y : |y|_K = |x+y|_K = |x|_K\}) d\mu_K(x).\end{aligned}$$

We can then break down the x integral and sum over the level sets $\pi_K^m O_K \setminus \pi_K^{m+1}O_K$. Thus

$$\begin{aligned}\int\limits_{|x+y|_K=|x|_K=|y|_K} |x|_K^{3s} d\mu_K^2(x,y) &= \sum_{m=0}^{\infty} \int\limits_{\pi_K^m O_K\setminus\pi_K^{m+1}O_K} |x|_K^{3s}\mu_K(\{y : |y|_K = |x+y|_K = |x|_K\}) d\mu_K(x) \\ &= \sum_{m=0}^{\infty} q^{-3ms} \int\limits_{\pi_K^m O_K\setminus\pi_K^{m+1}O_K} \mu_K(\{y : |y|_K = |x+y|_K = q^{-m}\}) d\mu_K(x).\end{aligned}$$

Fix some $x \in \pi_K^m O_K \setminus \pi_K^{m+1}O_K$; then $x = \sum_{i=m}^{\infty} a_i \pi_K^i$ for some $a_i \in S$ with $a_m \neq 0$. Now, $|y|_K = q^{-m}$ implies $y = \sum_{i=m}^{\infty} b_i \pi_K^i$ for some $b_i \in S$ with $b_m \neq 0$. Then $|y|_K = |x+y|_K = q^{-m}$ implies that $a_m + b_m \notin \pi_K O_K$. Thus $b_m \not\equiv 0, -a_m \mod \pi_K$, so there are $q-2$ choices for b_m in S. As any b_i for $i > m$ is irrelevant, we then have that $\mu_K(\{y : |y|_K = |x+y|_K = q^{-m}\}) = (q-2)\mu_K(\pi_K^{m+1}O_K) = (q-2)q^{-(m+1)}$. Thus

$$\int\limits_{|x+y|_K=|x|_K=|y|_K} |x|_K^{3s} d\mu_K^2(x,y) = \sum_{m=0}^{\infty} q^{-3ms}(q-2)q^{-(m+1)} \int\limits_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} d\mu_K(x)$$
$$= \sum_{m=0}^{\infty} q^{-3ms}(q-2)q^{-(m+1)}(q-1)q^{-(m+1)}$$
$$= \frac{(q-1)(q-2)}{q^2} \sum_{m=0}^{\infty} (q^{-(3s+2)})^m = \frac{(q-1)(q-2)}{q^2 - q^{-3s}}.$$

And finally for the third integral where $|x|_K = |y|_K > |x+y|_K$, by breaking it up into the x-level sets we get that

$$\int\limits_{|x+y|_K<|x|_K=|y|_K} |x|_K^{2s}|x+y|_K^s d\mu_K(x,y) = \int\limits_{O_K} |x|_K^{2s} \left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^s d\mu_K(y) \right) d\mu_K(x)$$
$$= \sum_{m=0}^{\infty} \int\limits_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} |x|_K^{2s} \left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^s d\mu_K(y) \right) d\mu_K(x)$$
$$= \sum_{m=0}^{\infty} q^{-2ms} \int\limits_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} \left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^s d\mu_K(y) \right) d\mu_K(x).$$

Now, given a fixed $x \in \pi_K^m O_K \setminus \pi_K^{m+1} O_K$, we have that $x = \sum_{i=m}^{\infty} a_i \pi_K^i$ for some $a_i \in S$ with $a_m \neq 0$. Thus there are $q-1$ choices for a_m. As $|y|_K = |x|_K$, we also have that $y = \sum_{i=m}^{\infty} b_i \pi_K^i$ for some $b_i \in S$ with $b_m \neq 0$. As we need $|x+y|_K < |x|_K, |y|_K$, that means that we must have $a_m + b_m \in \pi_K O_K$. As there is only one element in S such that $x \equiv -a_m \mod \pi_K$, we have that b_m has a fixed value. All other coefficients are arbitrary, so we get that

$$\int\limits_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} \left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^s d\mu_K(y) \right) d\mu_K(x) = (q-1) \int\limits_{\pi_K^{m+1} O_K^2} |x+y|_K^s \mu_K^2(x,y).$$

Making the change of variables $x' = \pi_K^{-(m+1)} x$ and $y' = \pi_K^{-(m+1)} y$, we get that

$$\int\limits_{\pi_K^{m+1}O_K^2} |x+y|_K^s d\mu_K^2(x,y) = \int\limits_{O_K^2} |\pi_K^{m+1}(x'+y')|_K^s d\mu_K(\pi_K^{m+1}x', \pi_K^{m+1}y')$$
$$= q^{-(m+1)(s+2)} \int\limits_{O_K^2} |x'+y'|_K^s d\mu_K(x',y') = q^{-(m+1)(s+2)} \frac{q-1}{q-q^{-s}}.$$

Thus

$$\int\limits_{|x+y|_K<|x|_K=|y|_K} |x|_K^{2s}|x+y|_K^s d\mu_K(x,y)$$
$$= \sum_{m=0}^{\infty} q^{-2ms} \int\limits_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} \left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^s d\mu_K(y) \right) d\mu_K(x)$$
$$= \sum_{m=0}^{\infty} q^{-2ms}(q-1)q^{-(m+1)(s+2)} \frac{q-1}{q-q^{-s}} = \frac{q^{-s}(q-1)}{q^2(q-q^{-s})} \sum_{m=0}^{\infty} (q^{-(3s+2)})^m$$
$$= \frac{q^{-s}(q-1)^2}{(q-q^{-s})(q^2-q^{-3s})}.$$

Summing up the results of those three integrals, we have that our initial integral

$$\int\limits_{O_K^2} |f|_K^s d\mu_K^2(x,y) = 2 \int\limits_{|x|_K>|y|_K} |x|_K^{2s}|y|_K^s d\mu_K^2(x,y) + \int\limits_{|x+y|_K=|x|_K=|y|_K} |x|^{3s} d\mu_K^2(x,y)$$
$$+ \int\limits_{|x+y|_K<|x|_K=|y|_K} |x|_K^{2s}|x+y|_K^s d\mu_K^2(x,y)$$
$$= 2\frac{q^{-s}(q-1)^2}{(q-q^{-s})(q^2-q^{-3s})} + \frac{(q-1)(q-2)}{q^2-q^{-3s}} + \frac{q^{-s}(q-1)^2}{(q-q^{-s})(q^2-q^{-3s})}$$
$$= \frac{(q-1)(2(q-1)q^{-s} + (q-2)(q-q^{-s}) + (q-1)q^{-s})}{(q-q^{-s})(q^2-q^{-3s})}$$
$$= \frac{(q-1)((2q-1)q^{-s} + q^2 - 2q)}{(q-q^{-s})(q^2-q^{-3s})}.$$

Thus $Z(f,s) = \dfrac{(q-1)((2q-1)q^{-s} + q^2 - 2q)}{(q-q^{-s})(q^2-q^{-3s})}$. □

In general, for any positive integers d, e, the polynomial $f(x,y) = (xy)^d(x+y)^e$

has local zeta function

$$Z(f,s) = \frac{(q-1)((1-2q)q^{-(d+e)s} + (q^2)q^{-ds} + (q)q^{-es} + q^3 - 2q^2)}{(q-q^{-ds})(q-q^{-es})(q^2-q^{-(2d+e)s})}.$$

The calculation follows the exact same form as the one above, just with a little more bookkeeping. See appendix for complete proof.

It's now readily apparent that for even relatively simple polynomials in 2 variables, calculating the local zeta function quickly becomes complicated. This raises two very important questions: what kind of forms do these local zeta functions take, and why should we bother to calculate them? There is a good answer to the first:

Theorem 2.2.14. *Let $f(\boldsymbol{x}) \in O_K[x_1, \ldots, x_n]$. Then the local zeta function of f, $Z(f,s)$ is a rational function of q^{-s}.*

The theorem is due to Igusa, and involves a large amount of geometry that is beyond the scope of this paper. See 8.2 of [1] or [7] for proof.

As for the second question, one answer is the study and calculation of Poincaré series.

2.3 Poincaré Series

The original number theoretic for the Poincaré Series is as follows: fix a prime p, and let $f(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$ be an integer polynomial. Let

$$N_m = \text{card}(\{\mathbf{y} \in (\mathbb{Z}/p^m\mathbb{Z})^n : f(\mathbf{y}) \equiv 0 \mod p^m\})$$

denote the the number of zeroes of $f \bmod p^m$, with $N_0 = 1$ by convention. Then the Poincaré series of f is defined to be

$$Q(f,t) := \sum_{m=0}^{\infty} N_m t^m.$$

The classical definition of the Poincaré series can easily be expanded to p-adic fields as follows.

Definition 2.3.1. Let $f(\mathbf{x}) \in O_K[x_1, \ldots, x_n]$. Then let $N_0 = 1$, and for any positive integer $m \in \mathbb{N}$, let

$$N_m = \text{card}(\{\mathbf{y} + \pi_K^m O_K^n \in (O_K/\pi_K^m O_K)^n : f(\mathbf{y}) \equiv 0 \mod \pi_K^m\})$$

We define the Poincaré series of f to be

$$Q(f,t) := \sum_{m=0}^{\infty} N_m t^m$$

As we necessarily have $N_m \leq \text{card}((O_K/\pi_K^m O_K)^n) = q^{mn}$, it follows that $Q(f,t)$ is a convergent series whenever $|t| < q^{-n}$.

