p-adic Fourier Theory and applications
CTNT 2022

Jeremy Teitelbaum

Overview

1. Brief look at classical fourier analysis for motivation
2. Continuous functions on $\mathbb{Z}_p$ and Mahler's Theorem
3. Distributions, characters, and the Iwasawa algebra
4. The Kubota-Leopoldt p-adic zeta function.

Classical Fourier Analysis

Let G be an compact topological group that is abelian.

- G is a topological space
- G is an abelian group
- the group operations are continuous

Examples:

- $G = \{z \in \mathbb{C} : |z| = 1\}$, so G is the circle group $\mathbb{T}$.
- G is any finite abelian group.
- G is the additive group of p-adic integers $\mathbb{Z}_p$
- G is the multiplicative group of p-adic units $\mathbb{Z}_p^*$

Haar Measure

A compact abelian group G has a unique invariant measure μ such that $\mu(G) = 1$.

"Invariant" means $\mu(gX) = \mu(X)$ for subsets X of G.

On $\mathbb{T}$ this is Lebesgue measure.

On a finite group it is the measure that assigns mass $|G|^{-1}$ to each point.

On $\mathbb{Z}_p$, we have

$$\mu(a + p^n\mathbb{Z}_p) = 1/p^n$$

because

$$\mathbb{Z}_p = \coprod_{a=0}^{p^n-1} (a + p^n\mathbb{Z}_p).$$

Characters and the dual group

A **character** of a compact abelian group G is a continuous homomorphism $\phi : G \to \mathbb{T}$.

The set of characters $X(G)$ form a topological group in their own right. This is called the **dual group** to G.

When $G = \mathbb{T}$, then the continuous characters are the functions

$$\phi_n(z) = z^n$$

where $n \in \mathbb{Z}$ and $X(\mathbb{T}) = \mathbb{Z}$.

When G is finite, the character group $X(G)$ is a finite group isomorphic to G. To see this:

- If $G = \mathbb{Z}/n\mathbb{Z}$, then $X(G)$ is isomorphic to the cyclic group group μ_n of n^{th}-roots of unity via $\phi \mapsto \phi(1)$.
- Now use the fundamental theorem of abelian groups.

Distributions

$L^2(G)$ is the Hilbert space of complex valued functions on G with inner product

$$< f, g >= \int_G f\overline{g} d\mu$$

where $d\mu$ is the normalized Haar measure on G.

A distribution on G is a continuous linear map $\lambda : L^2(G) \to \mathbb{C}$.

By Hilbert space theory, any such λ is of the form $\lambda(f) =< f, g_\lambda >$ for some $g_\lambda \in L^2(G)$.

Fourier transform

A distribution λ gives a function F_λ on the space of characters $X(G)$ by

$$F_\lambda(\phi) = \lambda(\phi) =< \phi, g_\lambda > .$$

This function is called the Fourier transform of λ.

Examples

If $G = \mathbb{T}$, then:

- $X(G) = \mathbb{Z}$
- the function $F_\lambda(n)$ gives the Fourier coefficients of g_λ.

If G is finite:

- the distributions on G are the group algebra $\mathbb{C}[G]$.
- If $\lambda = \sum_g a(g)g$ and $\phi \in X(G)$ then

$$F_\lambda(\phi) = \sum_g a(g)\phi(g).$$

- this is the *discrete fourier transform*.

Key ingredients

- Compact abelian group G
- Function space $C(G)$ on G
- Distributions are continuous linear forms on $C(G)$.
- Continuous characters form another topological group $X(G)$.
- Distributions -> functions on character space $X(G)$.

p-adic Fourier Theory

Overview

In p-adic Fourier theory the ingredients are:

- $\mathbb{G} = \mathbb{Z}_p$ or $G = \mathbb{Z}_p^*$.
- The space of continuous functions $C(G, K)$ where K is a complete extension field of $\mathbb{Q}_p$.
- The space $X(G)$ of continuous characters $\phi : G \to K^*$.
- Distributions are continuous linear maps $C(G, K) \to K$.
- Fourier transform converts distributions to functions on $X(G)$ by $\lambda \mapsto F_\lambda$ where $F_\lambda(\phi) = \lambda(\phi)$.

