

CHAPTER 3. p -ADIC INTEGRATION

CONTENTS

1. Basics on p -adic fields	1
2. p -adic integration	5
3. Integration on K -analytic manifolds	8
4. Igusa's theorem on the rationality of the zeta function	15
5. Weil's measure and the relationship with rational points over finite fields	19
References	22

The aim of this chapter is to set up the theory of p -adic integration to an extent which is sufficient for proving Igusa's theorem [Ig] on the rationality of the p -adic zeta function, and Weil's interpretation [We1] of the number of points of a variety over a finite field as a p -adic volume, in case this variety is defined over the ring of integers of a p -adic field. After recalling a few facts on p -adic fields, I will introduce p -adic integrals, both in the local setting and with respect to a global top differential form on a K -analytic manifold. I will explain Igusa's proof of the rationality of the zeta function using Hironaka's resolution of singularities in the K -analytic case, and the change of variables formula. Weil's theorem on counting points over finite fields via p -adic integration will essentially come as a byproduct; it will be used later in the course to compare the number of rational points of K -equivalent varieties.

1. BASICS ON p -ADIC FIELDS

We will first look at different approaches to constructing the p -adic integers \mathbf{Z}_p and the p -adic numbers \mathbf{Q}_p , as well as more general rings of integers in p -adic fields, and recall some of their basic properties. I highly recommend [Ne] Chapter II for a detailed discussion of this topic.

p -adic numbers. Let p be a prime, and $x \in \mathbf{Q}$. One can write uniquely $x = p^m \cdot \frac{a}{b}$ with $m \in \mathbf{Z}$ and a and b integers not divisible by p . We define the *order* and the *norm* of x with respect to p as

$$\text{ord}_p(x) := m \quad \text{and} \quad |x|_p := \frac{1}{p^m}.$$

This norm on \mathbf{Q} is an example of the following general concept:

Definition 1.1. Let K be a field. A *non-archimedean absolute value* on K is a map $|\cdot| : K \rightarrow \mathbf{R}_{\geq 0}$ satisfying, for all $x, y \in K$, the following properties:

- (i) $|x| \geq 0$ for all x , and $|x| = 0$ if and only if $x = 0$.
- (ii) $|xy| = |x| \cdot |y|$.
- (iii) $|x + y| \leq \max \{|x|, |y|\}$.

If we consider the mapping $d(x, y) := |x - y|$, then this is a (non-archimedean) distance function (or metric), which in turn induces a topology on K .

Definition 1.2. The field of *p-adic numbers* \mathbf{Q}_p is the completion of the topological space \mathbf{Q} in the norm $|\cdot|_p$, i.e. the set of equivalence classes of all Cauchy sequences with respect to this norm.¹ Note that \mathbf{Q}_p is a field of characteristic 0.

It is standard to see that every $x \in \mathbf{Q}_p$ has a unique “Laurent series (base p) expansion”, namely a representation of the form

$$(1) \quad x = a_m p^m + a_{m+1} p^{m+1} + \dots$$

where $m = \text{ord}_p(x) \in \mathbf{Z}$ and $a_i \in \{0, 1, \dots, p-1\}$ for all i .

Exercise 1.3. Check that in \mathbf{Q}_p one has:

- (i) $\frac{1}{1-p} = 1 + p + p^2 + \dots$
- (ii) $-1 = (p-1) + (p-1)p + (p-1)p^2 + \dots$

Exercise 1.4. Show that \mathbf{Q}_p is a totally disconnected, locally compact topological space.

Definition 1.5. The *ring of p-adic integers* \mathbf{Z}_p is the unit disk in the space \mathbf{Q}_p with the norm $|\cdot|_p$, namely

$$\mathbf{Z}_p = \{x \in \mathbf{Q}_p \mid |x|_p \leq 1\}.$$

This is precisely the set of x with no Laurent part in the expression in (1), i.e. such that $a_i = 0$ for $i < 0$, easily checked to be a ring via the properties of the norm.

The following exercise collects some of the most important properties of \mathbf{Z}_p .

Exercise 1.6. (i) \mathbf{Z}_p is open and closed in \mathbf{Q}_p .

(ii) \mathbf{Z}_p is compact.

(iii) \mathbf{Z}_p is a local ring, with maximal ideal $p\mathbf{Z}_p = \{x \in \mathbf{Z}_p \mid |x|_p < 1\}$, and

$$\mathbf{Z}_p/p\mathbf{Z}_p \simeq \mathbf{Z}/p\mathbf{Z}.$$

Completions of DVR's. More generally, one can approach and extend the constructions above is via completions in the \mathfrak{m} -adic topology. Consider a DVR (R, \mathfrak{m}) , with field of fractions $K = Q(R)$ and associated discrete valuation $v : K \rightarrow \mathbf{Z}$. On R , or K , one can consider the \mathfrak{m} -adic topology, which is the unique translation invariant topology with a

¹Thus in \mathbf{Q}_p every Cauchy sequence is convergent, and \mathbf{Q} can be identified with its subfield consisting of classes of constant sequences.

basis of neighborhoods of 0 consisting of $\{\mathfrak{m}^i\}_{i \geq 1}$. (See for instance [Ma] §8 for the general setting, and for a detailed treatment of the properties discussed below.)

Definition 1.7. The *completion* of R with respect to the \mathfrak{m} -adic topology is

$$\widehat{R} := \varprojlim_i R/\mathfrak{m}^i.$$

This is a Noetherian local ring with a canonical embedding $R \hookrightarrow \widehat{R}$. Its maximal ideal is $\mathfrak{m} \cdot \widehat{R}$, and we have

$$\widehat{R}/(\mathfrak{m} \cdot \widehat{R})^i \simeq R/\mathfrak{m}^i \text{ for all } i \geq 1.$$

This implies in particular that $\dim \widehat{R} = \dim R = 1$, and that the maximal ideal of \widehat{R} is generated by the image in \widehat{R} of a uniformizing parameter π of R , so that \widehat{R} is in fact a DVR as well. Note that

$$\widehat{K} := Q(\widehat{R}) \simeq \widehat{R}_{(\pi)} \simeq K \otimes_R \widehat{R}.$$

Recall now that if $v : K \rightarrow \mathbf{Z}$ is the discrete valuation corresponding to R , one has for every $r \in R$, $v(r) = \max \{i \mid r \in \mathfrak{m}^i\}$.

Definition 1.8. Let $0 < \alpha < 1$. For every $x \in K$, define

$$|x| \text{ (} = |x|_v \text{)} := \alpha^{v(x)} \text{ for } x \neq 0$$

and $|0| = 0$. This can be easily seen to be a non-archimedean norm, as in the special case of $|\cdot|_p$ above. Its corresponding distance function is $d(x, y) = |x - y|$, and one can check that the associated topology is the \mathfrak{m} -adic topology described above (and hence independent of the choice of α).

Exercise 1.9. Check that \widehat{K} has a valuation and a non-archimedean norm extending those on K , and that as such it is the completion of K with respect to the topology induced by $|\cdot|$.

Example 1.10. The main example of course is that of p -adic integers discussed in the previous subsection. Concretely, fix a prime p , and take $R = \mathbf{Z}_{(p)}$, the localization of \mathbf{Z} in the prime ideal generated by p . One has $K = Q(\mathbf{Z}_{(p)}) \simeq \mathbf{Q}$, and

$$\widehat{R} = \varprojlim_i \mathbf{Z}_{(p)}/p^i \mathbf{Z}_{(p)} \simeq \varprojlim_i \mathbf{Z}/p^i \mathbf{Z} = \mathbf{Z}_p \text{ and } \widehat{K} = \mathbf{Q}_p.$$

By taking $\alpha = 1/p$, we obtain the p -adic absolute value $|\cdot|_p$ defined before.

p -adic fields and rings of integers. We collect only a few properties necessary later on for working with K -analytic manifolds.

Definition 1.11. A p -adic field K is a finite extension of \mathbf{Q}_p . The *ring of integers* $\mathcal{O}_K \subset K$ is the integral closure of \mathbf{Z}_p in K .

Lemma 1.12. *We have the following:*

- (i) $K = Q(\mathcal{O}_K)$.
- (ii) $K \simeq \mathcal{O}_K \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

(iii) \mathcal{O}_K is a DVR.

