p-adic analysis and zeta functions

Institute of Mathematics, Eötvös Loránd Tudományegyetem

Ritoprovo Roy

January 9, 2024

A Little Bit of History

We begin with a little bit of history in order to spark up the interest

A Little Bit of History

We begin with a little bit of history in order to spark up the interest

- In the year of 1897, **Hensel** came up with the concept of p-adic numbers.

A Little Bit of History

We begin with a little bit of history in order to spark up the interest

- In the year of 1897, **Hensel** came up with the concept of p-adic numbers.
- A formalisation was done by **Ostrowski**, and he classified the norm on $\mathbb{Q}$. His theorem, upgraded the view of p-adic's from a mere subset of rationals to a subset of topological spectrum over rationals.

A Little Bit of History

We begin with a little bit of history in order to spark up the interest

- In the year of 1897, **Hensel** came up with the concept of p-adic numbers.
- A formalisation was done by **Ostrowski**, and he classified the norm on $\mathbb{Q}$. His theorem, upgraded the view of p-adic's from a mere subset of rationals to a subset of topological spectrum over rationals.
- In the later part of 20^{th} century a much more wider spectrum from **Kubota** and **Leopoldt** was established bringing out it's importance in number theory.

A Little Bit of History

We begin with a little bit of history in order to spark up the interest

- In the year of 1897, **Hensel** came up with the concept of p-adic numbers.
- A formalisation was done by **Ostrowski**, and he classified the norm on $\mathbb{Q}$. His theorem, upgraded the view of p-adic's from a mere subset of rationals to a subset of topological spectrum over rationals.
- In the later part of 20^{th} century a much more wider spectrum from **Kubota** and **Leopoldt** was established bringing out it's importance in number theory.
- Formally, given a prime number p, a p-adic number can be defined as a series (for $k \in \mathbb{Z}$ and $0 < a_i < p$)

$$s = \sum_{i=k}^{\infty} a_i p^i$$

Introduction to p-adic numbers

Motivation, An overview of p-adic numbers and metric formulation on $\mathbb{Q}$ and $\mathbb{Q}_p$

Motivation

We use two different directions to motivate us to go into p-adic numbers,

Motivation

We use two different directions to motivate us to go into p-adic numbers,

- Solving Polynomial Equations.

Motivation

We use two different directions to motivate us to go into p-adic numbers,

- Solving Polynomial Equations.
- Completing the number system i.e, finding limits to all Cauchy Sequences.

Motivation

We use two different directions to motivate us to go into p-adic numbers,

- Solving Polynomial Equations.
- Completing the number system i.e, finding limits to all Cauchy Sequences.

Let us recall the construction of $\mathbb{R}$,

Motivation

We use two different directions to motivate us to go into p-adic numbers,

- Solving Polynomial Equations.
- Completing the number system i.e, finding limits to all Cauchy Sequences.

Let us recall the construction of $\mathbb{R}$,

Solving Equations

Linear Equations

$x + a = 0$, $ax = b$

Quadratic Equations

$x^2 - a = 0$

Motivation

We use two different directions to motivate us to go into p-adic numbers,

- Solving Polynomial Equations.
- Completing the number system i.e, finding limits to all Cauchy Sequences.

Let us recall the construction of $\mathbb{R}$,

Solving Equations

Linear Equations

$x + a = 0$, $ax = b$

Quadratic Equations

$x^2 - a = 0$

Cauchy Sequences via completion

Let S be the set of all Cauchy Sequences of rational numbers. We say two sequence $\{a_i\}$ and $\{b_i\}$ are equivalent($\sim$) iff $|a_i - b_i| \to 0$ as $i \to \infty$. This is an equivalent relation. One can observe that $\mathbb{R} = S/\sim$ i.e set of all equivalence classes of S.

Motivation (Contd.....)

- But still we are not done. Going by approach of algebraically closeness we still don't have answer to $x^2 + 2 = 0$.

Motivation (Contd.....)

- But still we are not done. Going by approach of algebraically closeness we still don't have answer to $x^2 + 2 = 0$.
- So we define $\mathbb{C} = \{a + ib | a, b \in \mathbb{R}\}$, and by fundamental theorem of algebra $\mathbb{C}$ is algebraically closed.

Motivation (Contd.....)