Different because:

- continuous functions aren't Haar integrable (measures of small sets get p-adically large)
- there are many more continuous functions from $\mathbb{Z}_p$ to K than from $\mathbb{Z}_p$ to $\mathbb{C}$.

$\mathbb{Z}_p^*$ and $\mathbb{Z}$ are almost the same (p>2)

Proposition: The group $\mathbb{Z}_p^*$ is isomorphic to the product

$$\mu_{p-1} \times (1 + p\mathbb{Z}_p)$$

where μ_{p-1} is the finite group of $(p-1)^{st}$ roots of 1.

Proof:

- Hensel's lemma applied to $x^{p-1} - 1 = 0$ gives $\mu_{p-1} \subset \mathbb{Z}_p^*$.
- There's one element of μ_{p-1} in each congruence class. So every element $a \in \mathbb{Z}_p^*$ can be written uniquely as

$$a = \omega(a)\langle a \rangle$$

where $\omega(a) \in \mu_{p-1}$ and $\langle a \rangle \in 1 + p\mathbb{Z}_p$.

$\mathbb{Z}_p^*$ and $\mathbb{Z}_p$ are almost the same (p>2)

The power series

$$\frac{1}{p}\log(1+x) = \frac{1}{p}(x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots)$$

converges for any $1+x \in 1+p\mathbb{Z}_p$ and satisfies $\log((1+x)(1+y)) = \log(1+x) + \log(1+y)$.

The power series

$$\exp(px) = 1 + px + \frac{(px)^2}{2!} + \frac{(px)^3}{3!} + \dots$$

converges for $x \in \mathbb{Z}_p$ and satisfies $\exp(p(x+y)) = \exp(px)\exp(py)$.

These maps give mutually inverse isomorphisms between $1+\mathbb{Z}_p$ and $\mathbb{Z}_p$.

So $1+p\mathbb{Z}_p$ (under multiplication) is isomorphic to $\mathbb{Z}_p$ (under addition).

Continuous functions on $\mathbb{Z}_p$

Let $G = \mathbb{Z}_p$ and let K be a complete extension field of $\mathbb{Q}_p$. Let $C(G, K)$ be the space of continuous functions from G to K.

Example elements of $C(G, K)$:

- locally constant functions such as f where $f(x) = 1$ if $x \in p\mathbb{Z}_p$ and 0 otherwise.
- characters of order p^n. Let $\zeta \in \mu_{p^n}$.

  $$\zeta^x = \zeta^{a_0 + a_1 p + a_2 p^2 + \cdots}$$

  makes sense, is locally constant, and satisfies $\zeta^{x+y} = \zeta^x \zeta^y$.
- polynomial functions
- locally polynomial functions

Continuous functions on $\mathbb{Z}_p$

The space $C(G, K)$ is a K-vector space with a norm given by

$$\|f\| = \sup_{x \in G} |f(x)|.$$

Proposition: $C(G, K)$ is complete (it is a "Banach Space").

Proof: It is a general fact that if X is a compact metric space and Y is a complete metric space, then the continuous functions $C(X, Y)$ is complete under the sup norm. This is an exercise in uniform convergence.

Binomial polynomials

For $n \in \mathbb{Z}$, let $\binom{x}{n}$ be the binomial coefficient viewed as a polynomial in x. For example

$$\binom{x}{3} = \frac{x(x-1)(x-2)}{3!}.$$

Proposition: The polynomials $\binom{x}{n}$ have the property that

$$x \in \mathbb{Z}_p \implies \binom{x}{n} \in \mathbb{Z}_p.$$

This follows from the fact that $\binom{x}{n}$ takes integer values when x is a positive integer, and these are dense in $\mathbb{Z}_p$.

