ESA

Ashvni Narayanan

July 2, 2021

1 Contents

2. Introduction . . . 1
3. Definitions . . . 3
4. Bernoulli polynomials . . . 4
5. Locally compact Hausdorff spaces . . . 7
5.1. Density of locally constant functions . . . 7
5.2. Clopen sets of the p-adic integers . . . 8
6. p-adic L-functions . . . 9
6.1. p-adic Measures . . . 9
6.2. p-adic Integrals . . . 12
6.3. Teichmuller character . . . 13
6.4. Construction . . . 13
7. Conclusion . . . 15
8. Bibliography . . . 15

2 Introduction

I am working on formalizing mathematics in an automated theorem prover called Lean. The aim of my PhD is to formalize the statement of the Iwasawa Main Conjecture. The statement somehow unifies an "algebraic side", coming from characteristic polynomials, with an "analytic side", coming from p-adic L-functions. I have been working on formalizing p-adic L-functions in Lean. This is still a work in progress, and will hopefully be complete by August 2021.

Lean has a mathematical library called `mathlib`. This is maintained by several mathematicians and computer scientists. It is essential to remember

that this is a communal effort, and it would be impossible to construct such a vast library otherwise.

Apart from Iwasawa theory, the p-adic L-functions are a very well studied number theoretic object. They appear in several places, such as the Birch and Swinnerton-Dyer Conjecture. They take twisted values of the Dirichlet L-function at negative integers. These values are also related to the generalized Bernoulli numbers and the p-adic zeta function.

There are several different ways of constructing the p-adic L-functions. I refer to the constructions given in [1]. An optimal definition is one that minimizes the amount of code needed to obtain the required properties, and that is the "most general", so that it can be used to its full potential. I have chosen this specific definition in terms of p-adic integrals because it seems to be the closest to what I need for the Iwasawa Main Conjecture. It is also helpful because it minimizes the code needed to show analytic continuity of several functions that would be needed in other definitions, and by keeping the preexisting theorems in `mathlib` in mind. Since `mathlib` is an everchanging and increasing library, it is possible that this might not be the best definition in the future.

A lot of tools are needed in order to construct the p-adic L-functions, including but not restricted to: Bernoulli numbers and polynomials, locally compact Hausdorff totally disconnected spaces, and the p-adic integers and its topological properties. I introduce these, and then define the p-adic L-function, finishing with a summary of what has been accomplished and what will be.

All the code for this can be found in src/number_theory/L_functions.lean and src/number_theory/weight_space.lean on the branch p-adic, [2]. For an introduction to Lean, one may refer to my previous report submission for the RPC. The most current version of `mathlib` (which is not the one I am using) is [3].

3 Definitions

The following definitions are used throughout this section :

A set s in a topological space is *compact* if for every cover $s \subseteq \cup_i U_i$

of s by open sets U_i, there exists a finite subcover $U_1, \ldots, U_m$ such that $s \subseteq \cup_{i=1}^{m} U_i$. A topological space is compact if it is compact when considered as a set. Note that, in Lean, is_compact s is used for a set s, while compact_space X is used for a topological space X.

A Hausdorff topological space X is called *locally compact* if for every $x \in X$, there exists a compact neighbourhood z containing x.

A set s of a topological space is called *totally separated* if $\forall x, y \in s$ with $x \neq y$, there exist disjoint open sets U, V such that $x \in U$, $y \in V$, and $s \subseteq uv$. A topological space is totally separated if it is totally separated as a subset of itself.

A set s of a topological space is called *totally disconnected* if every connected subset of s is atmost a singleton. A topological space is totally disconnected if it is totally disconnected as a subset of itself.

A *profinite* space is compact, Hausdorff and totally disconnected. It is also an inverse limit of finite spaces.

A function on a topological space is *locally constant* if the preimage of every set is open. By definition, all locally constant functions are continuous. The set of locally constant functions from X to A are denoted $LC(X, A)$. We define the canonical (linear) injection inclusion : LC(X,A) $\to$ C(X, A).

A *clopen set* of a topological space is a set which is both open and closed.

Given a set U of a topological space X, the *characteristic function* of U on X takes value 1 for every element of U, and 0 otherwise. Characteristic functions of clopen sets are locally constant.