Proof. Take any $x \in K$. Since K is algebraic over \mathbf{Q}_p , one can easily check that there is some $a \in \mathbf{Z}_p$ such that $ax \in \mathcal{O}_K$. This implies that $K = Q(\mathcal{O}_K)$, and in fact $K = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} \mathcal{O}_K$, which proves (i) and (ii). For (iii), note first that clearly \mathcal{O}_K is normal, while since $\mathbf{Z}_p \subset \mathcal{O}_K$ is an integral extension and $\dim \mathbf{Z}_p = 1$, we also have $\dim \mathcal{O}_K = 1$. To conclude that \mathcal{O}_K is a DVR, it remains to show that it is local. Now every integral extension of a DVR is a finite algebra over it, and therefore in our case \mathcal{O}_K is a finite \mathbf{Z}_p -algebra. The assertion then follows from the following general statement: if (R, \mathfrak{m}) is a complete local ring, and S is a finite R -algebra, then S is a local ring as well. This is a well-known consequence of Hensel's Lemma (explain). \square

Given the Lemma, let $v_K : K \rightarrow \mathbf{Z}$ be the discrete valuation of K corresponding to \mathcal{O}_K . The *ramification index* of K over \mathbf{Q}_p is $e_K := v_K(p)$; K is called *unramified* if $e_K = 1$, and otherwise *ramified*. We can define a non-archimedean norm on K extending $|\cdot|_p$ on \mathbf{Q}_p by

$$|\cdot| = |\cdot|_p : K \rightarrow \mathbf{Q}, \quad |x|_p := \frac{1}{p^{v_K(x)/e_K}} \quad \text{for } x \neq 0$$

and $|0| = 0$. We clearly have

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

while the maximal ideal $\mathfrak{m}_K \subset \mathcal{O}_K$ is given by the condition $|x|_p < 1$. As before, we consider on K and \mathcal{O}_K the topology corresponding to this norm.

Proposition 1.13. *Let K be a p -adic field, with the topology associated to $|\cdot|_p$. Then:*

- (i) *As a \mathbf{Z}_p -module, \mathcal{O}_K is isomorphic to the free module \mathbf{Z}_p^d , where $d := [K : \mathbf{Q}_p]$.*
- (ii) *There exists a basis of open neighborhoods of 0 in \mathcal{O}_K given by $\{p^i \mathcal{O}_K\}_{i \geq 1}$.*
- (iii) *Fixing an isomorphism $\mathcal{O}_K \simeq \mathbf{Z}_p^d$, the topology on \mathcal{O}_K corresponds to the product topology on \mathbf{Z}_p^d .*
- (iv) *\mathcal{O}_K and K are complete topological spaces.*

Proof. (i) The ring \mathbf{Z}_p is a PID (every ideal is generated by a power of p) and \mathcal{O}_K is a torsion-free \mathbf{Z}_p -module. Since \mathcal{O}_K is finite over \mathbf{Z}_p , by the structure theorem for modules over PID's we get that \mathcal{O}_K is a free \mathbf{Z}_p -module, of finite rank equal to $d = [K : \mathbf{Q}_p]$.

(ii) The topology given by $|\cdot|_p$ coincides with the \mathfrak{m}_K -adic topology, and so the family $\{\mathfrak{m}_K^i\}_{i \geq 1}$ gives a basis of open neighborhoods of the origin. Now the statement follows by observing that by the definition of ramification it follows that $p\mathcal{O}_K = \mathfrak{m}_K^{e_K}$, so the \mathfrak{m}_K -adic topology and the $p\mathcal{O}_K$ -adic topology on \mathcal{O}_K coincide.

(iii) Via such an isomorphism, the ideal $p\mathcal{O}_K$ corresponds to the product of the ideals $p\mathbf{Z}_p$. Now by (ii) and the basic properties of \mathbf{Z}_p , the powers of these ideals on the two sides give bases for the respective topologies.

(iv) This follows immediately from (iii): since the topology on \mathbf{Z}_p is complete, so is the product topology on \mathbf{Z}_p^d and hence that on \mathcal{O}_K . As every point in K has a neighborhood homeomorphic to \mathcal{O}_K , this implies that K is complete as well. \square

Remark 1.14. The reasoning in (i) and (ii) above can be made a bit more precise. On one hand the quotient $\mathcal{O}_K/p\mathcal{O}_K$ is free of rank d over \mathbf{F}_p . On the other hand, it has a filtration with successive quotients isomorphic to $\mathcal{O}_K/\mathfrak{m}_K$, namely

$$(0) \subset \mathfrak{m}_K^{e_K-1}/\mathfrak{m}_K^{e_K} \subset \cdots \subset \mathfrak{m}_K/\mathfrak{m}_K^{e_K} \subset \mathcal{O}_K/\mathfrak{m}_K^{e_K}.$$

This implies that the residue field $\mathcal{O}_K/\mathfrak{m}_K$ is a finite extension of \mathbf{F}_p of degree $[K : \mathbf{Q}_p]/e_K$.

Proposition 1.15. *A p -adic field K is locally compact, and its ring of integers \mathcal{O}_K is compact.*

Proof. Since \mathcal{O}_K is complete with respect to the topology given by $|\cdot|_p$, which is the same as the \mathfrak{m}_K -adic topology, we have

$$\mathcal{O}_K \simeq \varprojlim_i \mathcal{O}_K/\mathfrak{m}_K^i.$$

Now, as in any discrete valuation ring, we have

$$\mathfrak{m}_K^n/\mathfrak{m}_K^{n+1} \simeq \mathcal{O}_K/\mathfrak{m}_K.$$

(If $\mathfrak{m}_K = (\pi_K)$, then the mapping is given by $a\pi_K^n \mapsto a(\bmod m_K)$.) Since $\mathcal{O}_K/\mathfrak{m}_K$ is a finite field, the exact sequences

$$0 \longrightarrow \mathfrak{m}_K^{i-1}/\mathfrak{m}_K^i \longrightarrow \mathcal{O}_K/\mathfrak{m}_K^i \longrightarrow \mathcal{O}_K/\mathfrak{m}_K^{i-1} \longrightarrow 0.$$

imply inductively that all the rings $\mathcal{O}_K/\mathfrak{m}_K^i$ are finite, and hence compact. The product $\prod_{i=1}^{\infty} \mathcal{O}_K/\mathfrak{m}_K^i$ is then compact, and so the closed subset $\varprojlim_i \mathcal{O}_K/\mathfrak{m}_K^i$ is compact as well.

Now \mathcal{O}_K is open in K , so for every $x \in K$ the set $x + \mathcal{O}_K$ is a neighborhood of x which is compact. \square

Finally, let's note the following fact, in analogy with the p -adic expansion of an element in \mathbf{Q}_p . Let K be a p -adic field, and let π_K be a uniformizing parameter for \mathcal{O}_K . Recall that $\mathcal{O}_K/\mathfrak{m}_K \simeq \mathbf{F}_q$ with $q = p^{[K:\mathbf{Q}_p]/e_K}$, and choose a system of representatives $S \subset \mathcal{O}_K$ for $\mathcal{O}_K/\mathfrak{m}_K$ (so a finite set of cardinality q , including 0). Then every element $x \in K$ admits a unique representation as a convergent Laurent series

$$x = a_m \pi_K^m + a_{m+1} \pi_K^{m+1} + \cdots$$

with $a_i \in S$, $a_m \neq 0$, and $m \in \mathbf{Z}$.

Remark 1.16. A p -adic field is a (not quite so) special example of the more general notion of a *local field* (see [Ne] Ch.II §5). Most of the general aspects of the discussion above can be extended to the setting of local fields.

2. p -ADIC INTEGRATION

Let G be a topological group, i.e. endowed with a topology which makes the group operation $G \times G \rightarrow G$, $(g, h) \mapsto gh$, and the inverse map $G \rightarrow G$, $g \mapsto g^{-1}$, continuous. If G is abelian² and locally compact, it is well-known that it has a non-zero translation invariant³ measure μ with a mild regularity property, which is unique up to scalars. This is called the *Haar measure*. More precisely, a Haar measure is characterized by the following integration properties:

- Any continuous function $f : G \rightarrow \mathbf{C}$ with compact support is μ -integrable.
- For any μ -integrable function f and any $g \in G$, one has

$$\int_G f(x) d\mu = \int_G f(gx) d\mu.$$

Other important properties of the Haar measure are as follows: every Borel subset of G is μ -measurable, $\mu(A) > 0$ for every nonempty open subset A of G , while A is compact subset if and only if $\mu(A)$ is finite. For a thorough treatment, including a proof of existence and uniqueness, see [RV] §1.2.

We use this in the p -adic setting (see for instance [Ig] §7.4 or [We1]). Let's start with the more down-to-earth case of \mathbf{Q}_p . Since \mathbf{Q}_p is locally compact, it has Haar measure μ , which according to the discussion above can be normalized so that for the compact subring \mathbf{Z}_p it satisfies

$$\mu(\mathbf{Z}_p) = 1.$$

For any measurable function $f : \mathbf{Q}_p \rightarrow \mathbf{C}$, one can consider the integrals

$$\int_{\mathbf{Q}_p} f d\mu \quad \text{and especially} \quad \int_{\mathbf{Z}_p} f d\mu.$$

Here are some first examples of calculations.

Example 2.1. $\mu(p\mathbf{Z}_p) = \frac{1}{p}$.

Proof. Since $\mathbf{Z}_p/p\mathbf{Z}_p \simeq \mathbf{F}_p$, with a set of representatives $0, 1, \dots, p-1$, we have a disjoint union decomposition

$$\mathbf{Z}_p = p\mathbf{Z}_p \cup (p\mathbf{Z}_p + 1) \cup \dots \cup (p\mathbf{Z}_p + p-1).$$

By translation invariance, all of the sets on the right have the same measure, and since $\mu(\mathbf{Z}_p) = 1$, this immediately gives the result. \square

Exercise 2.2. Show more generally that for every $m \geq 1$ one has $\mu(p^m\mathbf{Z}_p) = \frac{1}{p^m}$.

