Eötvös Loránd University

Faculty of Sciences

Department of Algebra and Number Theory

p-adic analysis and zeta functions

Supervisor:
Dr. Zabradi Gergely
Associate Professor

Author:
Ritoprovo Roy
Pure Mathematics, MSc

Budapest, 2023

Contents

Chapter 1

Introduction

1.1 p-adic numbers and the metric formulation on $\mathbb{Q}$

Definition 1. A *norm* or *valuation* of a field $\mathbb{F}$ is a map $\|.\| : \mathbb{F} \to \mathbb{R}^+ \cup \{0\}$ that satisfies

- $\|x\| = 0$ iff $x = 0$
- $\|xy\| = \|x\|\|y\|$
- $\|x + y\| \leq \|x\| + \|y\|$ (Triangle Inequality)

The pair $(F, \|.\|)$ is called a valued field.

We can use norms to induce metric by setting

$$d(x, y) = \|x - y\|$$

The usual absolute value is a norm on $\mathbb{Q}$ with the usual distance metric induced by the absolute value norm. We try to construct a new norm in the following way:

Let p be a prime number and for each $x \in \mathbb{Q}$ we write x in the following way

$$x = p^{v_p(x)} x_1$$

where v_p is the highest power of p dividing x and x_1 is a rational number co-prime to p. We now define a norm on $\mathbb{Q}$ given by

$$\|x\|_p = p^{-v_p(x)} \tag{1.1}$$

It is easy to check that such a definition satisfies the properties in accordance with the definition above.

1.2 Ultrametric(The Strong Triangle Inequality)

We observe that our definition in Eqn.(1.1) satisfies a much stronger condition than triangle inequality

$$\|x+y\|_p \leq \max(\|x\|_p, \|y\|_p)$$

A simple example of a valuation that satisfies a similar criterion is the following

For a non-zero polynomial $f \in \mathbb{R}[X]$ given by

$$f = a_0 + a_1 x + a_2 x^2 + \ldots a_n X^n$$

$\deg(f) = n$ and $\deg(f) = -\infty$ if f is the zero polynomial.

We observe that this satisfies the valuation as well as the ultrametric property and valuation. Except for the fact here it is no more a valuation *field* but more of a valuation *ring*.

The definition of the metric given above in (1.1) is the $p-$adic metric and will be denoted by $|.|_p$ in future. We now state a strong characterisation theorem due to Ostrowski in 1918. We first start by defining what we mean by equivalent metrics,

Definition 2. Two metrics d_1 and d_2 on the same set are said to be equivalent if they induce the same topology on the set.

1.3 The Theorem of Ostrowski and Metric over $\mathbb{Q}_p$

We now proceed to state the theorem we were building up on,

Theorem 1 (Ostrowski, 1918)**.** *Every non-trivial norm $\|.\|$ on $\mathbb{Q}$ is equivalent to $|.|_p$ for some prime p or the usual absolute value.*

Given a field F with norm $\|.\|$, let R be the set of all sequences with $\{a_n\}_{n=1}^{\infty}$, $a_n \in \mathbb{F}$, which are Cauchy with respect to the given norm. Then we can define

$$\begin{aligned} \{a_n\}_{n=1}^{\infty} + \{b_n\}_{n=1}^{\infty} &= \{a_n + b_n\}_{n=1}^{\infty} \\ \{a_n\}_{n=1}^{\infty} \times \{b_n\}_{n=1}^{\infty} &= \{a_n \times b_n\}_{n=1}^{\infty} \end{aligned}$$

Thus $(R, +, \times)$ is a commutative ring. Moreover, the set $\mathbb{M}$ of all Cauchy sequences converging to zero is a maximal ideal, and hence $\frac{R}{\mathbb{M}}$ is a field.

We can embed F in R via the natural map $a \rightarrow (a, a, a, \dots)$, which is clearly a Cauchy Sequence. We can therefore view F as a subfield of $\frac{R}{\mathbb{M}}$. $\frac{R}{\mathbb{M}}$ is called the completion of the field F with respect to the given norm. In the case $F = \mathbb{Q}$ when our norm is usual norm, our completion is the set of real numbers $\mathbb{R}$. On the other hand if $F = \mathbb{Q}$, and the metric is $\|.\|_p$, the completion is $\mathbb{Q}_p$, of p-adic numbers.