Example: Consider $f(x) = x$. Then for every $m \in \mathbb{N}$, $f(x) \equiv 0 \mod \pi_K^m$ if and only if $x \equiv 0 \mod \pi_K^m$. Thus there is a unique zero, so $N_m = 1$ and thus $Q(f,t) = \sum_{m=0}^{\infty} t^m = \frac{1}{1-t}$.

Example: Let $f(x,y) = x^2 - y$. Let $x + \pi_K^m O_K \in O_K/\pi_K^m O_K$. Then there is a unique $y + \pi_K^m O_K \in O_K/\pi_K^m O_K$ such that $y \equiv x^2 \mod \pi_K^m$, and thus a unique y such that $f(x,y) \equiv 0 \mod \pi_K^m$. Thus as there are q^m choices for x, we have that $N_m = q^m$ so $Q(f,t) = \sum_{m=0}^{\infty} q^m t^m = \frac{1}{1-qt}$.

These are two rather simple examples, but in general things can get complicated very quickly.

Example: Take $f(x,y) = xy$, and suppose $xy \equiv 0 \mod \pi_K^m$. We have that each pair (x,y) can be uniquely represented $\mod \pi_K^m$ as $x \equiv \sum_{i=0}^{m-1} a_i \pi_K^i \mod \pi_K^m$ and $y \equiv \sum_{i=0}^{m-1} b_i \pi_K^i \mod \pi_K^m$, where $a_i, b_i \in S$. We consider $m+1$ different cases. First, suppose $x \equiv 0 \mod \pi_K^m$. Then there as there are q choices for each b_i for y, giving q^m total possibilities. Now if $x \not\equiv 0 \mod \pi_K^m$, then we have that there is an $0 \leq k \leq m-1$ such that $a_i = 0$ for all $i < k$, but $a_k \neq 0$. Then as $xy \equiv 0 \mod \pi_K^m$, we must then have $b_i = 0$ for all $i \leq m-k$. We then have $(q-1)$ choices for a_k, and q choices for each a_i, b_j with $i > k$, $j > m-k$. Thus we have $(q-1)q^{m-1}$ possible choices for the a_i, b_j. As there are m choices for k, that gives us a total of $q^m + m(q-1)q^{m-1} = (m+1)q^m - mq^{m-1}$ zeroes of $f \mod \pi_K^m$. Thus

$$\begin{aligned} Q(f,t) &= \sum_{m=0}^{\infty} ((m+1)q^m - mq^{m-1})t^m = \sum_{m=0}^{\infty} (m+1)q^m t^m - t\sum_{m=0} mq^{m-1}t^{m-1} \\ &= \frac{1}{(1-qt)^2} - \frac{t}{(1-qt)^2} = \frac{1-t}{(1-qt)^2}. \end{aligned}$$

So even an incredibly simple polynomial $f(x,y) = xy$ requires some effort in order to calculate it's Poincaré series. For complicated polynomials, counting the number of zeroes very quickly becomes a combinatorial nightmare. However, these functions

do always have nice structure:

Theorem 2.3.2. *$Q(f,t)$ is a rational function of t.*

This statement was conjectured Borevich and Shafarevich, and then proved by Igusa. Igusa proved this by showing that $Z(f,s)$ was a rational function of q^{-s}, and then relating the two by

Proposition 2.3.3. *Let $f(\boldsymbol{x}) \in O_K[x_1,\ldots,x_n]$. Then*

$$Z(f,s) = Q(f,q^{-(n+s)})(1-q^s)+q^s$$

Proof. For every $m \geq 0$, take $V_m = \{\mathbf{x} \in O_K^n : |f(\mathbf{x})|_K \leq q^{-m}\}$. Now as f is a polynomial in $O_K[x_1,\ldots,x_n]$, we have that if $\mathbf{y} \in O_K$ is such that $f(\mathbf{y}) \in V_m$, then $f(\mathbf{y}+\pi_K^m O_K^n) \subseteq V_m$. Now there are N_m distinct zeroes $\mathbf{y}+\pi_K^m O_K^n$ of $f \mod \pi_K^m$, and thus f maps N_m distinct balls to V_m. As K is an ultrametric space, all balls are disjoint so V_m is the union N_m disjoint balls of the form $\mathbf{y}+\pi_K^m O_K^n$. Thus $\mu_K^n(V_m) = N_m \mu_K^n(\pi_K^m O_K^n) = N_m q^{-mn}$.

But $V_m \setminus V_{m+1} = \{\mathbf{x} \in O_K^n : |f(\mathbf{x})|_K = q^{-m}\}$, so

$$\begin{aligned}
Z(f,s) &= \sum_{m=0}^{\infty} q^{-ms}\mu_K^n(V_m \setminus V_{m+1}) = \sum_{m=0}^{\infty} q^{-ms}(\mu_K^n(V_m)-\mu_K^n(V_{m+1})) \\
&= \sum_{m=0}^{\infty} q^{-ms}\mu_K^n(V_m) - \sum_{m=0}^{\infty} q^{-ms}\mu_K^n(V_{m+1}) \\
&= \sum_{m=0}^{\infty} N_m q^{-m(n+s)} - q^s \sum_{m=0}^{\infty} N_{m+1} q^{-(m+1)(n+s)} \\
&= Q(f,q^{-(n+s)}) - q^s(Q(f,q^{-(n+s)})-1) = Q(f,q^{-(n+s)})(1-q^s)+q^s.
\end{aligned}$$

□

Thus taking $t = q^{-s}$, we have that $Z(f,s) = Q(f,q^{-n}t)(1-t^{-1})+t^{-1}$, making

$$Q(f,q^{-n}t) = \frac{tZ(f,s)-1}{t-1}$$

Thus as $Z(f,s)$ is a rational function of $t = q^{-s}$, we have that $Q(f,t)$ is a rational function as well.

So by calculating the local zeta function $Z(f,s)$ of a polynomial f, we can then turn it into the Poincaré series of f and thus count the number of zeroes of f mod π_K^m for all $m \in \mathbb{N}$.

Example: Take $f(\mathbf{x}) = \sum_{i=1}^{n} x_i = x_1 + x_2 + \ldots + x_n$. Then as we showed in section 2.2,

$$Z(f,s) = \int_{O_K^n} |x_1 + \ldots + x_n|_K^s d\mu_K^n(\mathbf{x}) = \int_{O_K^{n-1}} \left(\int_{O_K} |x_1 + \ldots + x_n|_K^s d\mu_K(x_n) \right) d\mu_K^{n-1}(\mathbf{x})$$
$$= \int_{O_K^{n-1}} \left(\int_{O_K} |x_n|_K^s d\mu_K(x_n) \right) d\mu_K^{n-1}(\mathbf{x}) = \int_{O_K^{n-1}} \frac{q-1}{q-q^{-s}} d\mu_K^{n-1}(\mathbf{x}) = \frac{q-1}{q-q^{-s}}$$

by Fubini's theorem and the translation invariance of the Haar measure. Thus

$$Q(f, q^{-n}t) = \frac{t\frac{q-1}{q-t} - 1}{t-1} = \frac{tq - t - q + t}{(t-1)(q-t)} = \frac{q(t-1)}{(t-1)(q-t)}$$
$$= \frac{1}{1-t/q} = \sum_{m=0}^{\infty} \left(\frac{t}{q}\right)^m.$$

And hence $Q(f,t) = \sum_{m=0}^{\infty} q^{(n-1)m} t^m$.

We could have also gotten this result with a combinatorial argument: For any choice of $x_1, x_2, \ldots, x_{n-1}$, there is a unique $x_n \mod \pi_K^m$ such that $x_n \equiv -\sum_{i=1}^{n-1} x_i$. As we have q^m choices for each x_i, and our choices of each x_i are independent of each other for $i = 1, \ldots, n-1$, we thus have $q^{(n-1)m}$ zeroes of $f \mod \pi_K^m$. Thus $Q(f,t) = \sum_{m=0}^{\infty} q^{(n-1)m} t^m$

Comparing the calculation of the zeta function and the combinatorial argument, we can see how the translation invariance of the Haar measure corresponds to how our choice of x_i for $i < n$ fixes the value for x_n.

As we have at our disposal a large number of tools in order to help calculate the integral $\int_{O_K^n} |f(\mathbf{x})|_K^s d\mu_K^n(\mathbf{x})$, oftentimes this is less difficult for more complicated polynomials, or even seemingly simple polynomials.