²This is not necessary, but otherwise we would have to speak separately of left and right invariant measures.

³This means that for every measurable set $A \subset G$ and any $g \in G$, one has $\mu(A) = \mu(gA)$.

A useful observation for calculating integrals is the following: the functions $f : \mathbf{Z}_p \rightarrow \mathbf{C}$ we will be dealing with have their image equal to a countable subset, say $C \subset \mathbf{C}$. Suppose we want to calculate the integral $\int_A f(x) d\mu$, for some measurable set A . If

$$A_f(c) := \{x \in A \mid f(x) = c\}$$

are the level sets of f in A , then

$$\int_A f(x) d\mu = \sum_{c \in C} \int_{A_f(c)} f(x) d\mu = \sum_{c \in C} c \cdot \mu(A_f(c)).$$

For arbitrary functions $f : \mathbf{Z}_p \rightarrow \mathbf{C}$, the definition and calculation of the integral is of course much more complicated.

Example 2.3. Let $s \geq 0$ be a real number, and $d \geq 0$ an integer. Then

$$\int_{\mathbf{Z}_p} |x^d|^s d\mu = \frac{p-1}{p-p^{-ds}}.$$

Proof. We take advantage of the fact that in this context the function we are integrating is the analogue of a step function, as in the comment above. We clearly have:

- $|x^d|^s = 1$ for $x \in \mathbf{Z}_p - p\mathbf{Z}_p$.
- $|x^d|^s = \frac{1}{p^{ds}}$ for $x \in p\mathbf{Z}_p - p^2\mathbf{Z}_p$.
- $|x^d|^s = \frac{1}{p^{2ds}}$ for $x \in p^2\mathbf{Z}_p - p^3\mathbf{Z}_p$.

and so on. Since these sets partition \mathbf{Z}_p we get

$$\int_{\mathbf{Z}_p} |x^d|^s d\mu = 1 \cdot \mu(\mathbf{Z}_p - p\mathbf{Z}_p) + \frac{1}{p^{ds}} \cdot \mu(p\mathbf{Z}_p - p^2\mathbf{Z}_p) + \frac{1}{p^{2ds}} \cdot \mu(p^2\mathbf{Z}_p - p^3\mathbf{Z}_p) + \dots$$

Using the exercise above, this sum is equal to

$$\begin{aligned} & 1 \cdot \left(1 - \frac{1}{p}\right) + \frac{1}{p^{ds}} \cdot \left(\frac{1}{p} - \frac{1}{p^2}\right) + \frac{1}{p^{2ds}} \cdot \left(\frac{1}{p^2} - \frac{1}{p^3}\right) + \dots = \\ & = \left(1 + \frac{1}{p^{ds+1}} + \frac{1}{p^{2ds+2}} + \dots\right) - \frac{1}{p} \cdot \left(1 + \frac{1}{p^{ds+1}} + \frac{1}{p^{2ds+2}} + \dots\right) = \\ & = \left(1 - \frac{1}{p}\right) \cdot \frac{1}{1 - p^{-ds-1}} = \frac{p-1}{p-p^{-ds}}. \end{aligned}$$

□

Let now K be more generally any p -adic field, with ring of integers \mathcal{O}_K . Recall that if $\mathfrak{m}_K = (\pi_K)$ is the maximal ideal, then $\mathcal{O}_K/\mathfrak{m}_K \cong \mathbf{F}_q$, where $q = p^r$ for some $r > 0$. Take on K the topology discussed in the previous section, namely that induced by the norm $|\cdot|_p$ extending the p -adic norm on \mathbf{Q}_p . We have seen that K is a (totally disconnected) locally compact abelian topological group, hence we can consider a Haar measure μ on K . According to the discussion above, since \mathcal{O}_K is compact we can normalize this measure so that it satisfies

$$\mu(\mathcal{O}_K) = 1.$$

For any $r \geq 1$, we can also consider the Haar measure on K^r with the product topology, normalized such that $\mu(\mathcal{O}_K^r) = 1$. We can integrate any measurable function f defined on K^r , for instance $f \in \mathcal{O}_K[X_1, \dots, X_r]$.

Lemma 2.4. *For every $k \geq 1$, $\mu(\mathfrak{m}_K^k) = \frac{1}{q^k}$.*

Proof. First note that we have a disjoint union

$$\mathcal{O}_K = \bigcup_{s \in S} (\mathfrak{m}_K + s),$$

where S is a set of representatives in \mathcal{O}_K for $\mathcal{O}_K/\mathfrak{m}_K \simeq \mathbf{F}_q$. By translation invariance, this immediately implies that $\mu(\mathfrak{m}_K) = 1/q$. By a completely similar argument we see that

$$\mu(\mathfrak{m}_K^k) = \frac{1}{|\mathcal{O}_K/\mathfrak{m}_K^k|}.$$

Now a simple filtration argument as in the previous subsection shows that

$$|\mathcal{O}_K/\mathfrak{m}_K^k| = |\mathfrak{m}_K^{k-1}/\mathfrak{m}_K^k| \cdot \dots \cdot |\mathfrak{m}_K/\mathfrak{m}_K^2| \cdot |\mathcal{O}_K/\mathfrak{m}_K| = q^k.$$

The last equality follows since for each i we have $\mathfrak{m}_K^{i-1}/\mathfrak{m}_K^i \simeq \mathcal{O}_K/\mathfrak{m}_K$. □

Exercise 2.5. Show that $\mu(\mathcal{O}_K^*) = 1 - \frac{1}{q}$.

Exercise 2.6. Show that for any non-negative integers k_1, \dots, k_r , one has

$$\mu(\mathfrak{m}_K^{k_1} \times \dots \times \mathfrak{m}_K^{k_r}) = \frac{1}{q^{k_1 + \dots + k_r}}.$$

Exercise 2.7. Let $s \geq 0$ be a real number, and $d \geq 0$ an integer. Then

$$\int_{\mathcal{O}_K} |x^d|^s d\mu = \frac{q-1}{q - q^{-ds}}.$$

More generally, for any non-negative integers k_1, \dots, k_r ,

$$\int_{\mathcal{O}_K^r} |x_1^{k_1} \cdot \dots \cdot x_r^{k_r}|^s d\mu = \prod_{i=1}^r \frac{q-1}{q - q^{-k_i s}}.$$

(Hint: Fubini's formula holds for p -adic integrals.)

Remark 2.8. (1) The computations above still work if one takes $s \in \mathbf{C}$, imposing the condition $\operatorname{Re}(s) > -1$.

(2) What makes an integral as above easy to compute is the fact that the integrand is a monomial in the variables, i.e. it involves only multiplication (for which we have the norm formula $|xy| = |x||y|$). As soon as addition appears in the integrand, things become a lot more complicated, partly due to the absence of a formula for $|x+y|$. Here is a typical example:

Exercise 2.9 (Challenge; cf. [duS]). For $s \geq 0$, compute the integral

$$\int_{\mathbf{Z}_p^2} |xy(x+y)|^s d\mu.$$

Definition 2.10. Let $f \in \mathcal{O}_K[X_1, \dots, X_r]$ (or more generally any K -analytic function as defined below), and let $s \in \mathbb{C}$. The (local) zeta function of f is

$$Z(f, s) := \int_{\mathcal{O}_K^r} |f(x)|^s d\mu.$$

It is a holomorphic function of s for $\operatorname{Re}(s) > 0$ (exercise). (This is a special example of a more general type of zeta functions introduced in [We1].)

3. INTEGRATION ON K -ANALYTIC MANIFOLDS

K -analytic functions and manifolds. In this section, besides Igusa's book [Ig], I am benefitting from lecture notes of Lazarsfeld [La]. Let K be a p -adic field, and $r > 0$ an integer. For any open set $U \subset K^r$, a K -analytic function $f : U \rightarrow K$ is a function which is locally around any point in U given by a convergent power series. Such a function can be seen in a standard fashion to be differentiable, with all partial derivatives again K -analytic functions (see [Ig] Ch.2). We call $f = (f_1, \dots, f_m) : U \rightarrow K^m$ a K -analytic map if all f_i are K -analytic functions.

Definition 3.1 (K -analytic manifold). Let X be a Hausdorff topological space, and $n \geq 0$ an integer. A *chart* of X is a pair (U, φ_U) consisting of an open subset of X together with a homeomorphism $\varphi_U : U \rightarrow V$ onto an open set $V \subset K^n$. An *atlas* is a family of charts $\{(U, \varphi_U)\}$ such that for every U_1, U_2 with $U_1 \cap U_2 \neq \emptyset$ the composition

$$\varphi_{U_2} \circ \varphi_{U_1}^{-1} : \varphi_{U_1}(U_1 \cap U_2) \rightarrow \varphi_{U_2}(U_1 \cap U_2)$$

is bi-analytic. Two atlases are equivalent if their union is also an atlas. Finally, X together with an equivalence class of atlases as above is called a K -analytic manifold of dimension n . If we vary x around a point $x_0 \in U$, where U is an open set underlying a chart, then $\varphi_U(x) = (x_1, \dots, x_n)$ is called a *system of coordinates* around x_0 . K -analytic maps between manifolds X and Y are defined in the obvious way.