We can extend the norm on Q_p as follows, given any equivalence class of sequences $a = \{a_n\}_{n=1}^{\infty}$ in $\mathbb{Q}_p$, we can see that $\{|a_n|_p\}_{n=1}^{\infty}$ is a Cauchy sequence in $\mathbb{R}$ and as reals are complete we have a limit and let it be a so that

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

We can easily check that the above is well-defined, and moreover $\mathbb{Q}_p$ is complete in $|.|_p$. Indeed, let $\{a^{(j)}\}_{j=1}^{\infty}$, be a Cauchy sequence of equivalence classes in $\mathbb{Q}_p$, we must show that there is a Cauchy sequence to which it converges. To achieve this we observe that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Thus we can find a rational number $^{(j)}$ so that

$$\lim_{n\rightarrow\infty} |a^{(j)} - \lambda^{(j)}|_p = 0$$

and this implies what we needed to complete our assertion.

Chapter 2

Geometry, Arithmetic in $\mathbb{Q}_p$ and the Hensel's Lemma

2.1 The interesting Geometry of $\mathbb{Q}_p$

The field $\mathbb{Q}_p$, has interesting geometry induced to it by the metric topology. We recall from the last chapter that our metric induces a so called "ultrametric topology" on $\mathbb{Q}$. Two of the very famous observations are

Theorem 2. *All triangles in ultrametric spaces are isoceles.*

This in the first sense quite counter-intuitive, but the proof can be observed easily by considering the metrics over the valuations, and going on routine calculations and observations.

For non-archimedean valuations, an interesting observation in terms on topology is the following,

Theorem 3. *Let $\mathbb{K}$ be a with a non-archimedean absolute valuation. Then we have the following,*

- *Every point that is present in an open(closed) ball, is the center of the ball.*
- *All balls are both open or closed.*
- *Any two open balls are either disjoint or contained in one-another.*
- *K is a totally disconnected topological space.*

2.2 Arithmetic in $\mathbb{Q}_p$ and the Hensel's Lemma

The mechanics of addition, subtraction, multiplication and long division in $\mathbb{Q}_p$ is similar to elementary school arithmetic methods, except for the fact that the "carrying" and "borrowing" goes from left to right rather than right to left.

Although however, an important aspect is to find roots of polynomials in $\mathbb{Q}_p$. This is indeed the most useful method to find out existence of n^{th} roots of number in the field. It is tackled by a well know result stated below,

Theorem 4 (Hensel's Lemma)**.** *Let $F(x) = c_0+c_1x+c_2x^2+\cdots+c_nx^n$ be a polynomial whose coefficients are p-adic integers. Denote $F'(x)$ to be the natural derivative of F. Let a_0 be the p-adic integer such that $F(a_0) \equiv 0 \ (mod\ p)$ and $F'(a_0) \not\equiv 0 \ (mod\, p)$. Then there exists a unique p-adic integer a such that*

$$F(a) = 0 \quad \textit{and} \quad a \equiv a_0 \ (mod \ \ p)$$

We discuss a special case where we investigate the existence of $\sqrt{6}$ in $\mathbb{Q}_5$. For that we consider the polynomial

$$F(x) = x^2 - 6 \quad \text{and} \quad F'(x) = 2x$$

and we let $a_0 = 1, 4$(as these are the only possibilities). And we see our unique in the respective cases are $4, 1$.

Chapter 3

p-adic interpolation of the zeta function

The aim of this chapter to establish the so called p-adic continuity for the ζ values at even integers.

Definition 3. The Riemann ζ-function is defined by the Dirichlet Series for $\mathrm{Re}(s) > 1$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

We fix a prime p. Let us consider the set of numbers

$$f(2k) = (1 - p^{2k-1})\frac{c_k}{\pi^{2k}}\zeta(2k), \quad \text{where} \quad c_k = (-1)^k \frac{(2k-1)!}{2^{2k-1}}$$

as $2k$ runs through all positive even integers in the same congruence class $\mathrm{mod}(p-1)$. It turns out that $f(2k)$ is always a rational number. Moreover if two such numbers are p-adically close(i.e their difference is divisible by a large power of p), then we shall see that ther corresponding $f(2k)$ is also p-adically closed. This means we can uniquely extend f from integers to p-adic integers and the resulting function is continuous in $\mathbb{Q}_p$, which essentially is what I meant by p-adic interpolation.