Mahler's Theorem

Theorem: Any continuous function $f : G \to K$ has a unique expansion

$$f(x) = \sum_{n=0}^{\infty} a(n) \binom{x}{n}$$

where $a(n) \in K$ for all n and $\lim_{n \to \infty} |a(n)| = 0$. Furthermore,

$$\|f\| = \sup_{n=0}^{\infty} |a(n)|.$$

Since the $a(n)$ go to zero, such an f converges pointwise. A uniform convergence argument shows that $f(x)$ is continuous.

Corollary: The space $C(G, K)$ is isomorphic (as a Banach space) to the space of sequences $(a(n))_{n=0}^{\infty}$ where $a(n) \in K$, under pointwise addition and scalar multiplication and with norm given by the sup-norm.

Comments on Mahler's Theorem

Let Δ be the finite difference operator $\Delta(f) = f(x+1) - f(x)$.

The finite difference calculus says that, if $f : \mathbb{Z} \to \mathbb{Z}$, then

$$f(x) = \sum_{n=0}^{\infty} \Delta^i(f)_{x=0} \binom{x}{i}.$$

If $f : \mathbb{Z}_p \to K$ one can still construct this series and if it makes sense it will agree with f on the integers, and then by continuity on all of $\mathbb{Z}_p$.

To prove convergence you need to show that the coefficients $\Delta^i(f)_{x=0}$ go to zero. A detailed proof is given by Conrad (google "conrad mahlerexpansions")

Characters

A continuous character is a continuous function $f : \mathbb{Z}_p \to K^*$. Such a function is determined by continuity and by $f(1)$:

- $f(1) = a$
- $f(n) = a^n$ for $n \in \mathbb{Z} \subset \mathbb{Z}_p$.
- $f(\sum_{i=0}^{\infty} b_i p^i) = \lim_{N\to\infty} a^{\sum_{i=0}^{N} b_i p^i}$

In particular, $a^{p^n} \to 1$ as $n \to \infty$, which forces $|a - 1| < 1$.

If $a = 1 + z$ where $|z| < 1$ then Mahler's theorem tells us that

$$(1+z)^x = \sum_{i=0}^{\infty} \binom{x}{i} z^i$$

is a continuous function of $x \in \mathbb{Z}_p$ and the uniqueness tells us that

$$(1+z)^{(x+y)} = (1+z)^x(1+z)^y.$$

The space of (p-adic) characters

Proposition: The space of continuous K^* valued characters of $\mathbb{Z}_p$ is the set

$$X(\mathbb{Z}_p)(K) = \{1 + z \in K : |z| < 1\}.$$

That is, the character space is an "open p-adic disk of radius one centered at 1". Given z with $|z| < 1$, we write

$$\phi_z(x) = (1+z)^x = \sum \binom{x}{n} z^n.$$

Distributions

Proposition: The space $D(G,K)$ of continuous linear maps $C(G,K) \to K$ is isomorphic (as a Banach space) to the space of bounded power series with coefficients in K via

$$\lambda \mapsto \sum_{n=0}^{\infty} \lambda(\binom{x}{n}) T^n.$$

If $g(T) = \sum_{n=0}^{\infty} c(n) T^n$, then the duality pairing $D(G,K) \times C(G,K) \to K$ is given by

$$\langle \sum c(n) T^n, \sum a(n) \binom{x}{n} \rangle = \sum_{n=0}^{\infty} c(n) a(n)$$

The Fourier transform

Remember that the Fourier transform converts a distribution λ into a function on the character space by the rule $F_\lambda(\phi) = \lambda(\phi)$.

In our situation, if $\lambda = \sum c(n)T^n$ and $\phi = \phi_z$ then

$$F_\lambda(\phi) = \langle \sum c(n)T^n, \sum \binom{x}{n} z^n \rangle = \sum c(n) z^n.$$

In other words, the Fourier transform of the distribution λ is a power series whose value at z is the distribution evaluated at ϕ_z.