From the similar properties of K (and hence K^r) we get:

Lemma 3.2. *A K -analytic manifold is a locally compact, totally disconnected topological space.*

Example 3.3. (1) Every open set $U \subset K^n$ is a K -analytic manifold.

(2) $X = \mathcal{O}_K^n \subset K^n$ is a compact K -analytic manifold; note that it is a manifold since it is an open subset of K^n .

(3) Consider the projective line \mathbf{P}^1 over K , with homogeneous coordinates $(x : y)$. This is covered by two disjoint compact open sets (sic!), namely

$$U := \{(x : y) \mid |x/y| \leq 1\} \quad \text{and} \quad V := \{(x : y) \mid |y/x| < 1\}.$$

We have bi-analytic maps

$$U \rightarrow \mathcal{O}_K, (x : y) \mapsto x/y \quad \text{and} \quad V \rightarrow \mathfrak{m}_K \simeq_{\text{homeo}} \mathcal{O}_K, (x : y) \mapsto y/x.$$

(4) Let $\pi : \text{Bl}_0(K^2) \rightarrow K^2$ be the blow-up of the origin in the affine plane over K , naturally defined inside $K^2 \times \mathbf{P}^1$. Let

$$X = \mathcal{O}_K^2 \subset K^2 \quad \text{and} \quad Y = \pi^{-1}(X),$$

both compact K -analytic manifolds. Recall that $\text{Bl}_0(K^2)$ is covered by two copies of K^2 , mapping to the base K^2 via the rules

$$K^2 \rightarrow K^2 \quad (s, t) \mapsto (s, st) \quad \text{and} \quad K^2 \rightarrow K^2 \quad (u, v) \mapsto (uv, u).$$

We can then express Y as the disjoint union of the compact open sets

$$U = \{(s, t) \mid |s| \leq 1, |t| \leq 1\} \quad \text{and} \quad V = \{(u, v) \mid |u| < 1, |v| \leq 1\},$$

by noting that

$$\pi(U) = \{(x, y) \mid |y| \leq |x| \leq 1\} \quad \text{and} \quad \pi(V) = \{(x, y) \mid |x| < |y| \leq 1\} \cup \{(0, 0)\}.$$

What we saw in the examples above is a general fact:

Exercise 3.4. Every compact K -analytic manifold of dimension n is bi-analytic to a finite disjoint union of copies of \mathcal{O}_K^n .

Differential forms and measure. If X is an n -dimensional K -analytic manifold, we can define differential forms in the usual way. Locally on an open set U with coordinates x_1, \dots, x_n , a form of degree k can be written as

$$(2) \quad \nu = \sum_{i_1 < \dots < i_k} f_{i_1, \dots, i_k} dx_{i_1} \wedge \dots \wedge dx_{i_k},$$

with f_{i_1, \dots, i_k} K -valued functions on U . If these functions are K -analytic, then ν is a K -analytic differential form.

We will be particularly interested in forms of top degree n , and the measure they define. Let ω be such a K -analytic form on X . The associated measure $\mu_\omega = |\omega|$ on X is defined as follows. Let's assume first that X is a local $\pi_K^{p_1} \mathcal{O}_K \times \dots \times \pi_K^{p_n} \mathcal{O}_K$, on which (2) holds globally. For any compact-open polycylinder

$$A \simeq (x_1 + \pi_K^{k_1} \mathcal{O}_K) \times \dots \times (x_r + \pi_K^{k_n} \mathcal{O}_K) \subset X$$

we set

$$\mu_\omega(A) := \int_A |f(x)| d\mu,$$

where μ is the usual normalized Haar measure. This is easily checked to define a Borel measure on X .

To define the measure μ_ω on a global X , we need to check that it transforms precisely like differential forms when changing coordinates.

Theorem 3.5 (Change of variables formula, I). *Let $\varphi = (\varphi_1, \dots, \varphi_n) : K^n \rightarrow K^n$ be a K -analytic map. Suppose $x \in K^n$ is a point where $\det \left(\frac{\partial \varphi_i}{\partial x_j}(x) \right) \neq 0$. Then φ restricts to a bi-analytic isomorphism*

$$\varphi : U \subset K^n \xrightarrow{\simeq} V \subset K^n$$

with U a neighborhood of x and V a neighborhood of $\varphi(x)$, and $\mu_{\text{Haar}}^V = \left| \det \left(\frac{\partial \varphi_i}{\partial x_j}(x) \right) \right|_K \cdot \mu_{\text{Haar}}^U$, which means that for every measurable set $A \subset U$ one has

$$\int_{\varphi(A)} d\mu_{\text{Haar}}^V = \int_A \left| \det \left(\frac{\partial \varphi_i}{\partial x_j}(x) \right) \right|_K \cdot d\mu_{\text{Haar}}^U.$$

Here is just a brief sketch of the proof (for more details see [Ig] §7.4). The essential point is to treat the case when φ is given by multiplication by an invertible matrix M . For this in turn the essential case is that of a diagonal matrix $M = \text{diag}(\pi_K^{k_1}, \dots, \pi_K^{k_n})$. This maps the polydisk \mathcal{O}_K^n , of measure 1, to $\pi_K^{k_1} \mathcal{O}_K \times \dots \times \pi_K^{k_n} \mathcal{O}_K$, of measure $\frac{1}{q^{k_1 + \dots + k_n}}$; on the other hand $|\det(M)| = \frac{1}{q^{k_1 + \dots + k_n}}$, since $|\pi_K| = \frac{1}{q}$.

Remark 3.6. Let's change notation slightly in order to make this look more familiar: denote $|dx| = |dx_1 \wedge \dots \wedge dx_n|$ and $|dy| = |dy_1 \wedge \dots \wedge dy_n|$ the Haar measure on U and V respectively. Then the Theorem says that for $A \subset U$ measurable,

$$\int_{\varphi(A)} |dy| = \int_A |\varphi^* dy| = \int_A |\det(\text{Jac}(\varphi))| \cdot |dx|.$$

Putting together all of the above, we obtain

Corollary 3.7. *Let X be a compact K -analytic manifold, and ω a K -analytic n -form on X . Then there exists a globally defined measure μ_ω on X . In particular, for any continuous function $f : X \rightarrow \mathbf{C}$, the integral $\int_X f(x) d\mu_\omega$ is well-defined.*

Proof. By Exercise 3.4, we can cover X by finitely many disjoint compact open subsets U on which $\omega = f(x) dx_1 \wedge \dots \wedge dx_n$. But by Theorem 3.5, μ_ω is independent of the particular choice of coordinates, hence it gives a globally defined measure. \square

Since removing sets of measure 0 does not affect integrals, Theorem 3.5 immediately implies the following slightly more general statement.

Theorem 3.8 (Change of variables formula, II). *Let $\varphi : Y \rightarrow X$ be a K -analytic map of compact K -analytic manifolds. Assume that φ is bi-analytic away from closed subsets $Z \subset Y$ and $\varphi(Z) \subset X$ of measure 0. If ω is a K -analytic n -form on X and f is a K -analytic function on X , then*

$$\int_X |f|^s d\mu_\omega = \int_Y |f \circ \varphi|^s d\mu_{\varphi^* \omega}.$$

Example 3.9. Let $\pi : Y = \text{Bl}_0(\mathcal{O}_K^2) \rightarrow X = \mathcal{O}_K^2$ be the blow-up of the origin. Recall that in Exercise 2.7 we've computed

$$(3) \quad \int_X |x^a y^b|^w |dx \wedge dy| = \frac{1}{1 - q^{-wa-1}} \cdot \frac{1}{1 - q^{-wb-1}} \cdot \left(\frac{q-1}{q} \right)^2.$$

We verify the change of variables formula on the blow-up Y . We know from Example 3.3 (4) that Y is covered by two disjoint polydisks $Y = U \cup V$ with

$$U = \{(s, t) \mid |s| \leq 1, |t| \leq 1\} \quad \text{and} \quad V = \{(u, v) \mid |u| < 1, |v| \leq 1\}$$

with maps to X given by

$$(s, t) \mapsto (s, st) \quad \text{and} \quad (u, v) \mapsto (uv, u).$$

This means that

$$\pi^*(dx \wedge dy) = sds \wedge dt \text{ on } U \text{ and } \pi^*(dx \wedge dy) = vdu \wedge dv \text{ on } V.$$

while on the other hand

$$|\pi^*f|^s = |s^{a+b}|^w |t|^b|^w \text{ on } U \text{ and } |\pi^*f|^s = |u^a|^w |v^{a+b}|^w \text{ on } V.$$

This gives

$$\int_Y |\pi^*f|^w \cdot |\pi^*(dx \wedge dy)| = \int_{|s| \leq 1, |t| \leq 1} |s|^{w(a+b)+1} |t|^{wb} ds \wedge dt + \int_{|u| \leq \frac{1}{q}, |v| \leq 1} |u|^{wa} |t|^{w(a+b)+1} du \wedge dv.$$

We now use result similar to Exercise 2.7, namely

Exercise 3.10. For every non-negative integer m and any c ,

$$\int_{|x| \leq \frac{1}{q^m}} |x|^c |dx| = \frac{q^{-m(c+1)}}{1 - q^{-(c+1)}} \cdot \frac{q-1}{q}.$$

Given this formula, we can write the integral above as

$$\left(\frac{q-1}{q}\right)^2 \left(\frac{1}{(1 - q^{-w(a+b)-2})(1 - q^{-wb-1})} + \frac{1}{(1 - q^{-wa-1})(1 - q^{-w(a+b)-2})} \right)$$

and a simple calculation leads to the same formula as (3).