Example: Consider $f(\mathbf{x}) = \prod_{i=1}^{n} x_i$; then as f is separable, by Fubini's theorem

we have that

$$\begin{aligned} Z(f,s) &= \int_{O_K^n} |\prod_{i=1}^{n} x_i|_K^s d\mu_K^n(\mathbf{x}) = \prod_{i=1}^{n} \left(\int_{O_K} |x_i|_K^s d\mu_K(x_i) \right) \\ &= Z(x,s)^n = \left(\frac{q-1}{q-t} \right)^n. \end{aligned}$$

Plugging this into our formula for $Q(f,t)$, we then get that

$$\begin{aligned} Q(f,q^{-n}t) &= \frac{t\left(\frac{q-1}{q-t}\right)^n - 1}{t-1} = \frac{t(q-1)^n - (q-t)^n}{(q-t)^n(t-1)} \\ &= \frac{1}{(q-t)^n(t-1)} \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} q^k (t - t^{n-k}) \\ &= \frac{1}{(q-t)^n(t-1)} \left(q^n(t-1) + \sum_{k=0}^{n-2} (-1)^{n-k} \binom{n}{k} q^k (t - t^{n-k}) \right). \end{aligned}$$

As $\dfrac{t^r - 1}{t-1} = t^{r-1} + t^{r-2} + \ldots + t + 1$, we then get that

$$\begin{aligned} Q(f,q^{-n}t) &= \frac{1}{(q-t)^n} \left(q^n - \sum_{k=0}^{n-2} (-1)^{n-k} \binom{n}{k} q^k \sum_{l=1}^{n-k-1} t^l \right) \\ &= \frac{1}{(q-t)^n} \left(q^n - \sum_{l=1}^{n-1} \left(\sum_{k=0}^{n-1-l} (-1)^{n-k} \binom{n}{k} q^k \right) t^l \right). \end{aligned}$$

Replacing k with $n-k$ in the inner sum and dividing through by q^n, we now have

$$\begin{aligned} Q(f,q^{-n}t) &= \frac{1}{(1-t/q)^n} \left(1 - \sum_{l=1}^{n-1} \left(\sum_{k=l+1}^{n} (-1)^k \binom{n}{k} q^{-k} \right) t^l \right) \\ &= \sum_{m=0}^{\infty} \binom{m+n-1}{m} \left(1 - \sum_{l=1}^{n-1} \left(\sum_{k=l+1}^{n} (-1)^k \binom{n}{k} q^{-(k-l)} \right) (t/q)^l \right) (t/q)^m. \end{aligned}$$

Rearranging terms, replacing k with $k-l$, and noting that $\binom{h+n-1}{h} = 0$ whenever for $h < 0$, we finally get

$$Q(f,q^{-n}t) = \sum_{m=0}^{\infty}\left(\binom{m+n-1}{m} - \sum_{l=1}^{n-1}\binom{m+n-l-1}{m-l}\sum_{k=1}^{n-l}(-1)^{k+l}\binom{n}{k+l}q^{-k}\right)(t/q)^m$$
$$= \sum_{m=0}^{\infty}\left(\binom{m+n-1}{m} - \sum_{k=1}^{n-1}\sum_{l=1}^{n-k}(-1)^{k+l}\binom{m+n-l-1}{m-l}\binom{n}{k+l}q^{-k}\right)(t/q)^m.$$

Thus we get that the number of zeroes of $f \mod \pi_K^m$ is

$$N_m = q^{(n-1)m}\left(\binom{m+n-1}{m} - \sum_{k=1}^{n-1}\sum_{l=1}^{n-k}(-1)^{k+l}\binom{m+n-l-1}{m-l}\binom{n}{k+l}q^{-k}\right).$$

While this is the answer, with a bit more work we can get it into a more coherent form.

Evaluating $\sum_{l=1}^{n-k}(-1)^{k+l}\binom{m+n-l-1}{m-l}\binom{n}{k+l}$ in Wolfram Alpha gives us $-(-1)^k\frac{(k+1)(m+n-1)}{n(k+m)}\binom{m+n-2}{m-1}\binom{n}{k+1}$. With a bit more effort, we can then get that

$$\begin{aligned}\sum_{l=1}^{n-k}(-1)^{k+l}\binom{m+n-l-1}{m-l}\binom{n}{k+l} &= -(-1)^k\frac{(k+1)(m+n-1)}{n(k+m)}\binom{m+n-2}{m-1}\binom{n}{k+1}\\ &= -(-1)^k\frac{(m+n-1)!(n-1)!}{(k+m)(m-1)!(n-1)!k!(n-k-1)!}\\ &= -(-1)^k\frac{(m+n-1)!}{(k+m)!(n-k-1)!}\frac{(m+k-1)!}{(m-1)!k!}\\ &= -(-1)^k\binom{m+n-1}{m+k}\binom{m+k-1}{k}.\end{aligned}$$

Thus plugging this back into our equation for $Q(f,t)$, we have that

$$Q(f,q^{-n}t) = \sum_{m=0}^{\infty}\left(\binom{m+n-1}{m} + \sum_{k=1}^{n-1}(-1)^k\binom{m+n-1}{m+k}\binom{m+k-1}{k}q^{-k}\right)(t/q)^m$$
$$= \sum_{m=0}^{\infty}\left(\sum_{k=0}^{n-1}(-1)^k\binom{m+n-1}{m+k}\binom{m+k-1}{k}q^{-k}\right)(t/q)^m$$

and thus

$$Q(f,t) = \sum_{m=0}^{\infty} \left(\sum_{k=0}^{n-1} (-1)^k \binom{m+n-1}{m+k} \binom{m+k-1}{k} q^{(n-1)m-k} \right) t^m.$$

Thus the number of zeroes of $\prod_{i=1}^{n} x_i \mod \pi_K^m$ is

$$N_m = \sum_{k=0}^{n-1} (-1)^k \binom{m+n-1}{m+k} \binom{m+k-1}{k} q^{(n-1)m-k}.$$

Remark: At one step in our calculation we relied on Wolfram Alpha to evaluate a sum for us, so we technically haven't "proved" that this formula is correct. We will later come back to this example and independently prove that this calculation is correct.

While it took a couple pages to get the answer in a form that is useful to look at, in principle we had the answer as soon as we calculated the local zeta function, which took two lines. In general the local zeta function handles multiplication of functions much better than combinatorial arguments, motivating the following proposition.

Proposition 2.3.4. *Let $f, g_1, g_2, \ldots, g_k \in O_K[x_1, \ldots, x_n]$ be such that the local zeta function of f factors $Z(f,s) = \prod_{i=1}^{k} Z(g_i, s)$. Let $Q(f,t) = \sum_{m=0}^{\infty} N_m t^m$ and $Q(g_i,t) = \sum_{m=0}^{\infty} a_{i,m} t^m$. Then N_m obeys the recursive formula*

$$N_{m+1} = q^n N_m - \sum_{m_1+m_2+\ldots+m_k=m} q^n \prod_{i=1}^{k} \left(a_{i,m_i} - q^{-n} a_{i,m_i+1} \right).$$

Proof. By assumption and proposition 2.3.3, we have that

$$Q(f, q^{-n}t) \frac{t-1}{t} + \frac{1}{t} = Z(f,s) = \prod_{i=1}^{k} Z(g_i, s) = \prod_{i=1}^{k} \left(Q(g_i, q^{-n}t) \frac{t-1}{t} + \frac{1}{t} \right).$$

Evaluating the term on the left, we see that

$$Q(f, q^{-n}t) \frac{t-1}{t} + \frac{1}{t} = \sum_{m=0}^{\infty} (N_m - q^{-n} N_{m+1}) \left(\frac{t}{q^n} \right)^m$$

and similarly

$$Q(g_i, q^{-n}t)\frac{t-1}{t} + \frac{1}{t} = \sum_{m=0}^{\infty}(a_{i,m} - q^{-n}a_{i,m+1})\left(\frac{t}{q^n}\right)^m$$

for $i = 1, \ldots, k$. Equating coefficients of t^m, we then get that

$$N_{m+1} = q^n N_m - \sum_{m_1+m_2+\ldots+m_k=m} q^n \prod_{i=1}^{k} \left(a_{i,m_i} - q^{-n}a_{i,m_i+1}\right)$$

for each $m \geq 0$, with $N_0 = 1$. □

Thus if we already know the coefficients of $Q(g_i, t)$ for $i = 1, \ldots, k$, we can recursively solve for coefficients of $Q(f, t)$.

This was based only off of the zeta function equality, but what if we know a bit more. Suppose f is separable, so that we can write f as a product of polynomial functions f_i that depend on disjoint sets of independent variables. More precisely,

Corollary 2.3.5. *Suppose $f(\boldsymbol{x}) \in O_K[x_1, \ldots, x_n]$ is separable, so that $f(x_1, \ldots, x_n) = \prod_{i=1}^{k} f_i(x_{D_i+1}, x_{D_i+2}, \ldots, x_{D_i+d_i})$, where $d_i \in \mathbb{N}$, $D_i = \sum_{j=1}^{i-1} d_j$, and $d_1 + d_2 + \ldots + d_k = n$. So, each f_i is a polynomial in d_i independent variables. Let $Q(f, t) = \sum_{m=0}^{\infty} N_m t^m$ and $Q(f_i, t) = \sum_{m=0}^{\infty} N_{i,m} t^m$. Then N_m obeys the recursive formula*

$$N_{m+1} = q^n N_m - \sum_{m_1+m_2+\ldots+m_k=m} q^{nm-\sum d_i m_i} \prod_{i=1}^{k} \left(q^{d_i} N_{i,m_i} - N_{i,m_i+1}\right).$$

Proof. Let $\mathbf{x}^{(i)} = [x_{D_i+j}]_{j=1}^{d_i}$, so that f_i depends on the vector $\mathbf{x}^{(i)}$. Taking g_i to be the image of f_i in $O_K[x_1, \ldots, x_n]$, by Fubini's Theorem we then get that

$$\begin{aligned} Z(f, s) &= \int_{O_K^n} |f(\mathbf{x})|_K^s d\mu_K^n(\mathbf{x}) = \int_{O_K^n} \prod_{i=1}^{k} |f_i(\mathbf{x}^{(i)})|^s d\mu_K^n(\mathbf{x}) = \prod_{i=1}^{k} \int_{O_K^{d_i}} |f_i(\mathbf{x}^{(i)})|^s d\mu_K^{d_i}(\mathbf{x}^{(i)}) \\ &= \prod_{i=1}^{k} Z(f_i, s) = \prod_{i=1}^{k} Z(g_i, s). \end{aligned}$$