3.1 A formulae for $\zeta(2k)$

Definition 4. The k^{th} Bernoulli number denoted by B_k, is defined as $k!$ times the k^{th} coefficient of the Taylor expansion of the function

$$\frac{t}{e^t - 1}$$

That is to say $\frac{t}{e^t-1} = \frac{1}{1+\sum_{k=1}^{\infty} \frac{t^k}{(k+1)!}} = \sum_{k=0}^{\infty} B_k x^k$

Our main aim is to derive the formulae

$$\zeta(2k) = (-1)^k(\pi)^{2k}\frac{2^{2k-1}}{2k-1}(-\frac{B_{2k}}{2k})$$

Theorem 5. *For all $x \in \mathbb{R}$, the infinite product*

$$\pi x \prod_{n=1}^{\infty}(1 + \frac{x^2}{n^2})$$

converges and equals to $sinh(x)$.

The proof follows easily from logarithmic test.

Theorem 6. *Let $n = 2k + 1$ be an odd positive integer, then we can write*

$$\begin{aligned} sin(nx) &= P_n(sinx) \\ cos(nx) &= cosxQ_{n-1}(sinx) \end{aligned}$$

where P_n and Q_n are polynomials of degree n.

The proof readily follows from induction. Using the above two lemmas we can now prove our main result.

3.2 p-adic Interpolation $\zeta(s)$ function(Construction of Kubota-Leopoldt L-functions)

We now try to interpolate the zeta function. The naive way to interpolate $\zeta(s)$, p-adically is to interpolate through each term individually and then add out the result. Unfortunately this fails to work because even the terms which can be interpolated, those for which p does not divide n forms an infinite divergent sum in Z_p.

We can artificially remove the terms $\frac{1}{n^s}$, with n divisible by p,

$$\begin{aligned} \zeta(s) &= \sum_{n=1,p\not| n}^{\infty} \frac{1}{n^s} + \sum_{n=1,p|n} \frac{1}{n^s} \\ &= \sum_{n=1,p\not| n}^{\infty} \frac{1}{n^s} + \sum_{n=1} \frac{1}{p^s n^s} \\ &= \sum_{n=1,p\not| n} \frac{1}{n^s} + \frac{1}{p^s}\zeta(s) \\ \implies \zeta(s) &= \frac{1}{1-(1/p^s)} \sum_{n=1,p\not| n} \frac{1}{n^s} \end{aligned}$$

To evaluate the last term, we use the popular identity

$$\zeta(s) = \prod_p \frac{1}{(1-p^{-s})}$$

Thus multiplying by $\zeta(s)$ amounts to removing the p-Euler factors and hence we get the relation

$$\zeta^*(s) = \sum_{n=1,p\not| n} \frac{1}{n^s} = \prod_p \frac{1}{(1-p^{-s})}\zeta(s)$$

The next thing we want to do is fix $s_0 \in \{0, 1, 2, \ldots, p-1\}$ and only let s vary over non-negative integers $s \in \{s | s \equiv s_0 \pmod{(p-1)}\} = S_{s_0}$. As a result we get the numbers we saw previously as $(-\frac{B_{2k}}{2k})$, when multiplied by $(1-p^{2k-1})$, can be interpolated for $2k \in S_{2s_0}$.

More precisely it can be seen that, if $2k, 2k' \in S_{2k_0}$, and if $k \equiv k' \pmod{p^N}$ then,

$$(1-p^{2k-1})(-\frac{B_{2k}}{2k}) \equiv (1-p^{2k'-1})(-\frac{B_{2k'}}{2k'}) \pmod{p^{N+1}}$$

These congruences were observed by Kummer a long time ago, but the p-adic foundations using the interpolation of zeta functions was laid much later by Kubota and Leopoldt.

Chapter 4

p-adic measures, distributions and Iwasawa Algebras

4.1 Power series rings and p-adic measures

Let $K/\mathbb{Q}_p$ be a finite extension. Let O_K be the valuation ring of K and let π be a uniformizer of O_K. Let $k = O_K/(\pi)$ be the residue field of O_K which is a finite extension of $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Our main goal in this chapter is to understand the following diagram(diagram 4.1).