Resolution of singularities. We start with an example. Generalizing a previous exercise, given integers a, b, c let's consider the integral

$$I := \int_{X=\mathcal{O}_K^2} |f(x, y)|^w |dx \wedge dy|, \quad \text{with } f(x, y) = x^a y^b (x - y)^c.$$

Given the change of variables formula, and the fact that integrals of monomial functions are much easier to compute, a natural idea is to pass to a birational model of X on which the function f can be brought to a monomial form. In this particular case, fortunately one needs to consider only the blow-up $\pi : Y \rightarrow X$ at the origin. Recall yet again that Y is covered by two disjoint polydisks $Y = U \cup V$ with

$$U = \{(s, t) \mid |s| \leq 1, |t| \leq 1\} \quad \text{and} \quad V = \{(u, v) \mid |u| < 1, |v| \leq 1\}$$

with maps to X given by

$$(s, t) \mapsto (s, st) \quad \text{and} \quad (u, v) \mapsto (uv, u).$$

Consider now

$$I_U := \int_U |\pi^*f| |\pi^*(dx \wedge dy)|.$$

A simple calculation shows that on U we have

$$(\pi^*f)(s, t) = s^{a+b+c} t^b (1-t)^c \quad \text{and} \quad \pi^*(dx \wedge dy) = sds \wedge dt,$$

which gives

$$\begin{aligned} I_U &= \int_U |s^{a+b+c+1} t^b (1-t)^c|^s |ds \wedge dt| = \\ &= \left(\int_{|s| \leq 1} |s^{a+b+c+1}|^w |ds| \right) \cdot \left(\int_{|t| \leq 1} |t^b|^w |(1-t)^c|^w |dt| \right). \end{aligned}$$

We have already seen the calculation of the first integral in the product a few times. For the second integral, let's choose a set $S = \{\alpha_1 = 0, \alpha_2 = 1, \alpha_3, \dots, \alpha_q\} \subset \mathcal{O}_K$ of representatives for $\mathcal{O}_K/\mathfrak{m}_K \simeq \mathbf{F}_q$. We can then split the region $\{|t| \leq 1\}$ as a disjoint union

$$\{|t| \leq 1\} = T_1 \cup \dots \cup T_q, \quad T_i := \{|t - \alpha_i| \leq \frac{1}{q}\},$$

so that if we denote $g(t) = t^b(1-t)^c$, we have

$$\int_{|t| \leq 1} |g(t)|^w |dt| = \int_{T_1} |g(t)|^w |dt| + \dots + \int_{T_q} |g(t)|^w |dt|.$$

The point is that each of the integrals in the sum on the right can now be computed as a “monomial” integral. For instance, note that the condition $|t| \leq \frac{1}{q}$ defining T_1 implies that $|t - 1| = 1$, so that

$$\int_{T_1} |g(t)|^w |dt| = \int_{T_1} |t^b|^w |dt|,$$

which we know how to compute. Similarly, the condition defining T_2 implies $|t| = 1$, so that

$$\int_{T_2} |g(t)|^w |dt| = \int_{|t-1| \leq \frac{1}{q}} |(t-1)^c|^w |dt|,$$

which again we know how to compute after making the change of variables $t' = t - 1$. The same thing can be done for all the other T_i 's, which means that we can complete the calculation of I_U via only monomial computations. One can similarly define I_V and deal with it in an analogous fashion, while finally by the change of variables formula and the decomposition of Y we have $I = I_U + I_V$.

Exercise 3.11. Complete all the details of the calculation above to find a formula for I .

What happened here? Geometrically, by blowing up the origin in \mathcal{O}_K^2 , we “resolved the singularities” of the curve $f(x, y) = 0$. (Draw the picture.) The essential point is that on $\text{Bl}_0(\mathcal{O}_K^2)$, the function π^*f is locally monomial. Hironaka's famous theorem on resolution of singularities says that we can always do this. Let's recall first the better known version over \mathbf{C} , restricting only to the case of hypersurfaces in affine space.

Theorem 3.12 (Resolution of singularities over \mathbf{C}). *Let $X = \mathbf{C}^n$, and let $f \in \mathbf{C}[X_1, \dots, X_n]$ be a non-constant polynomial. Then there exists a complex manifold Y and a proper surjective map $\pi : Y \rightarrow X$ such that the divisor*

$$\text{div}(\pi^*f) + \text{div}(\pi^*(dx_1 \wedge \dots \wedge dx_n))$$

has simple normal crossings support.

Remark 3.13. Let's recall and expand a bit the terminology in the Theorem. A *simple normal crossings divisor* on X is an effective divisor $D = \sum_{i=1}^k F_i$ such that each F_i is a non-singular codimension 1 subvariety of X , and in the neighborhood of each point, D is defined in local coordinates x_1, \dots, x_n by the equation $x_1 \cdots x_k = 0$. The conclusion of the Theorem is that one can write

$$\operatorname{div}(\pi^* f) = \sum_{i=1}^k a_i F_i \quad \text{and} \quad \operatorname{div}(\pi^*(dx_1 \wedge \dots \wedge dx_n)) = \sum_{i=1}^k b_i F_i$$

for some integers a_i, b_i , $i \in \{1, \dots, k\}$, with $\sum_{i=1}^k F_i$ having simple normal crossings support. A mapping π as in the statement is called an *embedded resolution of singularities* of the hypersurface $(f = 0)$. The integers a_i, b_i are important invariants of the resolution, called *discrepancies*.

Example 3.14. Let $f(x, y) = y^2 - x^3$, i.e. the equation defining a cusp in \mathbf{C}^2 . Its embedded resolution is one of the best known examples of this procedure. In order to get to a simple normal crossings divisor, we have to blow-up the origin three successive times, keeping track of multiplicities; for the geometric picture, see [Ha] Example 3.9.1. If $Y \rightarrow \mathbf{C}^2$ is the composition of the three blow-ups, denoting by C the proper transform of $(f = 0)$, and by E_1, E_2, E_3 the three exceptional divisors in Y (coming from the successive blow-ups, in this order), we have

$$\operatorname{div}(\pi^* f) = C + 2E_1 + 3E_2 + 6E_3$$

and

$$K_{Y/\mathbf{C}^2} = \operatorname{div}(\pi^*(dx \wedge dy)) = E_1 + 2E_2 + 4E_3.$$

Exercise 3.15. Complete the details of the calculation.

Since we're at this, let's record a few more things about general birational maps between smooth complex varieties. Let $\pi : Y \rightarrow X$ be a birational map (not necessarily proper) between two such varieties of dimension n . A key point to note is that while we cannot talk about canonically defined divisors K_X and K_Y , there is a canonically defined *relative* canonical divisor $K_{Y/X}$, namely the zero locus of the Jacobian of the map π . This supported on the exceptional locus of π : if E_i are the exceptional divisors of π , with $1 \leq i \leq k$, then there exist positive integers a_{E_i} such that

$$(4) \quad K_{Y/X} := Z(\operatorname{Jac}(\pi)) = \sum_{i=1}^k a_{E_i} \cdot E_i.$$

Let's make this explicit. Fix an exceptional divisor E for π , and consider $Z = f(E) \subset X$, with $\operatorname{codim}_X Z = c \geq 2$. Let $y \in E$ be a general point, and $x = f(y) \in Z$. Since these are smooth points, we can then choose systems of coordinates y_1, \dots, y_n around y , and x_1, \dots, x_n around x , such that $E = (y_1 = 0)$ and $Z = (x_1 = \dots = x_c = 0)$. Then for each $1 \leq i \leq c$ there exist integers $k_i \geq 1$ such that

$$\pi^* x_i = y_i^{k_i} \cdot \psi_i,$$

with ψ_i an analytic function which is invertible at y . Noting that

$$\pi^* dx_i = k_i \psi_i \cdot y_i^{k_i-1} \cdot dy_i + d\psi_i \cdot y_i^{k_i},$$

this gives

$$\pi^*(dx_1 \wedge \dots \wedge dx_n) = y_1^{a_E} \cdot (\text{unit}) \cdot (dy_1 \wedge \dots \wedge dy_n),$$

with $a_E = (\sum_{i=1}^c k_i) - 1$. In other words, locally around a general point of E we have $K_{Y/X} = a_E \cdot E$. Globalizing this to include all exceptional divisors of π we get (4). Note also that for every effective divisor $D \subset X$ we have

$$\pi^*D = \tilde{D} + \sum_{i=1}^k b_i \cdot E_i,$$

where \tilde{D} is the proper transform of D , and b_i are non-negative integers.