The *p-adic valuation* is a function $\nu_p : \mathbb{Z} \to \mathbb{R}$, such that $\nu_p(p^k) = k$, and for $gcd(a, p) = 1$, $\nu_p(a) = 0$. By convention,$\nu_p(0) = \infty$, however, in Lean, valuation $0 = 0$. The *ring of p-adic integers*, denoted $\mathbb{Z}_p$, is the completion of $\mathbb{Z}$ by the p-adic valuation ν_p. They have the following properties :

1. As a profinite limit, $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. As a result, one can find (compatible) ring homomorphisms

```
    /-- A ring hom from ‘ℤ_[p]‘ to ‘zmod (p^n)‘ -/
def to_zmod_pow (n : ℕ) : ℤ_[p] →+* zmod (p ^ n)
```

2. As a topological space, $\mathbb{Z}_p$ has the profinite topology, with discrete topology on the finite sets. Hence, $\mathbb{Z}_p$ is a compact, Hausdorff totally disconnected space with a clopen basis coming from the inverse image of points on $\mathbb{Z}/p^n\mathbb{Z}$ for every n.

3. Note that $\mathbb{Z}_p^\times = \mathbb{Z}/p\mathbb{Z}\times(1+p\mathbb{Z}_p)$. By the Chinese Remainder Theorem, we have, for $gcd(d,p) = 1$, $(\mathbb{Z}/d\mathbb{Z})^\times \times \mathbb{Z}_p^\times = (\mathbb{Z}/dp\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)$

The fraction field of $\mathbb{Z}_p$ is denoted $\mathbb{Q}_p$. The p-adic completion of the algebraic closure of $\mathbb{Q}_p$ is denoted $\mathbb{C}_p$, and it is topologically and algebraically closed.

A *Dirichlet character* mod d is a multiplicative group homomorphism from $(\mathbb{Z}/d\mathbb{Z})^\times \to \mathbb{C}^\times$. This induces homomorphisms $(\mathbb{Z}/kd\mathbb{Z})^\times \to \mathbb{C}^\times$ for all $k \geq 0$. The smallest such d is called the *conductor*. A Dirichlet character mod d is called *primitive* if it has conductor d. All our Dirichlet characters are assumed to be primitive.

For a topological group A, define the *weight space*, denoted weight_space to be the continuous monoid homomorphisms from $(\mathbb{Z}/d\mathbb{Z})^\times \times \mathbb{Z}_p^\times$ to $A^\times$, with $gcd(d,p) = 1$.

4 Bernoulli polynomials

The Bernoulli polynomials are an important number theoretic object. They occur as special values of the Reimann-zeta functions / p-adic L-functions. They are a generalization of Bernoulli numbers.

The Bernoulli numbers B_n are generating functions given by :

$$\sum B_n \frac{t^n}{n!} = \frac{t}{e^t - 1}$$

Note that several authors think of Bernoulli numbers B'_n to be defined as :

$$\sum B'_n \frac{t^n}{n!} = \frac{t}{1 - e^{-t}}$$

The difference between these two is : $B'_n = (-1)^n * B_n$, with $B_1 = \frac{-1}{2}$. Using recursion, B_n is defined in `mathlib` as :

```
bernoulli' n = 1 - Σ k : fin n, n.choose k / (n - k + 1) *
 bernoulli' k
```

and B'_n as :

```
def bernoulli (n : ℕ) : ℚ := (-1)^n * bernoulli' n
```

The Bernoulli polynomials denoted $B_n(X)$, a generalization of the Bernoulli numbers, are generating functions :

$$\sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!} = \frac{te^{tX}}{e^t - 1}$$

We now define the Bernoulli polynomials as :

```
def bernoulli_poly (n : ℕ) : polynomial ℚ :=
Σ i in range (n + 1), polynomial.monomial (n - i) ((
 bernoulli i) * (choose n i))
```

The following properties of Bernoulli polynomials were proved :

1. $B_0(X) = X$:

```
lemma bernoulli_poly_zero : bernoulli_poly 0 = 1
```

2. $B_n(0) = B_n$:

```
lemma bernoulli_poly_eval_zero (n : ℕ) : (
bernoulli_poly n).eval 0 = bernoulli n
```

3. $B_n(1) = B'_n$:

```
lemma bernoulli_poly_eval_one (n : ℕ) : (
bernoulli_poly n).eval 1 = bernoulli' n
```