Consider the Poincaré series

$$Q(g_i, t) = \sum_{m=0}^{\infty} a_{i,m} t^m.$$

Then by proposition 2.3.4, we have that

$$N_{m+1} = q^n N_m - \sum_{m_1+m_2+\ldots+m_k=m} q^n \prod_{i=1}^{k} \left(a_{i,m_i} - q^{-n} a_{i,m_i+1}\right).$$

As the value of $g_i(\mathbf{x})$ only depends on d_i of it's variables, $n - d_i$ variables are free. Thus we get that $a_{i,m} = q^{(n-d_i)m} N_{i,m}$. Plugging this into our earlier formula, we then get that

$$N_{m+1} = q^n N_m - \sum_{m_1+m_2+\ldots+m_k=m} q^n \prod_{i=1}^{k} \left(q^{(n-d_i)m_i} N_{i,m_i} - q^{(n-d_i)(m_i+1)-n} N_{i,m_i+1}\right).$$

So, consider $q^n \prod_{i=1}^{k} \left(q^{(n-d_i)m_i} N_{i,m_i} - q^{(n-d_i)(m_i+1)-n} N_{i,m_i+1}\right)$. We can pull out a factor of $q^{(n-d_i)m_i}$ from each term in the product, so

$$q^n \prod_{i=1}^{k} \left(q^{(n-d_i)m_i} N_{i,m_i} - q^{(n-d_i)(m_i+1)-n} N_{i,m_i+1}\right) = q^n \prod_{i=1}^{k} q^{(n-d_i)m_i} \left(N_{i,m_i} - q^{-d_i} N_{i,m_i+1}\right).$$

As $n = \sum d_i$, we have that $q^n = q^{\sum d_i} = \prod q^{d_i}$. Thus we can distribute the q^n by multiplying each term in product by q^{d_i}, giving

$$q^n \prod_{i=1}^{k} q^{(n-d_i)m_i} \left(N_{i,m_i} - q^{-d_i} N_{i,m_i+1}\right) = \prod_{i=1}^{k} q^{(n-d_i)m_i} \left(q^{d_i} N_{i,m_i} - N_{i,m_i+1}\right).$$

Pulling the $q^{(n-d_i)m_i}$ out of the product, we then get that

$$\begin{aligned}\prod_{i=1}^{k} q^{(n-d_i)m_i} \left(q^{d_i} N_{i,m_i} - N_{i,m_i+1}\right) &= q^{n\sum m_i - \sum d_i m_i} \prod_{i=1}^{k} \left(q^{d_i} N_{i,m_i} - N_{i,m_i+1}\right) \\ &= q^{nm - \sum d_i m_i} \prod_{i=1}^{k} \left(q^{d_i} N_{i,m_i} - N_{i,m_i+1}\right).\end{aligned}$$

as $\sum m_i = m$. Thus we get that

$$N_{m+1} = q^n N_m - \sum_{m_1+m_2+\ldots+m_k=m} q^{nm-\sum d_i m_i} \prod_{i=1}^{k} \left(q^{d_i} N_{i,m_i} - N_{i,m_i+1}\right).$$

proving the corollary. □

In this special case, we can also derive the above formula using combinatorial methods. Suppose that $\mathbf{x} \in O_K^n$ is such that $f(\mathbf{x}) \equiv 0 \mod \pi_K^{m+1}$. Then necessarily $f(\mathbf{x}) \equiv 0 \mod \pi_K^m$. So as we count the number of points

$$\mathbf{x} + \pi_K^{m+1} O_K^n \in (O_K/\pi_K^{m+1} O_K)^n$$

such that $f(\mathbf{x}) \equiv 0 \mod \pi_K^{m+1}$, we need only consider those points such that $f(\mathbf{x}) \equiv 0 \mod \pi_K^m$.

Suppose there are N_m points $\mathbf{y} + \pi_K^m O_K^n \in (O_K/\pi_K^m O_K)^n$ with $f(\mathbf{y}) \equiv 0 \mod \pi_K^m$. For each fixed $\mathbf{y} + \pi_K^m O_K^n$, there are q^n distinct points $\mathbf{x} + \pi_K^{m+1} O_K^n \in (O_K/\pi_K^{m+1} O_K)^n$ with $\mathbf{x} \equiv \mathbf{y} \mod \pi_K^m$. Thus we have $q^n N_m$ candidates for the roots of $f \mod \pi_K^{m+1}$.

We now count the number of possible candidates which are NOT roots of $f \mod \pi_K^{m+1}$ using the fact that f is separable. As f_i depends only on d_i independent variables, define

$$N_{i,j} = \text{card}(\{\mathbf{z}^{(i)} + \pi_K^j O_K^{d_i} \in (O_K/\pi_K^j O_K)^{d_i} : f_i(\mathbf{z}^{(i)}) \equiv 0 \mod \pi_K^j\}).$$

For each $\mathbf{x} = [x_l]_{l=1}^n \in O_K^n$, define $\mathbf{x}^{(i)} = [x_{D_i+l}]_{l=1}^{d_i}$, where d_i, D_i are as in the statement of corollary 2.3.5. Then $|f(\mathbf{x})|_K = \prod_{i=1}^{k} |f_i(\mathbf{x}^{(i)})|_K$, we have that $f(\mathbf{x}) \equiv 0 \mod \pi_K^m$ if and only if there are are nonnegative integers m_i such that $f_i(\mathbf{x}^{(i)}) \equiv 0 \mod \pi_K^{m_i}$ for $i = 1, \ldots, k$ and $\sum_{i=1}^{k} m_i = m$. Thus if $f(\mathbf{x}) \equiv 0 \mod \pi_K^m$ but $f(\mathbf{x}) \not\equiv 0 \mod \pi_K^{m+1}$, then there are some $m_i \geq 0$ with $\sum_{i=1}^{k} m_i = m$ such that $f_i(\mathbf{x}^{(i)}) \equiv 0 \mod \pi_K^{m_i}$ but $f_i(\mathbf{x}^{(i)}) \not\equiv 0 \mod \pi_K^{m_i+1}$ for $i = 1, \ldots, k$.

The number of points $\mathbf{z}^{(i)} + \pi_K^{m_i+1} O_K^{d_i} \in (O_K/\pi_K^{m_i+1} O_K)^{d_i}$ such that $f_i(\mathbf{z}^{(i)}) \equiv 0 \mod \pi_K^{m_i}$ but $f_i(\mathbf{z}^{(i)}) \not\equiv 0 \mod \pi_K^{m_i+1}$ is $q^{d_i} N_{i,m_i} - N_{i,m_i+1}$. For each $\mathbf{z}^{(i)} + \pi_K^{m_i+1} O_K^{d_i} \in (O_K/\pi_K^{m_i+1} O_K)^{d_i}$, there are $q^{(m-m_i)d_i}$ points $\mathbf{x}^{(i)} + \pi_K^{m+1} O_K^{d_i} \in (O_K/\pi_K^{m+1} O_K)^{d_i}$ equivalent to it, giving $q^{(m-m_i)d_i}(q^{d_i} N_{i,m_i} - N_{i,m_i+1})$ choices for $\mathbf{x}^{(i)} + \pi_K^{m+1} O_K^{d_i}$ meeting our conditions. As we need this to be the case for each

$i = 1, \ldots, k$, this gives a total number

$$\prod_{i=1}^{k} q^{(m-m_i)d_i}(q^{d_i}N_{i,m_i} - N_{i,m_i+1}) = q^{m\sum d_i - \sum m_i d_i} \prod_{i=1}^{k}(q^{d_i}N_{i,m_i} - N_{i,m_i+1})$$
$$= q^{mn-\sum m_i d_i} \prod_{i=1}^{k}(q^{d_i}N_{i,m_i} - N_{i,m_i+1})$$

of $\mathbf{x}+\pi_K^{m+1}O_K^n \in (O_K/\pi_K^{m+1}O_K)^n$ such that $f_i(\mathbf{x}^{(i)}) \equiv 0 \mod \pi_K^{m_i}$ but $f_i(\mathbf{x}^{(i)}) \not\equiv 0 \mod \pi_K^{m_i+1}$ for $i = 1, \ldots, k$. Summing over all possibilities for m_i, we get that the total number of $\mathbf{x} + \pi_K^{m+1}O_K^n \in (O_K/\pi_K^{m+1}O_K)^n$ such that $f(\mathbf{x}) \equiv 0 \mod \pi_K^m$ but $f(\mathbf{x}) \not\equiv 0 \mod \pi_K^{m+1}$ is

$$\sum_{m_1+m_2+\ldots+m_k=m} q^{mn-\sum m_i d_i} \prod_{i=1}^{k} \left(q^{d_i}N_{i,m_i} - N_{i,m_i+1}\right)$$

thus giving the total number of points such that $f(\mathbf{x}) \equiv 0 \mod \pi^{m+1}$ as

$$N_{m+1} = q^n N_m - \sum_{m_1+m_2+\ldots+m_k=m} q^{mn-\sum m_i d_i} \prod_{i=1}^{k} \left(q^{d_i}N_{i,m_i} - N_{i,m_i+1}\right).$$