- But still we are not done. Going by approach of algebraically closeness we still don't have answer to $x^2 + 2 = 0$.
- So we define $\mathbb{C} = \{a + ib | a, b \in \mathbb{R}\}$, and by fundamental theorem of algebra $\mathbb{C}$ is algebraically closed.
- We also see that with respect to $\mathbb{C}$ is also closed with respect to the norm, $|a + ib| = a^2 + b^2$.

Motivation (Contd.....)

- But still we are not done. Going by approach of algebraically closeness we still don't have answer to $x^2 + 2 = 0$.
- So we define $\mathbb{C} = \{a + ib | a, b \in \mathbb{R}\}$, and by fundamental theorem of algebra $\mathbb{C}$ is algebraically closed.
- We also see that with respect to $\mathbb{C}$ is also closed with respect to the norm, $|a + ib| = a^2 + b^2$.

As a result $\mathbb{C}$ is our finish point.

Motivation (Contd.....)

- We follow a similar approach for defining a metric on $\mathbb{Q}$.

Approach

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

$$\mathbb{Q} \subset \mathbb{Q}_p \subset \bar{\mathbb{Q}}_p \subset \mathbb{C}_p$$

Introduction

Norm/Valuation

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)

Introduction

Norm/Valuation

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.

Introduction

Norm/Valuation

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

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

Introduction (Contd……)

- The usual absolute value is a norm on $\mathbb{Q}$ with the usual distance metric induced by the absolute value norm.

Introduction (Contd……)

- 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.

The Ultrametric Property

- One says that a valuation satisfies the ultrametric property, if it also satisfies the property,

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

The Ultrametric Property

- One says that a valuation satisfies the ultrametric property, if it also satisfies the property,

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

For example:

Defining the metric

Let ρ be any real number. We can now define the metric on $\mathbb{R}[X]$

$$|f| = \begin{cases} 0 & f = 0 \\ \rho^{d(f)} & f \neq 0 \end{cases}$$

Degree of polynomial

For a non-zero polynomial $f \in \mathbb{R}[X]$, we set

$$d(f) = \begin{cases} n & f(x) = a_0 + a_1 x + \ldots a_n x^n, \quad a_i \neq 0 \quad \forall i \\ -\infty & f(x) = 0 \end{cases}$$

The Topology and Arithmetic in $\mathbb{Q}_p$

The geometry, arithmetic and the Hensel's lemma

The Metric Structure

- We induce a metric structure on $\mathbb{Q}_p$,

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

The Metric Structure

- We induce a metric structure on $\mathbb{Q}_p$,

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

- We can check that this does satisfies the property of metrics.

The Metric Structure

- We induce a metric structure on $\mathbb{Q}_p$,

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

- We can check that this does satisfies the property of metrics.
- We also have a stronger property than triangle inequality,

$$d(x,y) \leq \max(d(x,y), d(x,z))$$

The Metric Structure

- We induce a metric structure on $\mathbb{Q}_p$,

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

- We can check that this does satisfies the property of metrics.
- We also have a stronger property than triangle inequality,

$$d(x,y) \leq \max(d(x,y), d(x,z))$$

The Geometry

- The structure of $\mathbb{Q}_p$, becomes interesting and counter-intuitive in some eyes.
- One can show that all triangles in this system are isoceles.
- Yet another interesting property, lies with topological concepts of open and closed balls

Structure of balls

Let K be a field with a non-archimedian absolute value then

— Every point that is contained in an open(closed) ball is the center of that ball.

— Every ball is both open and closed.

— Any two open(closed) balls are either disjoint or one is contained in another.

Arithmetic in $\mathbb{Q}_p$

The general arithmetic in $\mathbb{Q}_p$, is very usual as in our normal arithmetic except for the fact that, ”carrying”, ”borrowing” and ”long multiplication” go from left to right, rather than right to left.

$$
\begin{array}{rrrrrrrrrr}
 & 3 & + & 6 \times 7 & + & 2 \times 7^2 & + & \cdots \\
\times & 4 & + & 5 \times 7 & + & 1 \times 7^2 & + & \cdots \\
\hline
 & 5 & + & 4 \times 7 & + & 4 \times 7^2 & + & \cdots \\
 & & & 1 \times 7 & + & 4 \times 7^2 & + & \cdots \\
 & & & & & 3 \times 7^2 & + & \cdots \\
\hline
 & 5 & + & 5 \times 7 & + & 4 \times 7^2 & + & \cdots
\end{array}
$$

Figure: Arithmetic in $\mathbb{Q}_p$

Finding n^{th} roots in $\mathbb{Q}_p$

- A rather interesting topic is to find n^{th} roots in $\mathbb{Q}_p$.