4. $\left(\sum_{n=0}^{\infty} B_n(t)\frac{X^n}{n!}\right) * (e^X - 1) = Xe^{tX}$:

```
theorem exp_bernoulli_poly' (t : A) :
mk (λ n, aeval t ((1 / n! : ℚ) · bernoulli_poly n)) * (
 exp A - 1) =
X * rescale t (exp A)
```

The last point uses power_series.mk, which defines a formal power series in terms of its coefficients, that is,

$\sum_{n=0}^{\infty} a_n X^n =$ `mk (λ n, a_n)`

The symbol • represents scalar multiplication of $\mathbb{Q}$ on $\mathbb{Q}$-polynomials.
In the last theorem, A represents a commutative $\mathbb{Q}$-algebra. Also, the exponential function $e^{\times}$, which is defined as a Taylor series expansion, takes as input A, but not x. In order to define $e^{t\times}$, we need to use (the ring homomorphism) rescale y, which, for an element y of a commutative semiring R, takes a formal power series over R, say $f(X)$, to $f(yX)$.

The proof of the last theorem involves equating the n^{th} coefficients of the RHS and the LHS. After differentiating between n zero and nonzero, one requires the following lemma to complete the nonzero case :

```
theorem sum_bernoulli_poly (n : ℕ) :
Σ k in range (n + 1), ((n + 1).choose k : ℚ) ·
 bernoulli_poly k =
  polynomial.monomial n (n + 1 : ℚ)
```

The proof os this theorem follows from the following property of Bernoulli numbers :

```
theorem sum_bernoulli (n : ℕ):
Σ k in range n, (n.choose k : ℚ) * bernoulli k = if n = 1
 then 1 else 0
```

This follows from the analogous theorem sum_bernoulli', whose proof follows from rearranging sums and the definition of bernoulli'.

Given a primitive Dirichlet character χ of conductor f, let us now define the generalized Bernoulli numbers (section 4.1, [1]) :

$$\sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!} = \sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1}$$

These numbers have not been formalized in Lean yet. They are essential to obtain values of p-adic L-functions at negative integers.

5 Locally compact Hausdorff spaces

5.1 Density of locally constant functions

In Proposition 12.1 of [1], Washington defines the p-adic integral on $C(X, \mathbb{C}_p)$, the Banach space of continuous functions from a profinite space X to $\mathbb{C}_p$.

This is an extension of a function defined on a dense subset of $C(X, \mathbb{C}_p)$, the locally constant functions from X to $\mathbb{C}_p$. In fact, for any compact Hausdorff totally disconnected space X and a commutative normed ring A, $LC(X, A)$ is a dense subset of $C(X, A)$.

The mathematical proof is the following : For $f \in C(X, A)$, we want to prove that, for any $\epsilon > 0$, we have $R = \cup_{x \in R} B(x, \epsilon)$. Since X is compact, one can find finitely many open sets $U_1, \ldots, U_n$ such that $U_i = f^{-1}(B(x_i, \epsilon))$ for $x_1, \ldots, x_n$ in R. One needs the fact that compact Hausdorff totally disconnected spaces have a clopen basis. We then find a finite set of disjoint clopen sets $C_1, \ldots, C_m$ which form a basis, such that each C_j is contained in some U_i. Then, we pick elements $a_1, \ldots, a_m$ in $C_1, \ldots, C_m$, and construct the locally constant function $g(x) := \sum_{j=1}^{m} f(a_j)\chi_{C_j}(x)$, where χ_U is the characteristic (locally constant) function taking value 1 on every element of U and 0 otherwise. It then follows that $||f - g|| = sup_{x \in X}||f(x) - g(x)|| < \epsilon$, as required.

Formalizing this took about 500 lines of code. Let us show that locally compact Hausdorff totally disconnected spaces have a clopen basis :

```
lemma loc_compact_Haus_tot_disc_of_zero_dim {H : Type*} [
   topological_space H]
  [locally_compact_space H] [t2_space H] [
   totally_disconnected_space H] :
  is_topological_basis {s : set H | is_clopen s}
```

The mathematical proof is : We want to show that for every $x \in H$ and open set U such that $x \in U$, there exists a clopen set C such that $x \in C$ and $C \subseteq U$. Since H is a locally compact space, we can find a compact set s such that $x \in$ (interior s) and $s \subseteq U$. We have the following lemma :

```
  /-- Every member of an open set in a compact Hausdorff
   totally disconnected space
  is contained in a clopen set contained in the open set.  -/
lemma compact_exists_clopen_in_open {x : α} {U : set α} (
   is_open : is_open U) (memU : x ∈ U) :
   ∃ (V : set α) (hV : is_clopen V), x ∈ V ∧ V ⊆ U
```

This implies that we can find a clopen set $V \subseteq$ (interior s) of s, with $x \in V$. Since V is closed in s(compact, hence closed), V is closed in H. Since $V \subseteq$ (interior s) is open in s, hence in (interior s), V is open in H, thus we are done.