We end this thesis with an illustration of this recursive formula, applying it to $f(\mathbf{x}) = \prod_{i=1}^{n} x_i$. Then in this case, $N_{i,m_i} = d_i = 1$ for all $m_i \geq 0$, $i = 1, \ldots, n$. The recursive formula then simplifies to

$$N_{m+1} = q^n N_m - \sum_{m_1+m_2+\ldots+m_n=m} q^{mn-\sum m_i} \prod_{i=1}^{n}(q-1)$$
$$= q^n N_m - \binom{m+n-1}{m} q^{(n-1)m}(q-1)^n.$$

We now prove that $N_m = \sum_{k=0}^{n-1}(-1)^k \binom{m+n-1}{m+k}\binom{m+k-1}{k} q^{(n-1)m-k}$ by showing that it satisfies the recurrence relation. Now, as $q^{(n-1)m}(q-1)^n = q^{(n-1)m}\sum_{k=0}^{n}(-1)^k\binom{n}{k}q^{n-k} = q^{(n-1)(m+1)-1}\sum_{k=0}^{n}(-1)^k\binom{n}{k}q^{-k}$, we get that

$$q^n \sum_{k=0}^{n-1} (-1)^k \binom{m+n-1}{m+k} \binom{m+k-1}{k} q^{(n-1)m-k} - \binom{m+n-1}{m} q^{(n-1)m} (q-1)^n$$
$$= q^{(n-1)(m+1)} \left(q \sum_{k=0}^{n} (-1)^k \left(\binom{m+n-1}{m+k} \binom{m+k-1}{k} - \binom{m+n-1}{m} \binom{n}{k} \right) q^{-k} \right).$$

Note that when $k = n$, $\binom{m+n-1}{m+k} = 0$. Examining the middle term

$$\binom{m+n-1}{m+k} \binom{m+k-1}{k} - \binom{m+n-1}{m} \binom{n}{k}$$

we see that the $k = 0$ term is 0, and for each $0 < k < n$,

$$\begin{aligned}
&\binom{m+n-1}{m+k} \binom{m+k-1}{k} - \binom{m+n-1}{m} \binom{n}{k} \\
&\qquad = (m(n-k) - n(m+k)) \times \frac{(m+n-1)!}{m!k!(n-k)!(m+k)} \\
&\qquad = -\frac{(m+n)!}{m!(k-1)!(n-k)!(m+k)} = -\frac{(m+n)!(m+k-1)!}{m!(k-1)!(n-k)!(m+k)!} \\
&\qquad = -\binom{m+n}{m+k} \binom{m+k-1}{k-1}.
\end{aligned}$$

For $k = n$, we have that

$$\begin{aligned}
&\binom{m+n-1}{m+k} \binom{m+k-1}{k} - \binom{m+n-1}{m} \binom{n}{k} \\
&\qquad = -\binom{m+n-1}{m} = -\binom{m+n}{m+k} \binom{m+k-1}{k-1}.
\end{aligned}$$

So the equality holds for all $1 \leq k \leq n$. Plugging this back in, we get that

$$\begin{aligned}
&q^{(n-1)(m+1)} \left(q \sum_{k=0}^{n} (-1)^k \left(\binom{m+n-1}{m+k} \binom{m+k-1}{k} - \binom{m+n-1}{m} \binom{n}{k} \right) q^{-k} \right) \\
&\qquad = q^{(n-1)(m+1)} \left(q \sum_{k=1}^{n} (-1)^{k+1} \binom{m+n}{m+k} \binom{m+k-1}{k-1} q^{-k} \right).
\end{aligned}$$

Replacing our index k with $k+1$, we then have

$$\begin{aligned} & q^{(n-1)(m+1)} \left(q \sum_{k=1}^{n} (-1)^{k+1} \binom{m+n}{m+k} \binom{m+k-1}{k-1} q^{-k} \right) \\ &= q^{(n-1)(m+1)} \left(\sum_{k=0}^{n-1} (-1)^{k} \binom{m+n}{m+k+1} \binom{m+k}{k} q^{-k} \right) \\ &= \sum_{k=0}^{n-1} (-1)^{k} \binom{m+n}{m+k+1} \binom{m+k}{k} q^{(n-1)(m+1)-k}. \end{aligned}$$

But this is just our original term $\displaystyle\sum_{k=0}^{n-1} (-1)^{k} \binom{m+n-1}{m+k} \binom{m+k-1}{k} q^{(n-1)m-k}$ with now $m \to m+1$. Thus $\displaystyle\sum_{k=0}^{n-1} (-1)^{k} \binom{m+n-1}{m+k} \binom{m+k-1}{k} q^{(n-1)m-k}$ satisfies the recurrence relation, so we have that

$$N_m = \sum_{k=0}^{n-1} (-1)^{k} \binom{m+n-1}{m+k} \binom{m+k-1}{k} q^{(n-1)m-k}.$$

Bibliography

[1] J. Igusa. *An Introduction to the Theory of Local Zeta Functions*, American Mathematical Society and International Press, Providence, RI, 2000.

[2] D. Ramakrishnan and R. Valenza. *Fourier Analysis on Number Fields*, Springer-Verlag New York, Inc., New York, NY, 1999.

[3] A. N. Kolmogorov and S. V. Fomin. *Introductory Real Analysis*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1970.

[4] H. Weizsäcker. *Basic Mearure Theory* [PDF], `http://www.mathematik.uni-kl.de/~wwwstoch-alt/skripte/basicmeasuretheory_skript.pdf`

[5] P. Balachandran. *Product Measures - Fubini and Tonelli* [PDF], `http://math.bu.edu/people/prakashb/Math/241%20makeup%20lecture%20-%20fall%2008.pdf`

[6] V. Bogachev. *Measure Theory, Volume 1*, Springer-Verlag New York, Inc., New York, NY, 2007.

[7] M. Popa. *Chapter 3. p-Adic Integration* [PDF], `http://homepages.math.uic.edu/~mpopa/571/chapter3.pdf`

[8] E. Turner. *The P-Adic Numbers and Finite Extensions* [PDF], `http://www.math.uchicago.edu/~may/VIGRE/VIGRE2011/REUPapers/Turner.pdf`

[9] R. Singh and S. Maity. *Permutation Polynomials modulo p^n* [PDF], `https://eprint.iacr.org/2009/393.pdf`

Appendix A

Appendix

A.1 Extension to Manifolds

In this section, we develop the theory of K-analytic manifolds to the point that we can state and prove Serre's Theorem. As is the theme of this thesis, before we can say anything useful, we first need the proper language to talk about the structures we are interested. So without further ado,

Definition A.1.1. Let X be a Hausdorff topological space, and n be a fixed integer. Then we say that X is an n-dimensional K-manifold if X is locally homeomorphic to K^n. That is, if for any point $x \in X$, there is a neighborhood $U \subseteq X$ of x and a homeomorphism ϕ_U from U to an open subset $\phi_U(U)$ of K^n. We then write $\dim(X) = n$.

Roughly speaking, an n-dimensional K-manifold is a topological space that at every point resembles K^n topologically. But as we have shown throughout this thesis, p-adic fields contain much more than just topological structure, so in order to really resemble K^n we need more requirements.

Definition A.1.2. Let X be an n-dimensional K-manifold. A chart is a pair (U, ϕ_U) where U is a nonempty open subset of X and ϕ_U is a homeomorphism from U to an open subset $\phi_U(U)$ of K^n. An atlas on X is a collection of charts $\{(U, \phi_U)\}$ such that the union of all U is X, and for every U, U' such that $U \cap U' \neq \emptyset$, the map

$$\phi_{U'} \circ \phi_U^{-1} : \phi_U(U \cap U') \to \phi_{U'}(U \cap U')$$

is a K-analytic map. Two atlases are considered equivalent if their union is also an atlas. An n-dimensional K-manifold X along with an equivalence class of atlases is called an n-dimensional K-analytic manifold.

Clearly, for any open set $U \subseteq K^n$, we have that U is an n-dimensional K-analytic manifold defined by the single chart (U, ϕ_U), where ϕ_U is the inclusion map $x \to x$.

A less trivial example is the projective line $P^1(K)$, which may be defined as the set of one dimensional subspaces of K^2, i.e. as the collection of lines in K^2 passing through the origin. More precisely, the projective line is the collection of homogenous points $P^1(K) = \{(x : y)\}$, where $x, y \in K$ and at least one of x, y is nonzero, and $(x : y) = (\lambda x : \lambda y)$ for all $\lambda \neq 0$. We can identify $P^1(K)$ with the compactification of K, $\overline{K} = K \cup \{\infty\}$, by $(x : y) \to \dfrac{x}{y}$ whenever $y \neq 0$, and $(1 : 0) \to \infty$. Taking $U = \{(x : y) : |x|_K \leq |y|_K\}$ and $V = \{(x : y) : |x|_K > |y|_K\}$, we have that the projective line $P^1(K)$ is the disjoint union of the two open sets U, V. Both U and V are homeomorphic to O_K, with respective homeomorphisms $(x : y) \to \dfrac{x}{y}$, and $(x : y) \to \pi_K^{-1}\dfrac{y}{x}$. Thus $P^1(K)$ is a 1-dimensional K-analytic manifold.

The addition of an atlas $\{(U, \phi_U)\}$ allows us to define analytical/differential structures on X.

Definition A.1.3. Let X, Y be K-analytic manifolds, and $f : X \to Y$ be a map. Then we say that f is a K-analytic map if for any charts $(U, \phi_U), (V, \psi_V)$ such that $U \cap f^{-1}(V) \neq \emptyset$, then the map

$$\psi_V \circ f \circ \phi_U^{-1} : \phi_U(U \cap f^{-1}(V)) \to K^{dim(Y)}$$

is K-analytic. If $Y = K$, then we call f a K-analytic function. If f is a bijection and f^{-1} is a K-analytic map as well, then we say that f is bianalytic and that X is bianalytic to Y.