Finding n^{th} roots in $\mathbb{Q}_p$

- A rather interesting topic is to find n^{th} roots in $\mathbb{Q}_p$.
- For example $\sqrt{6}$ in $\mathbb{Q}_5$ is given by,

$$\sqrt{6} = 1 + 3 \times 5 + 0 \times 5^2 + 4 \times 5^3 + \dots$$

Finding n^{th} roots in $\mathbb{Q}_p$

- A rather interesting topic is to find n^{th} roots in $\mathbb{Q}_p$.
- For example $\sqrt{6}$ in $\mathbb{Q}_5$ is given by,

$$\sqrt{6} = 1 + 3 \times 5 + 0 \times 5^2 + 4 \times 5^3 + \dots$$

- In general our method, is based as follows, let $a_0 + a_1 \times 5 + a_2 \times 5^2 + a_3 \times 5^3 + \dots$ be the square root. Then we have,

$$(a_0 + a_1 \times 5 + a_2 \times 5^2 + a_3 \times 5^3 + \dots)^2 = 1 + 1 \times 5$$

Finding n^{th} roots in $\mathbb{Q}_p$

- A rather interesting topic is to find n^{th} roots in $\mathbb{Q}_p$.
- For example $\sqrt{6}$ in $\mathbb{Q}_5$ is given by,

$$\sqrt{6} = 1 + 3 \times 5 + 0 \times 5^2 + 4 \times 5^3 + \ldots$$

- In general our method, is based as follows, let $a_0 + a_1 \times 5 + a_2 \times 5^2 + a_3 \times 5^3 + \ldots$ be the square root. Then we have,

$$(a_0 + a_1 \times 5 + a_2 \times 5^2 + a_3 \times 5^3 + \ldots)^2 = 1 + 1 \times 5$$

- Comparing the coefficients(modulo 5) on both sides we get the result.

Hensel’s Lemma

- The above method is placed as a generalised lemma formulated by Hensel.

Hensel’s Lemma

Let $F(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots a_nx^n$ be a polynomial in p-adic integers. Let $F'(x)$ be the natural derivative of F. Let a_0 be the p-adic integer $F(a_0) \equiv 0 \pmod p$ and $F(a_0) \not\equiv 0 \pmod p$ then there exists a unique p-adic integer a such that

$$F(a) = 0, \quad a \equiv a_0 \pmod p$$

- For our case with 6 and $\mathbb{Q}_5$, we have $F(x) = x^2 - 6$, $F'(x) = 2x$ and $a_0 = 1$.

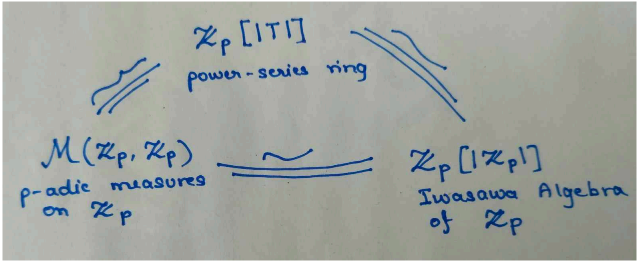
p-adic measures, distributions and Iwasawa Algebras

Power Series Rings, p-adic measures and Iwasawa Algebras

Setup and Introduction

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

Our main goal of this chapter is to understand the following,



Power Series Ring in p-adics

We begin with an important lemma,

Division Lemma

Suppose

$$f = a_0 + a_1T + a_2T^2 + \cdots \in O_K[|T|]$$

but $\pi \not| f$, 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 written as $q = qf + r$ where $q \in O_K[|T|]$, and $r \in O_K[T]$ is a polynomial of degree atmost $n - 1$.

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

Power Series Ring in p-adics

- We define the notion of a distinguished polynomial,

Distinguished Polynomial

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

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

- We allow $\pi^2 | a_0$ as to avoid for any irreducibility case due to Eisenstein criterion.
- An important implication from the theorem is, if F is a distinguished polynomial, then

$$O_K[T]/_F O_K[T] \simeq O_K[|T|]/_F O_K[|T|]$$

Power Series Ring in p-adics

- We begin with a rather important theorem,

p-adic Weirestrass Preperation 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 $n = \{\inf\ i : ord_{\pi}(a_i) = \mu\}$, $U(T)$ is unit in $O_K[|T|]$. As a consequence, $O_K[|T|]$ is a factorial domain.