This turned out to be harder to formalize than expected. This is because s, which is of type s : set H also has the property is_compact (s : set H). This is equivalent to saying that s is a compact space, that is, compact_space (set.univ : set s), where (set.univ : set s) is simply s viewed as a set of itself, instead of a topological space. Now, if we have V to be a subset of s of type V : set s, Lean does not recognize it as a subset of H. We construct V' : set H to be the image of V under the closed embedding coe : s → H. This process must be repeated each time we consider a subset as a topological space.

5.2 Clopen sets of the p-adic integers

As mentioned before, $\mathbb{Z}_p$ is a profinite space. Since it is the inverse limit of finite discrete topological spaces $\mathbb{Z}/p^n\mathbb{Z}$ for all n, it has a clopen basis of the form $U_{a,n} := proj_n^{-1}(a)$ for $a \in \mathbb{Z}/p^n\mathbb{Z}$ and $proj_n$ being the canonical projection.

We first define the collection of sets $(U_{a,n})_{a,n}$:

```
lemma proj_lim_preimage_clopen (n : ℕ) (a : zmod (d*(p^n)))
 : is_clopen (set.preimage (padic_int.to_zmod_pow n) {a} :
 set ℤ_[p]) :=

def clopen_basis : set (set ℤ_[p]) := {x : set ℤ_[p] | ∃ (n
 : ℕ) (a : zmod (p^n)),
x = set.preimage (padic_int.to_zmod_pow n) {a} }
```

We now want to show that clopen_basis forms a topological basis and that every element is clopen :

```
theorem clopen_basis_clopen : topological_space.
 is_topological_basis (clopen_basis p) ∧
∀ x ∈ (clopen_basis p), is_clopen x :=
```

The mathematical proof is to show that for any ϵ-ball, one can find $U_{a,n}$ inside it. This is true because :

```
lemma preimage_to_zmod_pow_eq_ball (n : ℕ) (x : zmod (p^n))
 : (padic_int.to_zmod_pow n) ⁻¹' {(x : zmod (p^n))} = metric
 .ball (x : ℤ_[p]) ((p : ℝ) ^ (1 - (n : ℤ))) :=
```

Proving this was fairly straightforward by using the expansion of a p-adic integer, that is, every $a \in \mathbb{Z}_p$ can be written as $\sum_{n=0}^{\infty} a_n p^n$, with $a_n \in \mathbb{Z}/p^n\mathbb{Z}$.

Approximating a by $\sum_{n=0}^{m} a_n p^n$ is done by the function $appr : \mathbb{Z}_p \to \mathbb{N} \to \mathbb{N}$. Note that appr returns a natural number, with a_n being the smallest natural number in the $\mathbb{Z}/p^n\mathbb{Z}$ equivalence class. This turned out to be very useful, along with the following lemmas :

```
lemma appr_spec (n : ℕ) : ∀ (x : ℤ_[p]), x - appr x n ∈ (
 ideal.span {p^n} : ideal ℤ_[p]) :=
lemma has_coe_t_eq_coe (x : ℤ_[p]) (n : ℕ) :
(((a.appr n) : zmod (p^n)) : ℤ_[p]) = ((a.appr n) : ℤ_[p])
 :=
```

The latter lemma is not true in general. It works here because the coercion from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{Z}_p$ is a composition of a coercion from $\mathbb{Z}/p^n\mathbb{Z}$ to $\mathbb{N}$, which takes $a \in \mathbb{Z}/p^n\mathbb{Z}$ to the smallest natural number in its $\mathbb{Z}/p^n\mathbb{Z}$ equivalence class.

6 p-adic L-functions

6.1 p-adic Measures

In this section, $X = \varprojlim X_i$ denotes a profinite space with X_i finite and projection maps $\pi_i : X \to X_i$ and surjective maps $\pi_{ij} : X_i \to X_j$ for all $i \geq j$. We use G to denote an abelian group, A for a commutative normed ring, and R for a commutative complete normed ring. We fix a prime p and an integer d such that $gcd(d, p) = 1$.