We now set about to define K-analytic differential forms on an n-dimensional K-analytic manifold X. Let a be an arbitrary point of X, and U, V be neighborhoods of a. If f, g are K-analytic functions defined on U, V respectively, we say that f and g are equivalent at a if there is a neighborhood $W \subseteq U \cap V$ such that $f|_W = g|_W$. This is an equivalence relation on analytic functions defined on a neighborhood of a. Let $\mathcal{O}_a$ be the set of equivalences classes of functions equivalent at a. As an abuse of notation, we refer to the equivalence class of f as f as well. $\mathcal{O}_a$ is a commutative ring, with addition $(f, g) \to f + g$ and multiplication $(f, g) \to fg$. Note that the value $f(a)$ is well defined for any equivalence class of functions f.

Definition A.1.4. Define the tangent space $T_a(X)$ of X at a as the K-vector space of K-linear maps $\partial : \mathcal{O}_a \to K$ satisfying the product rule

$$\partial(fg) = \partial(f)g(a) + f(a)\partial(g)$$

for all $f, g \in \mathcal{O}_a$. Denote the dual space of $T_a(X)$ by $\Omega_a(X)$.

Now, let (U, ϕ_U) be a chart of X with $\phi_U(x) = [x_i(x)]_{i=1}^n$. For each $a \in U$, $T_a(X)$ has $\{(\frac{\partial}{\partial x_j})_a : j = 1, \ldots, n\}$, where $(\frac{\partial}{\partial x_j})_a(f) = \frac{\partial(f \circ \phi_U^{-1})}{\partial x_j}(a)$. Then every element of $\partial' \in T_a(X)$ can be written uniquely as $\partial' = \sum_{j=1}^{n} (\frac{\partial}{\partial x_j})_a \partial' x_j$. Let $\{(dx_i)_a : i = 1, \ldots, n\}$ be the dual basis of $\{(\frac{\partial}{\partial x_j})_a\}$ in $\Omega_a(X)$, i.e. the basis defined by the property that

$$(dx_i)_a \left((\frac{\partial}{\partial x_j})_a \right) = \delta_{i,j}.$$

For any $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$, define

$$(dx_{i_1} \wedge dx_{i_2} \wedge \ldots \wedge dx_{i_k})_a = \sum_{\sigma \in S_k} (-1)^{p(\sigma)} (dx_{i_{\sigma(1)}} \otimes dx_{i_{\sigma(2)}} \otimes \ldots \otimes dx_{i_{\sigma(k)}})_a$$

where S_k is the set of permutations of 1 through k, $p(\sigma) = \begin{cases} 1, & \sigma \text{ odd} \\ 0, & \sigma \text{ even} \end{cases}$ is the parity of σ, and $(dx_{j_1} \otimes dx_{j_2} \otimes \ldots \otimes dx_{j_k})_a : T_a(X)^k \to K$ is defined by $(dx_{j_1} \otimes dx_{j_2} \otimes \ldots \otimes dx_{j_k})_a(f_1, \ldots, f_k) = \prod_{i=1}^{k} (dx_{j_i})_a(f_i)$. Then the set

$$\{(dx_{i_1} \wedge dx_{i_2} \wedge \ldots \wedge dx_{i_k})_a : 1 \leq i_1 < i_2 < \ldots < i_k \leq n\}$$

forms a basis for the space of alternating k-linear maps from $T_a(X)^k \to K$.

Definition A.1.5. We say that α is a differential form of degree k on X if for each $x \in X$, $\alpha(x) : T_x(X)^k \to K$ is an alternating k-linear map.

Then for each chart (U, ϕ_U), let $dx_{i_1} \wedge dx_{i_2} \wedge \ldots \wedge dx_{i_k}$ denote the differential k-form defined by $dx_{i_1} \wedge dx_{i_2} \wedge \ldots \wedge dx_{i_k}(a) = (dx_{i_1} \wedge dx_{i_2} \wedge \ldots \wedge dx_{i_k})_a$. Then locally on U we may write

$$\alpha(x) = \sum_{1 \leq i_1 < \ldots < i_k \leq n} f_{U, i_1, \ldots, i_k}(x) dx_{i_1} \wedge dx_{i_2} \wedge \ldots \wedge dx_{i_k}(x)$$

where $f_{U, i_1, \ldots, i_k}$ is a K-valued function on X.

Definition A.1.6. We say that α is a K-analtyic differential form of degree k if for each chart (U, ϕ_U) and $1 \leq i_1 < \ldots < i_k \leq n$, the function $f_{U, i_1, \ldots, i_k}(x)$ is a K-analytic function.

We are particularly interested in K-analytic differential forms of degree n. These functions are locally of the form

$$\alpha(x) = f_U(x)dx_1 \wedge dx_2 \wedge \ldots \wedge dx_n.$$

We say that α is a gauge if $f_U(x) \neq 0$ for all $x \in U$ and charts (U, ϕ_U) in our atlas.

Given a K-analytic differential form α on X of degree n, we can use it to define a measure on X.

Definition A.1.7. Let X be a K-analytic manifold of degree n, and α a K-analytic differential form of degree n with

$$\alpha(x) = f_U(x)dx_1 \wedge dx_2 \wedge \ldots \wedge dx_n$$

for each chart (U, ϕ_U). Then for any Borel set of X $A \subseteq U$, define

$$\begin{aligned}\mu_\alpha(A) &= \int_A |f_U(x)|_K d\mu_K^n(\phi_U(x)) \\ &= \sum_{e\in\mathbb{Z}} q^{-e}\mu_K^n(\{\phi_U(f^{-1}(\pi_K^e O_K \setminus \pi_K^{e+1}O_K) \cap A)\}).\end{aligned}$$

Given any compact set $A \subseteq X$, we have that $A \subseteq \bigcup_{i=1}^{m} U_i$ for some charts (U_i, ϕ_{U_i}). Taking $A_1 = A \cap U_1$, and $A_i = (A \cap U_i) \setminus (\bigcup_{j=1}^{i-1} A_j)$, we then define $\mu_\alpha(A) = \sum_{i=1}^{m} \mu_\alpha(A_i)$. Extending μ_α by inner regularity to all open sets and then by outer regularity to all Borel sets, this defines a Borel measure on X.

See Section 7.4 of [1] for details and proof that this is well defined, and independent of our choice of atlas.

Finally, we can use differential forms on one manifold can be used to induce differential forms on another.

Definition A.1.8. Let X, Y be n-dimensional K-analytic manifolds, β be a K-analytic differential form of degree n on Y, and $f : X \to Y$ be a K-analytic map. Let $(U, \phi_U), (V, \psi_V)$ be charts of X, Y respectively with $\phi_U(x) = [x_i(x)]_{i=1}^n$, $\psi_V(y) = [y_j(y)]_{j=1}^n$, and $f(U) \subseteq V$. Then define $f^*(\beta)$ the pullback of β by f as

$$f^*(\beta)(x) = g_V(f(x))\frac{\partial(y_1, \ldots, y_n)}{\partial(x_1, \ldots, x_n)}dx_1 \wedge \ldots \wedge x_n$$

where $\dfrac{\partial(y_1, \ldots, y_n)}{\partial(x_1, \ldots, x_n)} = \det\left[\dfrac{\partial(\psi_V \circ f \circ \phi_U^{-1})_j}{\partial x_i}\right]_{i,j=1}^n$

A.1.1 Serre's Theorem

Lemma A.1.9. *Let K be a p-adic field and $n \in \mathbb{N}$. Then any compact, open subset of K^n is the finite union of disjoint open balls.*

Proof. The metric on K^n is induced by the non-Archimedean norm $|\cdot|_K$. Thus the metric on K^n is an ultra metric, so any intersecting open balls must have one ball contained within the other. Now, given any compact open set $A \subset K^n$, for each $x \in A$ there is an open ball B_x such that $x \in B_x \subseteq A$. As $\{B_x : x \in A\}$ is an open cover of A, there is a finite subcover $B_1, \ldots, B_m$. Discarding all balls strictly contained in a larger ball, and any repeats of the same set, we then have an open cover of disjoint balls. Thus A is the union of finitely many disjoint open balls. □

Theorem A.1.10. *Let K be a p-adic field, and X a compact n-dimensional K-analytic manifold for some $n \in \mathbb{N}$. Then X is bianalytic to the disjoint union $r \circ O_K^n$ of r copies of O_K^n for some $0 < r < q$.*

Proof. Take an atlas $\{(U, \phi_U)\}$ on X. As the topology on X is generated by its compact open subsets, we may assume each U is compact and open. As X is compact, it is covered by finitely many U's, $U_1, U_2, \ldots$. Taking $V_i = U_i \setminus \bigcup_{j=1}^{i-1} U_j$, we have that X is covered by finitely many disjoint, open, compact subsets V_i, each homeomorphic to a compact open subset of K^n. Taking $\phi_i = \phi_{U_i}|_{V_i}$, by the previous lemma we have that for each i, $\phi_i(V_i)$ is the union of finitely many disjoint sets of the form $a + \pi^e O_K^n$ for some $a \in K^n$ and $e \in \mathbb{Z}$. As O_K^n is bianalytic to $a + \pi^e O_K^n$ by $x \to a + \pi^e x$, we have that X is bianalytic to $r' \circ O_K^n$ for some $r' \in \mathbb{N}$. If $\{c_1, \ldots, c_q\}$ is a class of representations mod π, then O_K is the disjoint union of $c_i + \pi O_K$ for $i = 1, \ldots, q$. Thus $O_K^n = O_K^{n-1} \times O_K$ is bianalytic to $q \circ O_K^n$. Thus writing $r' = (q-1)j + r$ where $0 < r < q$, then we see that X is K-bianalytic to $r \circ O_K^n$.