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

Iwasawa Algebras - The Setup

- The theory of commutative Iwasawa algebras were first introduced by the Japanese mathematician Kenkichi Iwasawa.
- 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 $r + \Gamma_n$.

Iwasawa Algebras - The Setup

- One has isomorphism

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

- 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.

Iwasawa Algebras - The Setup

- 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.
- We are now in a position to define what Iwasawa Algebras are,

Iwasawa Algebras

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

is called the Iwasawa Algebra over Γ.

Iwasawa Algebra

- An important thing to note is that,

Iwasawa Algebra on Profinite Group

Let G be a profinite abelian group, then Iwasawa algebra over G is given by,

$$\Gamma(G) = \varprojlim O_K[G/H]$$

when limit is taken over all $H \lhd G$.

- In fact we are able to identify the rings $O_K[|\Gamma|]$ and $O_K[|T|]$.

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

p-adic measures

- We begin with an important lemma,

Lemma

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

p-adic distributions

p-adic distribution

- Let X be a compact open subset of $\mathbb{Q}_p$. 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.

p-adic distributions

- An important result in this direction is the following,

Theorem

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.

Interpolation and related results

Zeta function, p-adic interpolation of the zeta function, Kubota-Leopoldt constructions for p-adic analougues of zeta function, Kummer's congruence

The ζ function

- The Riemann-zeta function is defined as a function on $s \in \mathbb{C}$ by

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

- The above series converges absolutely for $\text{Re}(s) > 1$.
- We can also show that it has a meromorphic continuation to all of $\mathbb{C}$ with a simple pole at $s = -1$.

The Γ function

- For $s \in \mathbb{C}$ the gamma function is defined as

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{dt}{t}$$

- We have $\Gamma(s+1) = s\Gamma(s)$ for all Re$(s) > 0$
- $\Gamma(n) = (n-1)!$
- Using the fact that $\Gamma(s+1) = s\Gamma(s)$, we can extended it meromorphically to with simple poles at all negative integers.

Connecting ζ and Γ functions

- We let,

$$\Lambda(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$$

- We observe by a simple computation that,

$$\Lambda(s) = \Lambda(1-s)$$

  for all $s \in \mathbb{C}$ with Re$(s) > 1$.
- And as a consequence one gets that ζ, can be extended analytically onto $\mathbb{C}$, with a simple pole at $s = 1$, with residue 1.

Mellin Transform

Mellin Transform

Let $g : \mathbb{R}_{>0} \to \mathbb{C}$, be a function of rapid decay (i.e $|g(t)| << t^{-N}, N \geq 0$), then the Mellin transform of g is given by

$$M(g)(s) = \int_0^\infty g(t)t^s \frac{dt}{t}$$

We define the L-function as follows,

$$L(f; s) = \frac{1}{\Gamma(s)} M(f)$$

for a function $f : \mathbb{R}_{>0} \to \mathbb{C}$, be a function of rapid decay

Connecting the ζ and Γ (contd...)

An useful proposition

$L(f; s)$ converges and is holomorphic function for Re$(s) > 0$ and hans an analytic continuation to the whole of $\mathbb{C}$ and

$$L(f, -n) = (-1)^n \frac{d^n}{dt^n} f(0)$$

Connecting the ζ and Γ (contd...)

We now recall what Bernoulli numbers are,

Bernoulli Numbers

The k^{th} Bernoulli number, B_k is given by

$$F(t) = \frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$$

- For our f as above we have

$$(s-1)\zeta(s) = L(F, s-1)$$

Connecting the ζ and Γ (contd...)

An important Corollary

For $n \geq 0$, we have $\zeta(-n) = -\frac{B_{n+1}}{n+1}$
$\zeta(-n) = 0$, when $n \geq 2$ is an even integer.

For $k \geq 0$, we have $\zeta(2k) = (-1)^{k-1} \frac{(2\pi)^{2k}}{2.(2k)!} B_{2k}$.