We begin by defining distributions on profinite sets. In Section 12.1 of [1], Washington gives 3 equivalent definitions of a distribution :

1. A system of maps $\phi_i : X_i \to G$ such that $\forall i \geq j$,
$$\phi_j(x) = \sum_{\pi_{ij}(y)=x} \phi_i(y)$$
2. A G-linear function $\phi : LC(X, G) \to G$.
3. A finitely additive function from the compact open sets of X to G.

Since switching between definitions is cumbersome, and(at that point of time), `mathlib` had no notion of thinking about profinite sets as inverse limits of finite sets, we chose to work with the second definition, since there was an established and vast API for locally constant functions :

```
  structure distribution' [nonempty X] :=
(phi : linear_map A (locally_constant X A) A)
```

The nonempty assumption is needed to make $C(X, A)$ (and in turn, $LC(X, A)$) a topological space (the subspace topology induced from $C(X, A)$). The topology on $C(X, A)$ comes from its normed group structure induced by the norm on A : $||f - g|| = sup_{x \in X} ||f(x) - g(x)||$. While showing that, $\forall f \in C(X, A)$, $||f|| = 0 \implies f = 0$, it suffices to show $||f|| \leq 0 \implies \forall x \in X, ||f(x)|| \leq 0$. We then use the following lemma, which requires the nonempty assumption :

```
theorem cSup_le_iff {α : Type*} [
  conditionally_complete_lattice α] {s : set α} {a : α}
(hb : bdd_above s) (ne : s.nonempty) : Sup s ≤ a ↔ (∀b ∈ s
  , b ≤ a)
```

Ideally, there is no need to define distribution', since there are no additional properties it satisfies which linear maps do not. An API needs to be built for every definition made, which can be costly, code wise. Hence, in the final version, this definition will probably be removed.

We can now define p-adic measures. Measures are bounded distributions. Note that the p-adic measures are not to be confused with measures arising from measure theory. The key difference lies in the fact that the clopen sets of a profinite space do not form a σ-algebra.

```
def measures'' [nonempty X] :=
{φ : distribution' X // ∃ K : ℝ, 0 < K ∧ ∀ f : (
  locally_constant X A), φ.phi f ≤ K * inclusion X A f }
```

The boundedness of the distribution is needed to make the measure continuous :

```
/-- Measures are continuous. -/
lemma integral_cont [nonempty X] (φ : measures'' X A) :
  continuous (φ.1).phi
```

The proof is straightforward : for $b \in LC(X, A)$, given $\epsilon > 0$, there exists a $\delta > 0$ such that for all $a \in LC(X, A)$ with $||b - a|| < \delta$, $||\phi(a) - \phi(b)|| < \epsilon$. Since ϕ is a measure, it suffices to prove that $K * ||inclusion(a - b)|| < \epsilon$. Choosing $\delta = \epsilon / K$ gives the desired result.

The Bernoulli measure is an essential p-adic measure. We make a choice of an integer c with $gcd(c, dp) = 1$, and c^{-1} is an integer such that $cc^{-1} \equiv 1 \bmod dp^{2n+1}$. For $x_n \in (\mathbb{Z}/dp^{n+1}\mathbb{Z})^\times$, the (first) Bernoulli measure is defined by

$$E_{c,n}(x_n) = B_1\left(\left\{\frac{x_n}{dp^{n+1}}\right\}\right) - cB_1\left(\left\{\frac{c^{-1}x_n}{dp^{n+1}}\right\}\right)$$

The system $(E_{c,n})_{n\in\mathbb{N}}$ forms a distribution according to the first definition given above. We want to get an equivalent reformulation in terms of the second definition. We know that, since X is compact, every locally constant function can be written in terms of a finite sum of a characteristic function of a basis element multiplied by a constant. Since X is profinite, from the previous section, we know that there exists a clopen basis of the form set.preimage (padic_int.to_zmod_pow n) a for $a \in \mathbb{Z}/dp^n\mathbb{Z}$. Thus, for a clopen set $U_{a,n}$:= set.preimage (padic_int.to_zmod_pow n) a, we define

$$E_c(\chi_{U_{a,n}}) = E_{c,n}(a)$$

In Lean, this translates to :

```
def E_c (hc : gcd c p = 1) := λ (n : ℕ) (a : (zmod (d * (p^n
 ))))), fract ((a : ℤ) / (d*p^(n + 1)))
  - c * fract ((a : ℤ) / (c * (d*p^(n + 1)))) + (c - 1)/2
def bernoulli_measure (hc : gcd c p = 1) :=
  {x : locally_constant (zmod d × ℤ_[p]) R →[R] R |
    ∀ U : (clopen_basis p d), x (char_fn (zmod d × ℤ_[p]) U
  .val) = E_c p d hc (classical.some U.prop)
    (classical.some (classical.some_spec U.prop)) }
```