□

Theorem A.1.11. *Serre's Theorem*
Suppose K is a p-adic field, and X a compact n-dimensional K-analytic manifold. Then X possess a gauge form α and $\mu_\alpha(X)$ is of the form N/q^m for some $m, N \in \mathbb{N}$. Define $0 < i(X) < q$ in $\mathbb{N}$ by $\mu_\alpha(X) - i(X) \in (q-1)\mathbb{Z}[1/q]$. Then $i(X)$ is independent of α, and X is K-bianalytic to $i(X) \circ O_K^n$. Further, X is K-bianalytic to another compact n-dimensional K-analytic manifold Y if and only if $i(X) = i(Y)$.

Proof. By the previous theorem, we have that X is bianalytic to $r \circ O_K^n$ for some $0 < r < q$. Taking $Y = r \circ O_K^n$, we have that X and Y are K-bianaltyic, and let $f : X \to Y$ be a fixed bianalytic map. Define the gauge form β on Y by

$\beta(y) = dy_1 \wedge dy_2 \wedge \ldots \wedge dy_n$ on each copy of O_K^n. Let V_i be the preimage under f of the i'th copy of O_K^n, and $\phi_i = f|_{V_i}$. Define α to be the pullback of β by f on X, i.e. $\alpha(x) = f^*(\beta)(x) = \dfrac{\partial(y_1, \ldots, y_n)}{\partial(x_1, \ldots, x_n)} dx_1 \wedge dx_2 \wedge \ldots \wedge dx_n$, where $x_1, \ldots, x_n$ are the local coordinates of x in V_i under ϕ_i. As V_i is bianalytic to O_K^n, we have that $\dfrac{\partial(y_1, \ldots, y_n)}{\partial(x_1, \ldots, x_n)} \neq 0$ for all $x \in V_i$. Thus α is a gauge form on X. Then by the change of variables formula

$$\mu_\alpha(X) = \sum_{i=1}^{r} \int_{V_i} \left|\frac{\partial(y_1, \ldots, y_n)}{\partial(x_1, \ldots, x_n)}\right|_K d\mu_K^n(\phi_i(x)) = \sum_{i=1}^{r} \int_{O_K^n} d\mu_K^n(x) = r.$$

Now, given an additional gauge form α' on X, take an atlas $\{(U, \phi_U)\}$ with $\phi_U(x) = (x_1, \ldots, x_n)$ such that $\alpha(x) = f_U(x) dx_1 \wedge dx_2 \wedge \ldots \wedge dx_n$ and $\alpha'(x) = g_U(x) dx_1 \wedge dx_2 \wedge \ldots \wedge dx_n$. Taking $F_U = |f_U|_K$, we have that $F_U^{-1}(\{q^m\})$ is open for each U and $m \in \mathbb{Z}$. As this is likewise true for each $|g_U|_K$, we can subdivide each U so that $|f_U(x)|_K = q^{e_U}$ and $|g_U(x)|_K = q^{e'_U}$ for some e_U, e'_U independent of $x \in U$. Then by the same process as outlined in the previous theorem, we can reduce this atlas to finitely many compact open disjoint $U's$. Thus $\mu_{\alpha'}(X) = \sum_U q^{e'_U} \mu_n(\phi_U(U))$. As $\phi_U(U)$ is a compact open subset of K^n, it is a disjoint union of finitely many open balls and thus $\mu_n(\phi_U(U))$ is a sum of finitely many elements of $q^{\mathbb{Z}}$. Thus $\mu_{\alpha'}(X) = N/q^m$ form some $m, N \in \mathbb{N}$. Taking $i(X) = r$, we get that

$$\mu_{\alpha'}(X) - i(X) = \mu_{\alpha'}(X) - r = \mu_{\alpha'}(X) - \mu_\alpha(X) = \sum_U (q^{e'_U} - q^{e_U}) \mu_n(\phi_U(U))$$

As $(q^{e'_U} - q^{e_U})$ is divisible by $(q-1)$ for each U, the sum is as well and thus $\mu_{\alpha'}(X) - i(X) \in (q-1)\mathbb{Z}[1/q]$

Now, let X and Y be n-dimensional K-analytic manifolds. It suffices to show that X is bianaltyic to $r' \circ O_K^n$ for $0 < r' < q$ if and only if $r' = r = i(X)$. If X is bianaltyic to $r' \circ O_K^n$, then through the same process as above we can construct a gauge form α' such that $\mu_{\alpha'}(X) = r'$. But then we have that $\mu_{\alpha'}(X) - r = \mu_{\alpha'}(X) - \mu_\alpha(X) \in (q-1)\mathbb{Z}[1/q]$. Thus as r, r' are integers, we must have that $r' - r$ is divisible by $q - 1$. As $0 < r, r' < q$, we then have that $r = r'$.

□

A.2 Local Zeta Function Calculation

Let $f(x,y) = (xy)^d(x+y)^e$, and consider the local zeta function of f,

$$Z(f,s) = \int\limits_{O_K^2} |(xy)^d(x+y)^e|_K^s d\mu_K^2(x,y).$$

For any $x, y \in O_K$, there are three basic scenarios: either $|x|_K > |y|_K, |x|_K < |y|_K$, or $|x|_K = |y|_K$. Thus we can break up our integral into three parts,

$$\int\limits_{O_K^2} |f|_K^s d\mu_K^2(x,y) = \int\limits_{|x|_K>|y|_K} |x|_K^{ds}|y|_K^{ds}|x+y|_K^{es} d\mu_K^2(x,y) + \int\limits_{|x|_K<|y|_K} |x|_K^{ds}|y|_K^{ds}|x+y|_K^{es} d\mu_K^2(x,y) + \int\limits_{|x|_K=|y|_K} |x|_K^{ds}|y|_K^{ds}|x+y|_K^{es} d\mu_K^2(x,y).$$

By the symmetry of x and y, we have that the first two parts are the same. Furthermore, $|x|_K > |y|_K$ implies $|x+y|_K = |x|_K$. Thus we get that

$$\int\limits_{O_K^2} |f|_K^s d\mu_K^2(x,y) = 2\int\limits_{|x|_K>|y|_K} |x|_K^{(d+e)s}|y|_K^{ds} d\mu_K^2(x,y) + \int\limits_{|x|_K=|y|_K} |x|_K^{ds}|y|_K^{ds}|x+y|_K^{es} d\mu_K^2(x,y).$$

Finally, there are two distinct cases when $|x|_K = |y|_K$; either $|x+y|_K = |x|_K = |y|_K$, or $|x+y|_K < |x|_K, |y|_K$. Thus we have that

$$\int\limits_{O_K^2} |f|_K^s d\mu_K^2(x,y) = 2\int\limits_{|x|_K>|y|_K} |x|_K^{(d+e)s}|y|_K^{ds} d\mu_K^2(x,y) + \int\limits_{|x+y|_K=|x|_K=|y|_K} |x|^{(2d+e)s} d\mu_K^2(x,y) + \int\limits_{|x+y|_K<|x|_K=|y|_K} |x|_K^{2ds}|x+y|_K^{es} d\mu_K^2(x,y).$$

Using Fubini's theorem, we then have that our first integral

$$\int\limits_{|x|_K>|y|_K} |x|_K^{(d+e)s}|y|_K^{ds} d\mu_K^2(x,y) = \int\limits_{O_K} |x|_K^{(d+e)s} \left(\int\limits_{|x|_K>|y|_K} |y|_K^{ds} d\mu_K(y) \right) d\mu_K(x).$$

Breaking down the x integral into the different level sets $\pi_K^m O_K \setminus \pi_K^{m+1} O_K$ and

summing them up, we get that

$$\begin{aligned}\int\limits_{|x|_K>|y|_K} |x|_K^{(d+e)s}|y|_K^{ds}d\mu_K^2(x,y) &= \sum_{m=0}^{\infty} \int\limits_{\pi_K^m O_K\setminus\pi_K^{m+1}O_K} |x|_K^{(d+e)s}\left(\int\limits_{\pi_K^{m+1}O_K} |y|_K^{ds}d\mu_K(y)\right)d\mu_K(x)\\ &= \sum_{m=0}^{\infty} q^{-m(d+e)s}\mu_K(\pi_K^m O_K\setminus\pi_K^{m+1}O_K)\int\limits_{\pi_K^{m+1}O_K}|y|_K^{ds}d\mu_K(y)\\ &= \sum_{m=0}^{\infty} q^{-m(d+e)s}\frac{q-1}{q^{m+1}}\int\limits_{\pi_K^{m+1}O_K}|y|_K^{ds}d\mu_K(y).\end{aligned}$$

By making the change of variables $y'=\pi_K^{-(m+1)}y$, we get that the inner integral is

$$\begin{aligned}\int\limits_{\pi_K^{m+1}O_K}|y|_K^{ds}d\mu_K(y) &= \int\limits_{O_K}|\pi_K^{m+1}y'|_K^{ds}d\mu_K(\pi_K^{m+1}y') = \int\limits_{O_K}|\pi_K^{m+1}y'|_K^{ds}|\pi_K^{m+1}|_K d\mu_K(y')\\ &= q^{-(m+1)(ds+1)}\int\limits_{O_K}|y'|_K^{ds}d\mu_K(y') = q^{-(m+1)(ds+1)}\frac{q-1}{q-q^{-ds}}.\end{aligned}$$