Going back to the K -analytic picture, for our present purposes the important fact is that a statement completely analogous to Theorem 3.12 holds for K -analytic manifolds.

Theorem 3.16 (*K -analytic resolution of singularities*). *Let K be a p -adic field, $X = K^n$, and $f \in K[X_1, \dots, X_n]$ a non-constant polynomial. Then there exists an n -dimensional K -analytic manifold Y , a proper surjective K -analytic map $\pi : Y \rightarrow X$ which is an isomorphism outside a set of measure 0, and finitely many submanifolds F_1, \dots, F_k of Y of codimension 1, such that the following hold:*

- *the divisor $\sum_{i=1}^k F_i$ has simple normal crossings support.*
- $\text{div}(\pi^*f) = \sum_{i=1}^k a_i F_i$ *for some non-negative integers a_1, \dots, a_k .*
- $\text{div}(\pi^*(dx_1 \wedge \dots \wedge dx_n)) = \sum_{i=1}^k b_i F_i$ *for some non-negative integers b_1, \dots, b_k .*

In terms of equations, this means that in suitable coordinates $y = (y_1, \dots, y_n)$ around any point $y \in Y$ we have

$$\pi^*f = \mu(y) \cdot y_1^{a_1} \cdot \dots \cdot y_n^{a_n}$$

and

$$\pi^*(dx_1 \wedge \dots \wedge dx_n) = \nu(y) \cdot y_1^{b_1} \cdot \dots \cdot y_n^{b_n} \cdot (dy_1 \wedge \dots \wedge dy_n)$$

with $\mu(0) \neq 0$ and $\nu(0) \neq 0$.

Roughly speaking, the Theorem follows from the usual version: by Theorem 3.12, there exists a smooth algebraic variety Z defined over K a morphism $\pi : Z \rightarrow \mathbb{A}_K^n$ which is an embedded resolution of $(f = 0)$. One takes $Y = Z(K)$.

4. IGUSA'S THEOREM ON THE RATIONALITY OF THE ZETA FUNCTION

In this section we prove a theorem of Igusa which was one of the first important applications of the theory of p -adic integration. The number theoretic set-up is as follows: fix a prime p , and let $f \in \mathbf{Z}_p[X_1, \dots, X_n]$ (for instance $f \in \mathbf{Z}[X_1, \dots, X_n]$). For any integer $m \geq 0$, define

$$N_m := |\{x \in (\mathbf{Z}/p^m\mathbf{Z})^n \mid f(\text{mod } p^m)(x) = 0\}|,$$

with the convention $N_0 = 1$. Consider the *Poincaré series*

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

The following result was conjectured by Borevich and Shafarevich [BS] and proved by Igusa (see e.g. §8.2).

Theorem 4.1. *$Q(f, t)$ is a rational function.*

A more general statement appears in Theorem 4.4, and a more precise statement appears in Theorem 4.8 below. Let's start by looking at some examples.

Example 4.2. (1) Take $f(x) = x$. Then $x \equiv 0 \pmod{p^m}$ has precisely one solution, so $N_m = 1$ for all m . Then

$$Q(f, t) = 1 + t + t^2 + \dots = \frac{1}{1-t}.$$

(2) Take $f(x) = x^2$. Then N_m is the number of solutions of $x^2 \equiv 0 \pmod{p^m}$:

- For $m = 1$, we have $p|x^2$ iff $p|x$, so $N_1 = 1$.
- For $m = 2$, we have $p^2|x^2$ iff $p|x$, so $N_2 = p$.
- For $m = 3$, we have $p^3|x^2$ iff $p^2|x$, so $N_3 = p$.
- For $m = 4$, we have $p^4|x^2$ iff $p^2|x$, so $N_4 = p^2$.
- For $m = 5$, we have $p^5|x^2$ iff $p^3|x$, so $N_5 = p^3$.

The pattern is now clear. We have

$$\begin{aligned} Q(f, t) &= 1 + t + pt^2 + pt^3 + p^2t^4 + p^2t^5 + \dots = \\ &= (1+t)(1+pt^2+p^2t^4+\dots) = \frac{1+t}{1-pt^2}. \end{aligned}$$

(3) Take $f(x, y) = y - x^2$. Fixing an arbitrary x , the congruence $y \equiv x^2 \pmod{p^m}$ determines y , so we easily get $N_m = p^m$ for each m . We have

$$Q(f, t) = 1 + pt + p^2t^2 + p^3t^3 + \dots = \frac{1}{1-pt}.$$

Exercise 4.3. (1) Compute $Q(f, t)$ for $f(x) = x^d$ with $d \geq 3$.

(2) Challenge: compute $Q(f, t)$ for $f(x, y) = y^2 - x^3$.

(2) Challenge: compute $Q(f, t)$ for $f(x_1, \dots, x_n) = x_1^{d_1} \cdots x_n^{d_n}$ with $n \geq 1$ and d_1, \dots, d_n arbitrary positive integers. Start with some small cases, like $x \cdot y$, etc.

Theorem 4.1 can be proved in the more general context of arbitrary p -adic fields. Consider such a field K , with ring of integers \mathcal{O}_K , such that $\mathcal{O}_K/\mathfrak{m}_K \simeq \mathbf{F}_q$, $q = p^r$. Let $f \in \mathcal{O}_K[X_1, \dots, X_n]$, and for any $m \geq 0$ define

$$N_m := |\{x \in (\mathcal{O}_K/\mathfrak{m}_K^m)^n \mid f(\bmod \mathfrak{m}_K^m)(x) = 0\}|,$$

with the convention $N_0 = 1$. Define as before the Poincaré series of f to be

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

Theorem 4.4 ([Ig] §8.2). $Q(f, t)$ is a rational function.

The key idea in Igusa's approach to Theorem 4.4 is to relate $Q(f, t)$ to a p -adic integral via the following:

Proposition 4.5. *With the notation above, we have*

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

Proof. For every $m \geq 0$, consider the subset of \mathcal{O}_K^n given by

$$V_m := \{x \in \mathcal{O}_K^n \mid |f(x)| \leq \frac{1}{q^m}\},$$

so that $V_m - V_{m+1}$ are the level sets of f . In Lemma 4.6 below we will show that

$$\mu(V_m) = N_m \cdot \frac{1}{q^{nm}}.$$

Assuming this, and decomposing the domain into the disjoint union of these level sets, we have

$$\begin{aligned} Z(f, s) &= \int_{\mathcal{O}_K^n} |f(x)|^s d\mu = \\ &= 1 \cdot (\mu(V_0) - \mu(V_1)) + \frac{1}{q^s} \cdot (\mu(V_1) - \mu(V_2)) + \frac{1}{q^{2s}} \cdot (\mu(V_2) - \mu(V_3)) + \dots = \\ &= 1 \cdot \left(1 - N_1 \cdot \frac{1}{q^n}\right) + \frac{1}{q^s} \cdot \left(N_1 \cdot \frac{1}{q^n} - N_2 \cdot \frac{1}{q^{2n}}\right) + \frac{1}{q^{2s}} \cdot \left(N_2 \cdot \frac{1}{q^{2n}} - N_3 \cdot \frac{1}{q^{3n}}\right) + \dots = \\ &= \left(1 + N_1 \cdot \frac{1}{q^{n+s}} + N_2 \cdot \frac{1}{q^{2(n+s)}} + \dots\right) - q^s \cdot \left(N_1 \cdot \frac{1}{q^{n+s}} + N_2 \cdot \frac{1}{q^{2(n+s)}} + \dots\right) = \\ &= Q\left(f, \frac{1}{q^{n+s}}\right) - q^s \cdot \left(Q\left(f, \frac{1}{q^{n+s}}\right) - 1\right). \end{aligned}$$

□

Lemma 4.6. *With the notation in the proof of Proposition 4.5, we have $\mu(V_m) = N_m \cdot \frac{1}{q^{nm}}$.*

Proof. Note that V_m is the preimage in \mathcal{O}_K^n of the subset

$$\{x \mid f(\text{mod } \mathfrak{m}_K^m)(x) = 0\} \subset (\mathcal{O}_K/\mathfrak{m}_K^m)^n.$$

But this is a disjoint union of N_m translates of the kernel of the natural mapping $\mathcal{O}_K^n \rightarrow (\mathcal{O}_K/\mathfrak{m}_K^m)^n$, i.e. a disjoint union of translates of $(\mathfrak{m}_K^m)^n$, from which the result follows using Lemma 2.4. □

Example 4.7. Let's verify the statement of Proposition 4.5 in the case of $f(x) = x^d$ for some positive integer d . We have seen before that

$$Z(f, s) = \frac{q - 1}{q - q^{-ds}}.$$

Rewriting this in terms of $t = q^{-s}$, we have

$$Z(f, t) = \frac{q - 1}{q - t^d}.$$

By the theorem we then have

$$Q(f, t) = \left(Z(f, qt) - \frac{1}{qt} \right) \cdot \left(\frac{qt}{qt - 1} \right) = \frac{qt - t - 1 + q^{d-1}t^d}{(1 - q^{d-1}t^d)(qt - 1)}.$$

This agrees with the examples above for $d = 1, 2$ (and also tells you what the answer should be in Exercise 4.3(1)).