The tactic classical.some makes an arbitrary choice of an element from a space, if the space is nonempty, and classical.some_spec lists down the properties of this random element coming from the space. Notice that bernoulli_measure is defined to be a set. One must now show that it is nonempty, and then use classical.some to pick an element of it. Also, it is only at this point that we need to think of $\mathbb{Z}_p$ as a compact, Hausdorff, totally disconnected space.

6.2 p-adic Integrals

The last piece in the puzzle is the p-adic integral. We use the same notation as in the previous section. Given a measure μ, and a function $f \in LC(X, R)$,

$\int f d\mu := \mu(f)$. As in Theorem 12.1 of [1], this can be extended to a continuous R-linear map :

$$\int_X f d\mu : C(X, R) \to R$$

This follows from the fact that $LC(X, R)$ is dense in $C(X, R)$, and that every measure μ is, in fact, uniformly continuous. One uses that the map $inclusion : LC(X, R) \to C(X, R)$ is dense_inducing, that is, it has dense range and the topology on $LC(X, R)$ is the one induced by inclusion from the topology on $C(X, R)$. We have the following useful lemmas :

```
/-- If ‘i : α → β‘ is dense inducing, then any function ‘f
  : α → γ‘ "extends" to a function ‘g = extend di f : β →
  γ‘. If ‘γ‘ is Hausdorff and ‘f‘ has a continuous extension
  , then ‘g‘ is the unique such extension. In general, ‘g‘
  might not be continuous or even extend ‘f‘. -/
def extend (di : dense_inducing i) (f : α → γ) (b : β) : γ :=
@@lim _ ⟨f (di.dense.some b)⟩ (comap i ( b)) f
```

and

```
uniform_continuous_uniformly_extend : [uniform_space α] [
  uniform_space β] [uniform_space γ]
{e : β → α} (h_e : uniform_inducing e) (h_dense :
  dense_range e) {f : β → γ}, uniform_continuous f →
∀ [separated_space γ] [complete_space γ], uniform_continuous
  (_.extend f)
```

The latter shows that the integral defined on $C(X, R)$ is actually uniformly continuous. Linearity of this map follows from properties of the dense_inducing map inclusion.

Let us now define the Teichmuller character.

6.3 Teichmuller character

Given $a \in \mathbb{Z}_p^\times$, there exists a unique p^{th}-root of unity $b \in \mathbb{Z}_p$ such that $a \equiv b(\text{mod p})$. This gives us the Teichmuller character $\omega : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$.

The initial effort was to formalize the proof of the above claim. However, it was discovered that Witt vectors, and in particular Teichmuller lifts had previously been added to `mathlib`. This was very helpful, and reiterates the importance of the collaborative spirit of Lean, and of making definitions in

the correct generality.

It is beyond the scope of this text to define Witt vectors and do it justice. For a commutative ring R and a prime number p, one can obtain a ring of Witt vectors $\mathbb{W}(R)$. When we take $R = \mathbb{Z}/p\mathbb{Z}$, we get that

```
def equiv : 𝕎 (zmod p) ≃+* ℤ_[p]
```

Composing equiv with to_zmod_pow 1 defined in the previous section, we obtain the desired homomorphism ω, defined in Lean as :

```
/-- The Teichmuller character defined on ‘p‘-adic units -/
noncomputable def teichmuller_character : monoid_hom (units ℤ_
    [p]) ℤ_[p] :=
{  to_fun := λ a, witt_vector.equiv p (witt_vector.
    teichmuller_fun p (padic_int.to_zmod (a : ℤ_[p]))),
  ..monoid_hom.comp (witt_vector.equiv p).to_monoid_hom
  (monoid_hom.comp (witt_vector.teichmuller p)
    (monoid_hom.comp (padic_int.to_zmod).to_monoid_hom
      ⟨(coe : units ℤ_[p] → ℤ_[p]), units.coe_one, units.
    coe_mul⟩)), }
```

The first two lines of the definition define the function, while the rest proves that it is a monoid homomorphism, since it is a composition of monoid homomorphisms.