The p-adic analogue of the ζ-function

- From our previous results, the p-adic analogue can be constructed in two ways
- First way:
  We observe that the set $\{-n : n \in \mathbb{Z}_{>0}\}$ is dense in $\mathbb{Z}_p$. We can exploit this fact and hope that if $1-n$ and $1-m$ are so called p-adically close, then so is $-\frac{B_n}{n}$ and $-\frac{B_m}{m}$ and hence would allow us to build the p-adic analogue via interpolation via measure. This is the method of Kubota-Leopoldt and Mazur.
- Second way:
  A much more direct method is to directly give a explicit formulae of p-adic L-function, which agrees with $\zeta(s)$ at almost all places except some modification at the negative integers. Such a construction was given by Washington.

The Kubota-Leopoldt construction

p-adic Bernoulli Distribution

We have

- The usual analogue of Bernoulli Distribution

$$\mu_k(a + p^n\mathbb{Z}_p) = p^{n(k-1)}B_k(\frac{a}{p^n})$$

- Regularized Bernoulli Distribution

$$\mu_{k,\alpha}(U) = \mu(U) - \alpha^k\mu_k(\alpha^{-1}U)$$

for any compact open set $U \subset \mathbb{Q}_p$ and $\alpha \in (\mathbb{Z}_p)^\times$.

The Kubota-Leopoldt construction (Contd.....)

We have two observations

- $\mu_{k,\alpha}$ is a p-adic measure.
- Let d_k = least common denominator of the coefficient of $B_k(x)$, then

$$d_k \mu_{k,\alpha}(a + p^n\mathbb{Z}_p) \equiv d_k k a^{k-1} \mu_{1,\alpha}(a + p^n\mathbb{Z}_p) \pmod{p^n}$$

An important theorem

If $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is a continuous function, then

$$\int_{\mathbb{Z}_p} f(x) d\mu_{k,\alpha}(x) = \int_{\mathbb{Z}_p} f(x) k x^{k-1} d\mu_{1,\alpha}(x)$$

The Kubota-Leopoldt construction (Contd.....)

An important corollary

For each $k \in \mathbb{N}$, and $\alpha \in (\mathbb{Z}_p)^\times$ is not a root of unity then,

$$B_k = \frac{k}{1-\alpha^n} \int_{\mathbb{Z}_p} x^{k-1} d\mu_{1,\alpha}(x)$$

- If $p|n$ then $f(s) = n^s$, does not extend to a continuous function of a p-adic variable, hence our naive approach won't work.
- We instead consider a much more constructive approach to get around it.
- We define:

$$\Lambda_{s_0} = \{s \in \mathbb{Z}_{>0} : s \equiv s_0 \mod p\}$$

The Kubota-Leopoldt construction (Contd.....)

- We consider the natural embedding

$$\begin{aligned}
\Lambda_{s_0} &\hookrightarrow \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \mathbb{Z}_p \\
\mathbb{Z}_{\geq 0} &\hookrightarrow \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \mathbb{Z}_p \\
n &\to ([n]_{p-1}, n)
\end{aligned}$$

The Kubota-Leopoldt construction (Contd.....)

An Important Lemma

If $p \not| n$, then $f(s) = n^s$ extends to a continuous analytic function on $\frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \mathbb{Z}_p$.

- So this suggest to shrink our domain to $(\mathbb{Z}_p)^\times$.

Defining the analogue

Let $\alpha \neq 1$ be a rational number and not divisible by p, then for any positive integer k we get,

$$\zeta_p(1-k) = \frac{1}{\alpha^{-k}-1} \int_{(\mathbb{Z}_p)^\times} x^{k-1} d\mu_{1,\alpha}$$

- One can check this is well-defined

The Kubota-Leopoldt construction (Contd.....)

- With a little manipulation, we can observe that,

$$\zeta_p(1-k) = (1-p^{k-1}) - \frac{B_k}{k}$$

- We are almost done except the continuity, which can achieved by the Kummer's congruences,

Kummer's Congruences

1. if $(p-1) \nmid k$ then $\frac{B_k}{k}$, is a p-adic integer.
2. if $(p-1) \nmid k$ and $k \equiv k' \mod (p-1)p^N$, then

$$(1-p^{k-1})\frac{B_k}{k} \equiv (1-p^{k'-1})\frac{B_k}{k'} \mod p^{N+1}$$

Kubota-Leoplodt p-adic L functions

We end our discussion with the Kubota-Leopoldt p-adic L functions.

Kubota-Leopoldt p-adic L functions

For any $\alpha \in \mathbb{Z}$, $\alpha \neq 1$ and $p \not| \alpha$ and for a fixed integer $s_0 \in \{0, 1, 2, \ldots, p-2\}$, then

$$\zeta_{p,s_0} = \frac{1}{\alpha^{-(s_0+(p-1)s)} - 1} \int_{(\mathbb{Z}_p)^\times} x^{s_0+(p-1)s-1} d\mu_{1,\alpha}$$

for any p-adic integer s except at $s = 0$, in case of $s_0 = 0$.