Thus we get that

$$\begin{aligned}\int\limits_{|x|_K>|y|_K}|x|_K^{(d+e)s}|y|_K^{ds}d\mu_K^2(x,y) &= \sum_{m=0}^{\infty}q^{-m(d+e)s}\frac{q-1}{q^{m+1}}\int\limits_{\pi_K^{m+1}O_K}|y|_K^{ds}d\mu_K(y)\\ &= \sum_{m=0}^{\infty}q^{-m(d+e)s}\frac{q-1}{q^{m+1}}\left(q^{-(m+1)(ds+1)}\frac{q-1}{q-q^{-ds}}\right)\\ &= \frac{q^{-ds}(q-1)^2}{q^2(q-q^{-ds})}\sum_{m=0}^{\infty}(q^{-((2d+e)s+2)})^m\\ &= \frac{q^{-ds}(q-1)^2}{q^2(q-q^{-ds})(1-q^{-((2d+e)s+2)})}\\ &= \frac{q^{-ds}(q-1)^2}{(q-q^{-ds})(q^2-q^{-(2d+e)s})}.\end{aligned}$$

Now for the second integral where $|x|_K = |y|_K = |x+y|_K$, we see that

$$\int\limits_{|x+y|_K=|x|_K=|y|_K} |x|_K^{(2d+e)s} d\mu_K^2(x,y) = \int\limits_{O_K} |x|_K^{(2d+e)s} \left(\int\limits_{|y|_K=|x+y|_K=|x|_K} d\mu_K(y) \right) d\mu_K(x)$$
$$= \int\limits_{O_K} |x|_K^{(2d+e)s} \mu_K(\{y : |y|_K = |x+y|_K = |x|_K\}) d\mu_K(x).$$

We can then break down the x integral and sum over the level sets $\pi_K^m O_K \setminus \pi_K^{m+1} O_K$. Thus

$$\int\limits_{|x+y|_K=|x|_K=|y|_K} |x|_K^{(2d+e)s} d\mu_K^2(x,y)$$
$$= \sum_{m=0}^{\infty} \int\limits_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} |x|_K^{(2d+e)s} \mu_K(\{y : |y|_K = |x+y|_K = |x|_K\}) d\mu_K(x)$$
$$= \sum_{m=0}^{\infty} q^{-m(2d+e)s} \int\limits_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} \mu_K(\{y : |y|_K = |x+y|_K = q^{-m}\}) d\mu_K(x).$$

Fix some $x \in \pi_K^m O_K \setminus \pi_K^{m+1} O_K$; then $x = \sum_{i=m}^{\infty} a_i \pi_K^i$ for some $a_i \in S$ with $a_m \neq 0$. Now, $|y|_K = q^{-m}$ implies $y = \sum_{i=m}^{\infty} b_i \pi_K^i$ for some $b_i \in S$ with $b_m \neq 0$. Then $|y|_K = |x+y|_K = q^{-m}$ implies that $a_m + b_m \notin \pi_K O_K$. Thus $b_m \not\equiv 0, -a_m \mod \pi_K$, so there are $q-2$ choices for b_m in S. As any b_i for $i > m$ is irrelevant, we then have that $\mu_K(\{y : |y|_K = |x+y|_K = q^{-m}\}) = (q-2)\mu_K(\pi_K^{m+1} O_K) = (q-2)q^{-(m+1)}$. Thus

$$\int\limits_{|x+y|_K=|x|_K=|y|_K} |x|_K^{(2d+e)s} d\mu_K^2(x,y) = \sum_{m=0}^{\infty} q^{-m(2d+e)s}(q-2)q^{-(m+1)} \int\limits_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} d\mu_K(x)$$
$$= \sum_{m=0}^{\infty} q^{-m(2d+e)s}(q-2)q^{-(m+1)}(q-1)q^{-(m+1)}$$
$$= \frac{(q-1)(q-2)}{q^2} \sum_{m=0}^{\infty} (q^{-((2d+e)s+2)})^m = \frac{(q-1)(q-2)}{q^2 - q^{-(2d+e)s}}.$$

And finally for the third integral where $|x|_K = |y|_K > |x+y|_K$, by breaking it up into the x-level sets we get that

$$\begin{aligned}\int\limits_{|x+y|_K<|x|_K=|y|_K} |x|_K^{2ds}|x+y|_K^{es}d\mu_K(x,y) &= \int\limits_{O_K} |x|_K^{2ds}\left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^{es}d\mu_K(y)\right)d\mu_K(x)\\ &= \sum_{m=0}^{\infty}\int\limits_{\pi_K^m O_K\setminus\pi_K^{m+1}O_K} |x|_K^{2ds}\left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^{es}d\mu_K(y)\right)d\mu_K(x)\\ &= \sum_{m=0}^{\infty} q^{-2mds}\int\limits_{\pi_K^m O_K\setminus\pi_K^{m+1}O_K}\left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^{es}d\mu_K(y)\right)d\mu_K(x).\end{aligned}$$

Now, given a fixed $x \in \pi_K^m O_K \setminus \pi_K^{m+1}O_K$, we have that $x = \sum_{i=m}^{\infty} a_i\pi_K^i$ for some $a_i \in S$ with $a_m \neq 0$. Thus there are $q-1$ choices for a_m. As $|y|_K = |x|_K$, we also have that $y = \sum_{i=m}^{\infty} b_i\pi_K^i$ for some $b_i \in S$ with $b_m \neq 0$. As we need $|x+y|_K < |x|_K, |y|_K$, that means that we must have $a_m + b_m \in \pi_K O_K$. As there is only one element in S such that $x \equiv -a_m \mod \pi_K$, we have that b_m has a fixed value. All other coefficients are arbitrary, so we get that

$$\int\limits_{\pi_K^m O_K\setminus\pi_K^{m+1}O_K}\left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^{es}d\mu_K(y)\right)d\mu_K(x) = (q-1)\int\limits_{\pi_K^{m+1}O_K^2} |x+y|_K^{es}\mu_K^2(x,y).$$

Making the change of variables $x' = \pi_K^{-(m+1)}x$ and $y' = \pi_K^{-(m+1)}y$, we get that

$$\begin{aligned}\int\limits_{\pi_K^{m+1}O_K^2} |x+y|_K^{es}d\mu_K^2(x,y) &= \int\limits_{O_K^2} |\pi_K^{m+1}(x'+y')|_K^{es}d\mu_K(\pi_K^{m+1}x',\pi_K^{m+1}y')\\ &= q^{-(m+1)(es+2)}\int\limits_{O_K^2} |x'+y'|_K^{es}d\mu_K(x',y') = q^{-(m+1)(es+2)}\frac{q-1}{q-q^{-es}}.\end{aligned}$$

Thus

$$\int\limits_{|x+y|_K<|x|_K=|y|_K} |x|_K^{2ds}|x+y|_K^{es}d\mu_K(x,y)$$

$$= \sum_{m=0}^{\infty} q^{-2mds} \int\limits_{\pi_K^m O_K \setminus \pi_K^{m+1} O_K} \left(\int\limits_{|x+y|_K<|x|_K=|y|_K} |x+y|_K^{es} d\mu_K(y) \right) d\mu_K(x)$$

$$= \sum_{m=0}^{\infty} q^{-2mds}(q-1)q^{-(m+1)(es+2)} \frac{q-1}{q-q^{-es}}$$

$$= \frac{q^{-es}(q-1)}{q^2(q-q^{-es})} \sum_{m=0}^{\infty} (q^{-((2d+e)s+2)})^m$$

$$= \frac{q^{-es}(q-1)^2}{(q-q^{-es})(q^2-q^{-(2d+e)s})}.$$

Summing up the results of those three integrals, we have that our initial integral

$$\int\limits_{O_K^2} |f|_K^s d\mu_K^2(x,y) = 2 \int\limits_{|x|_K>|y|_K} |x|_K^{(d+e)s}|y|_K^{ds} d\mu_K^2(x,y) + \int\limits_{|x+y|_K=|x|_K=|y|_K} |x|^{(2d+e)s} d\mu_K^2(x,y)$$

$$+ \int\limits_{|x+y|_K<|x|_K=|y|_K} |x|_K^{2ds}|x+y|_K^{es} d\mu_K^2(x,y)$$

$$= 2\frac{q^{-ds}(q-1)^2}{(q-q^{-ds})(q^2-q^{-(2d+e)s})} + \frac{(q-1)(q-2)}{q^2-q^{-(2d+e)s}} + \frac{q^{-es}(q-1)^2}{(q-q^{-es})(q^2-q^{-(2d+e)s})}$$

$$= \frac{(q-1)((1-2q)q^{-(d+e)s} + (q^2)q^{-ds} + (q)q^{-es} + q^3 - 2q^2)}{(q-q^{-ds})(q-q^{-es})(q^2-q^{-(2d+e)s})}.$$

Thus $Z(f,s) = \dfrac{(q-1)((1-2q)q^{-(d+e)s} + (q^2)q^{-ds} + (q)q^{-es} + q^3 - 2q^2)}{(q-q^{-ds})(q-q^{-es})(q^2-q^{-(2d+e)s})}.$