To begin with, we state some basic properties of power series ring,

Theorem 7 (Division Lemma)**.** *Suppose* $f = a_0 + a_1T + \cdots \in O_K[|T|]$*, but* $\pi \nmid f$*, i.e,* $f \notin O_K[|T|]$*. Let* $n = min\{i : a_i \notin (\pi)\}$*. Then any* $g \in O_K[|T|]$ *can be uniquely*

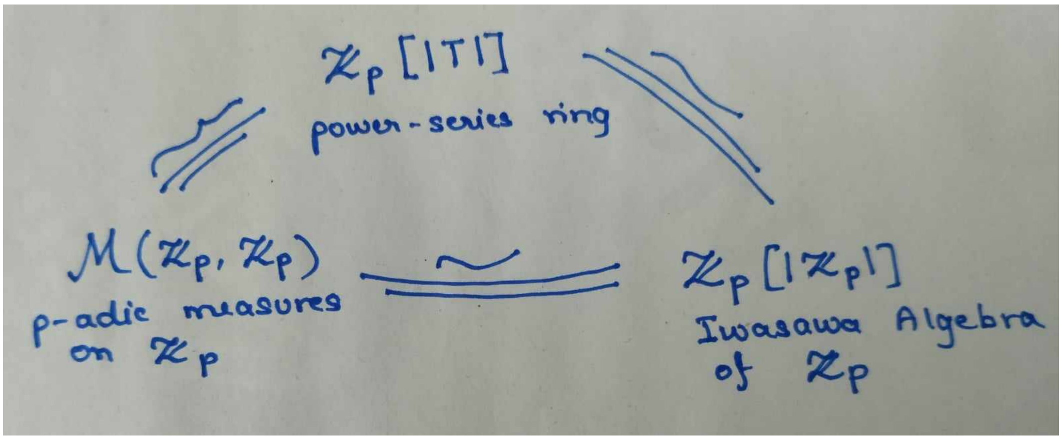

Figure 4.1: Relationship diagram between power series rings, p-adic measures and Iwasawa Algebra

written as $q = qf + r$ *where* $q \in O_K[|T|]$, *and* $r \in O_K[T]$ *is a polynomial of degree atmost* $n-1$.

We have an important note,

Note. If $\pi \not| f \in O_K[|T|]$, then $O_K[|T|]/(f)$ is a free O_K module of rank $n = \{\inf i : a_i \notin (\pi)\}$, with the basis $\{T^i | i < n\}$.

Definition 5. A distinguished polynomial $F(T) \in O_K[T]$ is a polynomial of the form

$$F(T) = T^n + a_{n-1}T^{n-1} + \dots a_0, \quad a_i \in (\pi)$$

Remark. We allow $\pi^2 | a_0$ as to avoid for any irreducibility case due to Eisenstein criterion.

We now towards a major important theorem of this chapter,

Theorem 8 (p-adic Weirestrass Preparation Theorem)**.** *Let* $f \in O_K[|T|]$, *then* f *can be uniquely written as*

$$f = \pi^\mu P(T)U(T)$$

is a distinguished polynomial of degree $n = \{\mathit{inf}\ i : \mathit{ord}_\pi(a_i) = \mu\}$, $U(T)$ *is unit in* $O_K[|T|]$. *As a consequence,* $O_K[|T|]$ *is a factorial domain.*

We omit the proof of this theorem, but I would like to mention that this theorem is as a consequence of the Division Lemma we proved before. However an important remark related to this.

Remark. For $\pi \not| f$, we have as a consequence

$$O_K[|T|]/(f(T)) \cong O_K[|T|]/(P(T))$$

Thus $P(T)$ is the characteristic polynomial of the linear transformation $T : O_K[|T|]/(f) \to O_K[|T|]/(f)$.

An important thing to note,

Note. Let $f(T) \in O_K[|T|]$, be non-zero. Then there can only be finitely many $x \in C_p$, $|x| < 1$ with $f(x) = 0$.

Another important note is the following,

Note. Let $P(T)$ be the distinguished polynomial. If $\frac{g(T)}{P(T)} \in O_K[|T|]$, $g(T) \in O_K[T]$ then $g(T) \in O_K[T]$.

We are now in a position to arrive at Iwasawa Algebras.