Using the substitution $t = q^{-s}$, the result in Proposition 4.5 can be rewritten as

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

A more precise version of Theorem 4.4 is then given by the following:

Theorem 4.8. *Let K be a p -adic field, and $f \in \mathcal{O}_K[X_1, \dots, X_n]$. Then the zeta function*

$$Z(f, s) = \int_{\mathcal{O}_K} |f|^s d\mu$$

is a rational function of q^{-s} . Moreover, let $(a_1, b_1), \dots, (a_k, b_k)$ be the discrepancies associated to an embedded resolution of singularities of $(f = 0)$ (as in Remark 3.13). Then

$$Z(f, s) = \frac{P(q^{-s})}{(1 - q^{-a_1 s - b_1 - 1}) \cdot \dots \cdot (1 - q^{-a_k s - b_k - 1})},$$

where $P \in \mathbf{Z}[1/q][X]$. Consequently, the poles of $Z(f, s)$ occur among the values $-\frac{b_1+1}{a_1}, \dots, -\frac{b_k+1}{a_k}$.

Proof. Let $\pi : V \rightarrow K^n$ be an embedded resolution of singularities of $(f = 0)$, and let $X = \mathcal{O}_K^n \subset K^n$ and $Y = \pi^{-1}(X)$, so that we get a restriction $\pi : Y \rightarrow X$. We've seen that Y is a compact K -analytic manifold which is covered by disjoint compact open charts U_i on which in coordinates we have

$$\pi^* f = \mu(y) \cdot y_1^{a_1} \cdot \dots \cdot y_n^{a_n}$$

and

$$\pi^*(dx_1 \wedge \dots \wedge dx_n) = \nu(y) \cdot y_1^{b_1} \cdot \dots \cdot y_n^{b_n} \cdot (dy_1 \wedge \dots \wedge dy_n)$$

with $\mu(y) \neq 0$ and $\nu(y) \neq 0$ for all $y \in U_i$. By the change of variables formula, we have

$$Z(f, s) = \sum_i \int_{U_i} |\mu(y)|^s |\nu(y)| |y_1|^{a_1 s + b_1} \cdot \dots \cdot |y_n|^{a_n s + b_n} |dy_1 \wedge \dots \wedge dy_n|.$$

Note now that the functions $|\mu(y)|$ and $|\nu(y)|$ are locally constant on each U_i . By shrinking the U_i , we can then assume that they are in fact constant, say

$$|\mu| = q^{-a} \quad \text{and} \quad |\nu| = q^{-b}.$$

Since U_i can be identified with a polydisk P_i given by $|y_i| \leq q^{-k_i}$ for all i , we obtain that $Z(f, s)$ is a sum of terms of the form

$$q^{-as-b} \cdot \int_{P_i} |y_1|^{a_1 s + b_1} \cdot \dots \cdot |y_n|^{a_n s + b_n} |dy_1 \wedge \dots \wedge dy_n| =$$

$$\begin{aligned}
 &= q^{-as-b} \cdot \int_{|y_1| \leq q^{-k_1}} |y_1|^{a_1s+b_1} |dy_1| \cdot \dots \cdot \int_{|y_n| \leq q^{-k_n}} |y_n|^{a_ns+b_n} |dy_n| = \\
 &= q^{-as-b} \cdot \left(\frac{q-1}{q} \right)^n \cdot \frac{q^{-k_1(a_1s+b_1+1)}}{1 - q^{-(a_1s+b_1+1)}} \cdot \dots \cdot \frac{q^{-k_n(a_ns+b_n+1)}}{1 - q^{-(a_ns+b_n+1)}},
 \end{aligned}$$

where we use Exercise 3.10 for the last line. So the statement follows if we check that no extra poles can arise from the term involving q^{-as} (note that a and b can be negative). To this end, note that $(f \circ \pi)(P_i) \subset \mathcal{O}_K$, so that $|\pi^* f| \leq 1$ on P_i . This means that for every $y \in P_i$ we have

$$|\mu(y)| \cdot |y_1|^{a_1} \cdot \dots \cdot |y_n|^{a_n} \leq 1.$$

This is equivalent to

$$q^{-a-k_1a_1-\dots-k_na_n} \leq 1, \text{ i.e. } a + k_1a_1 + \dots + k_na_n \geq 0,$$

so indeed q^{-s} appears with a non-negative power in the numerator of the expression above. \square

Remark 4.9 (Monodromy conjecture). Going back to the statement of Theorem 4.8, most of the time the poles of the local zeta function do not account for all the values $-\frac{b_i+1}{a_i}$ (at an even more basic level, some of these values are not invariant with respect to the choice of embedded resolution). A deeper conjecture due to Igusa, called the *monodromy conjecture*, aims to identify these poles more precisely.

Here is a brief explanation. Consider f as a mapping $f : \mathbf{C}^n \rightarrow \mathbf{C}$, and fix a point $x \in f^{-1}(0)$. The *Milnor fiber* of f at x is

$$M_{f,x} := f^{-1}(t) \cap B_\varepsilon(x),$$

where $B_\varepsilon(x)$ is the ball of radius ε around x , and $0 < t \ll \varepsilon \ll 1$. It was shown by Milnor that as a C^∞ manifold $M_{f,x}$ does not depend on t and ε . Each lifting of a path in a small disk of radius t around $0 \in \mathbf{C}$ induces a diffeomorphism $M_{f,x} \rightarrow M_{f,x}$, whose action on the cohomology $H^i(M_{f,x}, \mathbf{C})$ for each i is called the *monodromy action*.

Conjecture 4.10 (Igusa's Monodromy Conjecture). *Let s be a pole of $Z(f, s)$. Then $e^{2\pi is}$ is an eigenvalue of the monodromy action on some $H^i(M_{f,x}, \mathbf{C})$ at some point of $x \in f^{-1}(0)$.*

This truly remarkable conjecture, known in only a few cases, relates number theoretic invariants of $f \in \mathbf{Z}[X_1, \dots, X_n]$ to differential topological invariants of the corresponding function $f : \mathbf{C}^n \rightarrow \mathbf{C}$. An even stronger conjecture relates the poles of $Z(f, s)$ to the roots of the so-called *Bernstein-Sato polynomial* of f .

5. WEIL'S MEASURE AND THE RELATIONSHIP WITH RATIONAL POINTS OVER FINITE FIELDS

Let K be a p -adic field, with ring of integers \mathcal{O}_K , and residue field $\mathcal{O}_K/\mathfrak{m}_K \simeq \mathbf{F}_q$. In the next chapter we will need a result of Weil, roughly speaking relating the p -adic volume of a K -analytic manifold to the number of points of the manifold over \mathbf{F}_q .

Let \mathcal{X} be a scheme over $S = \operatorname{Spec} \mathcal{O}_K$, flat of relative dimension n . Recall that the set of \mathcal{O}_K -points of \mathcal{X} is the set $\mathcal{X}(\mathcal{O}_K)$ of sections of the morphism $\mathcal{X} \rightarrow S$. We can also consider the set $\mathcal{X}(K)$ of K -points of \mathcal{X} , i.e. sections of the induced $X_K := \mathcal{X} \times_S \operatorname{Spec} K \rightarrow \operatorname{Spec} K$.

Exercise 5.1. (1) If \mathcal{X} is an affine S -scheme, then

$$\mathcal{X}(\mathcal{O}_K) = \{x \in \mathcal{X}(K) \mid f(x) \in \mathcal{O}_K \text{ for all } f \in \Gamma(\mathcal{X}, \mathcal{O}_{\mathcal{X}})\} \subset \mathcal{X}(K).$$

(2) If \mathcal{X} is proper over S , then $\mathcal{X}(\mathcal{O}_K) = \mathcal{X}(K)$. (Hint: use the valuative criterion for properness.)

Definition 5.2. Assume that \mathcal{X} is smooth over S . A *gauge form* on \mathcal{X} is a global section $\omega \in \Gamma(\mathcal{X}, \Omega_{\mathcal{X}/S}^n)$ which does not vanish anywhere on \mathcal{X} . Note that such a form exists if and only if $\Omega_{\mathcal{X}/S}^n$ is trivial; more precisely, we have an isomorphism

$$\mathcal{O}_{\mathcal{X}} \rightarrow \Omega_{\mathcal{X}/S}^n, \quad 1 \mapsto \omega.$$

(Therefore gauge forms always exist locally on \mathcal{X} .)