Washington's Construction

Let χ be a Dirichlet character of conductor f, and let F be some multiple of q and f.

$$L_p(s,\chi) = \frac{1}{F}\frac{1}{s-1}\sum_{a=1,\ p\nmid a}^{F} \chi(a) < a >^{1-s} \sum_{j=0}^{\infty} \binom{1-s}{j} (B_j)(\frac{F}{a})^j$$

Conclusion (Local and Global Class Field Theory)

Investigating into Local and Global Class Field Theories, Statement of the Iwasawa Main Conjecture

Summary of Local and Global Class Field Theory

- We have seen existence of a power series $g(T) \in \mathbb{Z}_p[|T|]$ (from the analytic side).
- Now we try to construct a similar set up from the algebraic set side.
- Our main goal in modern number theory is to study $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ or the same for any number field K.
- Standard method for gaining insight into the structure of G_K, on arithmetic objects related to K(Galois representations).
- Class Field Theory describes G_K^{ab} =max abelian quotient of G_K as a first step towards the understanding of G_K.

Summary of Local and Global Class Field Theory

- We know that for each integer $m > 1$, the cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is an abelian extension with Galois group $G = \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$.
- So we get a simple process to construct abelian extensions of $\mathbb{Q}$. We pick $m \geq 1$ and take any subfield of $\mathbb{Q}(\zeta_m)$.
- A remarkable result would in this direction is the Kronecker Weber theorem in 1853.

Kronecker Weber Theorem (Global)

Every finite abelian extension of $\mathbb{Q}$ lies in $\mathbb{Q}(\zeta_m)$.

Summary of Local and Global Class Field Theory

Kronecker Weber Theorem (Local)

Every finite abelian extension of $\mathbb{Q}_p$ lies in $\mathbb{Q}_p(\zeta_m)$.

- An interesting proposition is that, the global theorem is true iff the local theorem is true.
- Also if we let, $K/\mathbb{Q}_p$ be a cyclic extension of l^r, for some prime $l \neq p$, then $K \subset \mathbb{Q}_p(\zeta_m)$ for some $m \in \mathbb{Z}_{\geq 1}$.
- If we let $l = p$ as above, then too it holds similarly, but the approach to proof is different.

Summary of Local and Global Class Field Theory

- Our main approach is to provide an analogue of the Kronecker-Weber theorem for any general number field.
- We head to the more general theorem,

Summary of Local and Global Class Field Theory

Local Class Field Theory

Let $K/\mathbb{Q}_p$ be a finite extension, then there exists an unique isomorphism

$$\varphi : \hat{K^\times} \to G_K^{ab}$$

(called local Artin map), with the following propositions,

- for any uniformizer π of K, restriction of $\varphi(\pi)$ to the maximal unramified extension of K is the Frobenius element.
- for any finite abelian extension L/K, we have an isomorphism,

$$K^\times / N_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$$

Summary of Local and Global Class Field Theory

- A remarkable consequence of the Local Class Field Theory is as follows: if p and q are two primes such that $p \equiv q \pmod{n} \implies \text{Frob}_p = \text{Frob}_q$ in $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and conversely.
- Now the Global Kronecker Weber Theory implies that a similar thing holds for any abelian extension of $\mathbb{Q}$, i.e if $K/\mathbb{Q}$ is finite abelian, then there exists n such that $\text{Frob}_p = \text{Frob}_q$, whenever $p \equiv q \pmod{n}$.
- This statement helps us get moving towards the global Class Field Theory.

Summary of Local and Global Class Field Theory

The Global Class Field Theory

(Reciprocity) L/K finite abelian and let $S =$set of primes of K ramifying in L, then there exists a modulus m of K, prime to S, such that the Artin map induces a surjection

$$c_m \to \text{Gal}(L/K)$$

Moreover it induces an isomorphism,

$$I^S/(i(K^{m,1}).N_{L/K}.I_L^S) \to \text{Gal}(L/K)$$

(Existence) Given any modulus n of K there exists an abelian extension K_m/K (also known as the Ray Class Field), the Artin map induces an isomorphism.

THANK YOU

I thank everyone for their valuable attention!