4.2 Iwasawa Algebras

Let $\Gamma = \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, where the inverse limit is taken on n, where Γ is compact and pro-cyclic as a profinite group. Let γ be a topological generator of Γ and hence $\Gamma =< \bar{\gamma} >$. Let Γ_n be generated by γ^{p^n}, and this be the unique closed group of index p^n of Γ, then Γ/Γ_n, is cyclic of order p^n generated by $r + \Gamma_n$. One has isomorphism

$$\begin{array}{rcl} O_K[\Gamma/\Gamma_n] & \cong & O_K[\Gamma]/((1+T)^{p^n} - 1) \\ \gamma_n \mod \Gamma_n & \to & (1+T) \mod ((1+T)^{p^n} - 1) \end{array}$$

Moreover, if $m \geq n \geq 0$, the natural map of $\Gamma/\Gamma_m \to \Gamma/\Gamma_n$ induces a natural map,

$$\phi_{m,n} : O_K[\Gamma/\Gamma_m] \to O_K[\Gamma/\Gamma_n]$$

We let

$$O_K[|\Gamma|] = \varprojlim O_K[\Gamma/\Gamma_n] = \varprojlim O_K[\Gamma]/((1+T)^{p^n} - 1)$$

where the limits are taken on n.

We finally note that O_K is a topological ring which is compact and complete with the π-adic topology, so are $O_K[\Gamma/\Gamma_n]$ and thus $O_K[|\Gamma|]$ is the endowed with the product topology of π-adic topology. It is also compact and complete in this topology.

Definition 6.

$$\Lambda = \Lambda(\Gamma) = O_K[|\Gamma|]$$

is defined to be the Iwasawa Algebra on Γ

We complete this section by stating an important theorem,

Theorem 9. *One has a topological isomorphism*

$$\begin{array}{rcl} O_K[||T|] & \cong & O_K[|\Gamma|] \\ T & \to & \gamma - 1 \end{array}$$

where $O_K[|T|]$ is the compact topological ring complete with π-adic topology.

We omit the proof of this theorem, as this can be established by induction.

4.3 p-adic measures

We begin with a useful result.

Theorem 10. *Any compact subset of $\mathbb{Q}_p$, can be expressed as a finite disjoint union of intervals $a + p^N\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x - a|_p \leq \frac{1}{p^N}\}$*

The proof of this theorem follows by a direct application of compactness definition.

Definition 7.

- Let X be a compact open subset of $\mathbb{Q}_{|}$. A p-adic distribution μ on X, is an additive map from the compact open set in X to $\mathbb{Q}_p$, i.e if U is compact open in X and is a finite disjoint union of compact open subsets $\{U_i\}_{i=1}^n$ then

$$\mu(U) = \sum_{i=1}^{n} U_i$$

- A p-adic distribution μ on X is called a measure if there exists a positive real number M, such that $|\mu(U)| \leq M$ for all compact open sets in U in X.

Theorem 11. *Let μ be a map from the set of compact open subsets in X, to $\mathbb{Q}_p$ such that*

$$\mu(a + p^N) = \sum_{b=0}^{p-1} \mu(a + bp^N + P^{N+1})$$

for any interval $a + p^N$ in X. Then μ extends uniquely to a p-adic distribution in X.

We end the discussion by stating that there are indeed various types of measures, the Haar distribution, The Mazur distribution and the Bernoulli distribution, specifics of which will be discussed in detail later.

Chapter 5

Conclusion

The idea behind this project is to the study on methods on Modern Number Theory. Much of modern number theory is dedicated to understand the structure of the Galois group,

$$G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

or in general if we replace $\mathbb{Q}$ by any number field K. This actually formally paves the way to the study of Local and Global Class Field Theory which will be covered in the final presentation on the topic. The text studied some formal methods of advancements in the direction of Number Theory, and much of the current research is based on these methods applied over and over again. Finally I would like to conclude with two quotes by famous mathematicians Gauss and Erdos,

"Mathematics is the Queen of all Sciences and Number Theory is the Queen of Mathematics" - C.F Gauss

"If numbers aren't beautiful then what is" - Paul Erdos

Acknowledgements

I would like to thank Professor Zabradi Gergely, my supervisor for this project, who introduced me to this topic and methods discussed here. I would also like to convey sincere thanks to Professor Istvan Agoston, for giving me this opportunity for directed studies. Last but not the least I would like to thanks Professor Arpad Toth, as his course on Special Functions exposed me to much of the topics in zeta functions which is discussed here.