The Iwasawa algebra

Let's look at $D(G, \mathbb{Q}_p)$, which is the space of power series with bounded $\mathbb{Q}_p$ coefficients.

Inside this ring is the subring

$$\Lambda = \mathbb{Z}_p[[T]]$$

of power series with integral coefficients. This important algebra is called the Iwasawa algebra.

Proposition: The Iwasawa algebra is the space of distributions λ on $C(G, \mathbb{Q}_p)$ with the property that $|\lambda(f)| \leq \|f\|$ for all f; that is, it is the unit ball in the Banach space $D(G, \mathbb{Q}_p)$.

Some special "integrals"

Let $F(T) \in D(G, K)$ be a distribution. We know that

$$\langle F(T), \phi_z \rangle = F(z).$$

In other words, the values of F give the integrals of characters.

Let $x \in \mathbb{Z}_p$ be fixed and let $F(T) = (1+T)^x = \sum_{n=0}^{\infty} \binom{x}{n} T^n$. Then

$$\langle F(T), \phi_z \rangle = \sum \binom{x}{n} z^n = \phi_z(x).$$

In other words, the power series $(1+T)^x$ with x fixed is the Dirac distribution at x.

More special integrals

Proposition:

$$\langle F(T), x^n \rangle = \partial^n F(T)|_{T=0}$$

where $\partial F = (1+T)\frac{d}{dT}F$.

To prove this, notice that

$$x\binom{x}{n} = (n+1)\binom{x}{n+1} + n\binom{x}{n}.$$

Then compare $\langle T^n, x\binom{x}{j}\rangle$ with $\langle \partial T^n, \binom{x}{j}\rangle$ and see that they are the same for all n and j.

By linearity (and continuity) we conclude that $\langle \partial F, h\rangle = \langle F, xh\rangle$ for any h and so

$$\partial^n F(T)|_{T=0} = \langle \partial^n F(T), 1\rangle = \langle F(T), x^n\rangle$$

The Kubota Leopoldt zeta function

The (analytic continuation of) the Riemann zeta function relates the values of $\zeta(s)$ at negative integers to Bernoulli numbers:

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}$$

where the Bernoulli numbers come from the generating function

$$\frac{t}{e^t - 1} = \sum_{n \geq 0} B_n \frac{t^n}{n!}.$$

The arithmetic significance of the Bernoulli numbers goes back to Kummer who showed that Fermat's Last Theorem held for *regular* primes, meaning primes p that do not divide the numerator of B_k for k between 2 and $p-3$.

This is the dawn of what we now call Iwasawa theory which relates the behavior of class groups in towers of fields to the divisibility of special values of L-functions.

The Kubota-Leopoldt zeta function

The K-L zeta function is an analytic function of a p-adic variable that "interpolates" the values $\zeta(n)$. Its construction is most elegantly done through Fourier theory.

Let

$$f_a(T) = \frac{1}{e^t - 1} - \frac{a}{e^{at} - 1}.$$

One can show that

$$f_a^{(}k)(0) = (-1)^k(1 - a^{1+k})\zeta(-k)$$

A chain rule exercise shows that if we set

$$F_a(T) = \frac{1}{T} - \frac{a}{(1+T)^a - 1}$$

then

$$f_a^{(k)}(0) = \partial^k F_a(T)|_{T=0}$$

.

The K-L zeta function

Lemma: The power series

$$F_a(T) = \frac{1}{T} - \frac{a}{(1+T)^a - 1}$$

has coefficients in $\mathbb{Z}_p$ provided a is an integer coprime to p.

Therefore $F_a(T)$ can be viewed as a distribution on $\mathbb{Z}_p$ that satisfies

$$\langle F_a(T), x^k \rangle = (-1)^k (1 - a^{1+k}) \zeta(-k).$$

We'd like this transform to be a p-adic function of k, but we're not quite there yet.