6.4 Construction

There are several possible definitions for the p-adic L-functions (fixing an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$), including :

1. (Theorem 5.11, [1]) The p-adic meromorphic function $L_p(s, \chi)$ on $\{s \in \mathbb{C}_p || s| < p\}$ obtained by the analytic continuation, such that
$$L_p(1-n, \chi) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}$$
for $n \geq 1$.
2. (Proof of Theorem 5.11, [1]) $L_p(s, \chi) = \sum_{a=1, p\nmid a}^{F} \chi(a) H_p(s, a, F)$
3. (Theorem 12.2, [1]) For $s \in \mathbb{Z}_p$, and Dirichlet character χ with conductor dp^m, with $gcd(d, p) = 1$ and $m \geq 0$, for a choice of $c \in \mathbb{Z}$ with $gcd(c, dp) = 1$:
$$L_p(-s, \chi) = \frac{-1}{1 - \chi(c) < c >^{s+1}} \int_{(\mathbb{Z}/dp\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)} \chi\omega^{-1}(a) < a >^s dE_c$$

It is beyond the scope of this article to explain all the notation in the points above. I chose to define the p-adic L-function as a reformulation of (3). This is because it is the most optimal definition that helps with stating the Iwasawa Main Conjecture. The integral is the p-adic integral defined in Section 5.3, and ω denotes the Teichmuller character.

Instead of using the variable s, we choose to use an element of the weight space. We replace $< a >^s$ with w : weight_space A. This is a generalization of point 3.

Given a primitive Dirichlet character χ of character dp^m with $gcd(d, p) = 1$ and $m \geq 0$, we now define the p-adic L-function to be :

$$L_p(w, \chi) := f * \int_{(\mathbb{Z}/dp\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)} \chi\omega^{p-2}(a) * w$$

```
def p_adic_L_function (hc : gcd c p = 1) :=
f * integral (units (zmod d) × units ℤ_[p]) R _ (
 bernoulli_measure_of_measure p d R hc)
⟨(λ (a : (units (zmod d) × units ℤ_[p])), ((
 pri_dir_char_extend p d R) a) *
(inj (teichmuller_character p a.snd))^(p - 2) * (w.to_fun a
 : R)), cont_paLf p d R inj w ⟩
```

Here R denotes a commutative complete normed space with an injection inj of $\mathbb{Z}_p$ into R, and f is the constant given in 3. Note that pri_dir_char_extend extends χ from $(\mathbb{Z}/dp^m\mathbb{Z})^\times$ to $(\mathbb{Z}/d\mathbb{Z})^\times \times \mathbb{Z}_p^\times$. Also, we have used $\omega^{p-2} = \omega^{-1}$, in order to avoid proving the existence of an inverse.

The lemma cont_paLf states that the integrand is continuous, hence belongs to the domain of the integral :

```
lemma cont_paLf : continuous (λ (a : (units (zmod d) × units
  ℤ_[p])), ((pri_dir_char_extend p d R) a) * (inj (
 teichmuller_character p (a.snd)))^(p - 2) * (w.to_fun a : R
 ))
```

Once the above lemma is proved, we can formalize properties of p-adic L-functions. One of the most important properties is, for an integer n with $n \geq 1$,

$$L_p(1 - n, \chi) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}$$

Recall that the function corresponding to $1-n$ is $< a >^{1-n}$, where $< a >:= \omega^{-1}(a)a$. We must then show that $< a >^{1-n}$ is an element of the weight space. Formalizing the first definition would have made showing this result a lot tougher, since showing the analytic continuation of these functions is nontrivial, even on paper.

7 Conclusion

It is safe to say that the p-adic L-function is now almost completely defined. The missing pieces include showing that the bernoulli_measure is nonempty, and showing that the integrand of the p-adic L-function is continuous.

It might also be possible to extend the definition of the p-adic L-function to more general profinite spaces. The Bernoulli measures obtained for $k > 1$ might also give rise to a system of "p-adic L-functors".

All the code is currently on a branch of `mathlib`. It will take a very long time to update it with respect to the most recent version of `mathlib`, and much longer to put it formally in the library. I hope to have all of it done by July 2022.

8 Bibliography

References

[1] Introduction to cyclotomic fields, Washington

[2] Source code

[3] mathlib