Weil's p -adic measure. We saw in §3 that if ω is a K -analytic n -form on $\mathcal{X}(K)$, one can associate to it a measure μ_{ω} . In a completely similar way, one can associate a measure μ_{ω} on $\mathcal{X}(\mathcal{O}_K)$ to any n -form $\omega \in \Gamma(\mathcal{X}, \Omega_{\mathcal{X}/S}^n)$. (Note that $\mathcal{X}(\mathcal{O}_K)$ is a compact space in the p -adic topology.) Although not important for our discussion here, following the arguments below one can see that when ω is a gauge form, the measure μ_{ω} can in fact be defined over the entire $\mathcal{X}(K)$. This is called the *Weil p -adic measure* associated to ω .

Theorem 5.3 (Weil, [We2] 2.25). *Let \mathcal{X} be a smooth scheme over S of relative dimension n , and let ω be a gauge form on \mathcal{X} , with associated Weil p -adic measure μ_{ω} . Then*

$$\int_{\mathcal{X}(\mathcal{O}_K)} d\mu_{\omega} = \frac{|\mathcal{X}(\mathbf{F}_q)|}{q^n}.$$

Proof. This is really just a globalization of the argument in Lemma 4.6. Consider the reduction modulo \mathfrak{m}_K map

$$\varphi : \mathcal{X}(\mathcal{O}_K) \longrightarrow \mathcal{X}(\mathbf{F}_q), \quad x \mapsto \bar{x}.$$

It is enough to show that for every $\bar{x} \in \mathcal{X}(\mathbf{F}_q)$, one has

$$\int_{\varphi^{-1}(\bar{x})} d\mu_{\omega} = \frac{1}{q^n}.$$

This follows from the following two observations. On one hand, we have a K -analytic isomorphism $\varphi^{-1}(\bar{x}) \simeq \mathfrak{m}_K^n$, since locally the mapping φ looks like $\mathcal{O}_K^n \rightarrow (\mathcal{O}_K/\mathfrak{m}_K)^n$. On the other hand, if we write in local coordinates $\omega = f(x) \cdot dx_1 \wedge \dots \wedge dx_n$, by virtue of the fact that ω is a gauge form we have that $f(x)$ is a p -adic unit for every x , so that $|f(x)| = 1$. This facts combined give

$$\int_{\varphi^{-1}(\bar{x})} d\mu_{\omega} = \int_{\mathfrak{m}_K^n} |dx_1 \wedge \dots \wedge dx_n| = \mu(\mathfrak{m}_K^n) = \frac{1}{q^n}.$$

□

Canonical measure. Let again \mathcal{X} be a smooth scheme over S , this time not necessarily endowed with a gauge form. One can nevertheless naturally produce a measure on $\mathcal{X}(\mathcal{O}_K)$ (but not necessarily on $\mathcal{X}(K)$ if \mathcal{X} is not proper over S) by gluing local measures given by gauge forms.

Consider a finite cover U_1, \dots, U_k of \mathcal{X} by Zariski open S -schemes such that for each i the line bundle $\Omega_{\mathcal{X}/S}^n$ is trivial over U_i , i.e. $\Omega_{\mathcal{X}/S}^n|_{U_i} \simeq \mathcal{O}_{U_i}$. This means that we can pick a gauge form ω_i on each U_i , with associated Weil measure μ_{ω_i} defined on $\mathcal{X}(K)$ as above. Consider its restriction to $\mathcal{X}(\mathcal{O}_K)$. Now any two gauge forms clearly differ by an invertible function, i.e. by a section $s_i \in \Gamma(U_i, \mathcal{O}_{U_i}^*)$, so that for any \mathcal{O}_K -point $x \in U_i$ we have $|s_i(x)| = 1$. Recalling how the measure associated to an n -form is defined in §3, this has the following consequences:

- The Weil measure μ_{ω_i} on $U_i(\mathcal{O}_K)$ does not depend on the choice of gauge form.
- These measures glue together to a global measure μ_{can} on the compact $\mathcal{X}(\mathcal{O}_K)$, called the *canonical measure*.

Weil's result Theorem 5.3 continues to hold in this setting.

Corollary 5.4. *Let \mathcal{X} be a smooth scheme over S of relative dimension n . Then*

$$\int_{\mathcal{X}(\mathcal{O}_K)} d\mu_{\text{can}} = \frac{|\mathcal{X}(\mathbf{F}_q)|}{q^n}.$$

Proof. Consider a Zariski-open covering U_1, \dots, U_k of \mathcal{X} as above, such that one has gauge forms on each U_i . Since μ_{can} is obtained by gluing the local Weil measures, we have

$$\int_{\mathcal{X}(\mathcal{O}_K)} d\mu_{\text{can}} = \sum_i \int_{U_i(\mathcal{O}_K)} d\mu_{\text{can}} - \sum_{i < j} \int_{(U_i \cap U_j)(\mathcal{O}_K)} d\mu_{\text{can}} + \dots + (-1)^k \int_{(U_1 \cap \dots \cap U_k)(\mathcal{O}_K)} d\mu_{\text{can}}.$$

Now for each of these integrals one can apply Theorem 5.3. The result follows by noting that by the inclusion-exclusion principle one has

$$|\mathcal{X}(\mathbf{F}_q)| = \sum_i |U_i(\mathbf{F}_q)| - \sum_{i < j} |(U_i \cap U_j)(\mathbf{F}_q)| + \dots + (-1)^k |(U_1 \cap \dots \cap U_k)(\mathbf{F}_q)|.$$

□

Let's conclude by noting a useful technical result which essentially says that proper Zariski closed subsets are irrelevant for the calculation of integrals with respect to the canonical measure.

Proposition 5.5. *Let \mathcal{X} be a smooth scheme over S , and let \mathcal{Y} be a reduced closed S -subscheme of codimension ≥ 1 . Then $\mathcal{Y}(\mathcal{O}_K)$ has measure zero in $\mathcal{X}(\mathcal{O}_K)$ with respect to the canonical measure μ_{can} .*

Proof. Using an affine open cover of \mathcal{X} , we can immediately reduce to the case when \mathcal{X} is a smooth affine S -scheme. Considering some hypersurface containing \mathcal{Y} , we can also reduce to the case of a principal divisor, i.e. $\mathcal{Y} = (f = 0)$ with $f \in \Gamma(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$

irreducible. By the Noether normalization theorem, we can then further assume that $\mathcal{X} = \mathbf{A}_{\mathcal{O}_K}^n = \text{Spec } \mathcal{O}_K[X_1, \dots, X_n]$ and $f = X_1$.⁴

To show that $\mu_{\text{can}}(\mathcal{Y}(\mathcal{O}_K)) = 0$, we will use a limit argument. Define for every integer $m \geq 1$ the subsets of $\mathbf{A}^n(\mathcal{O}_K)$

$$\mathcal{Y}_m(\mathcal{O}_K) := \{(x_1, \dots, x_n) \in \mathcal{O}_K^n \mid x_1 \in \mathfrak{m}_K^m\}.$$

Noting that $\cap_{m=1}^{\infty} \mathfrak{m}_K^m = 0$, we have

$$\mathcal{Y}(\mathcal{O}_K) = \bigcap_{m=1}^{\infty} \mathcal{Y}_m(\mathcal{O}_K).$$

It suffices then to show

$$\int_{\mathcal{Y}(\mathcal{O}_K)} d\mu_{\text{can}} = \lim_{m \rightarrow \infty} \int_{\mathcal{Y}_m(\mathcal{O}_K)} d\mu_{\text{can}} = 0.$$

But each one of the terms in the limit can be easily computed using Fubini:

$$\int_{\mathcal{Y}_m(\mathcal{O}_K)} d\mu_{\text{can}} = \int_{\mathfrak{m}_K^m} |dx_1| \cdot \prod_{i=2}^n \int_{\mathcal{O}_K} |dx_i| = \frac{1}{q^m},$$

hence the limit is indeed equal to zero. □

REFERENCES

- [BS] S. I. Borevich and I. R. Shafarevich, *Zahlentheorie*, Birkhäuser, 1966. 15
- [Ha] R. Hartshorne, *Algebraic Geometry*, Springer, 1977. 13
- [Ig] J. Igusa. *Introduction to the theory of local zeta functions*, Studies in Advanced Mathematics **14**, 2000. 1, 6, 8, 10, 16
- [La] R. Lazarsfeld, Lectures from a course at Univ. of Michigan, private communication. 8
- [Ma] H. Matsumura, *Commutative ring theory*, Cambridge Univ. Press, 1986. 2
- [Ne] J. Neukirch, *Algebraic number theory*, Springer, 1999. 1, 5
- [RV] D. Ramakrishnan and R. J. Valenza, Fourier analysis on number fields, Springer, 1999. 6
- [duS] M. P. F. du Sautoy, Zeta functions of groups: the quest for order versus the flight from ennui, Groups St. Andrews 2001 in Oxford. Vol. I, London Math. Soc. Lecture Note Ser. **304**, Cambridge Univ. Press, 2003, 150–189. 8
- [We1] A. Weil, *Basic number theory*, Academic Press, 1971. 1, 6, 8
- [We2] A. Weil, *Adèles and algebraic groups*, Progr. Math. **23**, Birkhäuser, Boston, 1982. 20

⁴Exercise: do this carefully, as we are not directly applying the usual Noether normalization for a finitely generated algebra over a field.