The Mellin transform

Remember that we showed that $\mathbb{Z}_p^*$ is isomorphic to $\mu_{p-1} \times \mathbb{Z}_p$ via the map sending x to the pair $(\omega(x), \langle x \rangle)$.

If $z \in 1 + p\mathbb{Z}_p$ and $0 \leq i < p - 1$ then we have a character

$$\psi = \omega^i \psi_z$$

where $\psi_z(x) = (1+z)^{\log(x)/p}$. The character $x \mapsto \langle x \rangle^s$ corresponds to ψ_z where $z = \exp(ps) - 1$ for $s \in \mathbb{Z}$.

If λ is a distribution on $\mathbb{Z}_p^*$, its "Mellin transform" is

$$M_\lambda(z, \omega^i) = \lambda(\omega^i \psi_z).$$

M_λ is a vector of $q - 1$ power series – it's a Fourier transform for the multiplicative group.

Mellin and Fourier

Suppose λ is a distribution on $\mathbb{Z}_p$ which vanishes on functions with support in $p\mathbb{Z}_p$. Therefore λ is also a distribution on $\mathbb{Z}_p^*$.

Let M_λ be its Mellin transform and F_λ be its Fourier transform.

if $n \equiv i \pmod{p-1}$, we have

$$M_\lambda(\exp(pn) - 1, \omega^i) = \lambda(x^n) = \partial^n F_\lambda(T)|_{T=0}$$

In addition, $M_\lambda(\exp(ps) - 1, \omega^i)$ is an analytic function in s – that is, given by a power series in s for $s \in \mathbb{Z}_p$.

From $\mathbb{Z}_p$ to $\mathbb{Z}_p^*$

To complete the construction of the K-L zeta function, we need to adjust our power series F_a so that it vanishes on functions supported on $p\mathbb{Z}_p$.

For this we use the function

$$H(x) = 1 - \frac{1}{p}\sum_{\zeta} \zeta^x$$

where ζ runs over the p^{th} roots of unity.

$H(x) = 1$ if x is not divisible by p and 0 if it is.

If F is a power series corresponding to a distribution, let F^* be the function

$$F^*(T) = F(T) - \frac{1}{p}\sum_{\zeta} F(\zeta - 1 + \zeta T).$$

One can show that this is still a power series with bounded coefficients, and is therefore still a distribution.

From $\mathbb{Z}_p$ to $\mathbb{Z}_p^*$

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

$$\langle F^*, f \rangle = \langle F, Hf \rangle.$$

Check this on characters. We have

$$\langle F^*, (1+z)^x \rangle = \langle F, (1+z)^x \rangle - \frac{1}{p} \sum_{\zeta} \langle F(\zeta - 1 + \zeta T), (1+z)^x \rangle.$$

But

$$\langle F(\zeta - 1 + \zeta T), (1+z)^x \rangle = \langle F(T), (\zeta(1+z))^x \rangle$$

and combining the terms gives you what you want.

Corollary: F^* vanishes on functions supported on $p\mathbb{Z}_p$ and is therefore a distribution on $\mathbb{Z}_p^*$.

Wrapping up.

To finish, apply the operation above to the power series

$$F_a(T) = \frac{1}{T} - \frac{a}{(1+T)^a - 1}.$$

It turns out that

$$F_a^*(T) = F_a(T) - F_a((1+T)^p - 1).$$

With some calculations using this you obtain the analytic function $M(\exp(ps) - 1, \omega^i)$ satisfying

$$M(\exp(pn) - 1, \omega^i) = (-1)^k (1 - a^{k+1})(1 - p^{k+1})\zeta(-k)$$

With a bit more work one can get rid of the $1 - a^{k+1}$ term, but the p-Euler factor has to be "removed" for the p-adic construction to work.