Kubota-Leopoldt p-adic L-functions

Hugo Castillo

Contents

Chapter 1

Introduction

Kubota-Leopoldt p-adic L-functions are, for the p-adic analysis, the functions corresponding to the complex variable L-functions associated to Dirichlet characters. Today we know at least three distinct constructions of these functions : the original by Kubota and Leopoldt and two power series expansions. The first expansion was discovered by Iwasawa, and uses sequences of Stickelberger elements. The second expansion was done by Iwasawa and Coleman for the special cases of the powers of the Teichmuller character, and has been recently generalized to all relevant Dirichlet characters by Tsuji in [Tsu99]. I describe these three constructions and show that they lead to the same object. About the structure of the document I can say:

1. **Chapter I: Formal Power Series.** I start with the basics of formal power series as completions of a polynomial rings giving in the last sections special interest to power series over $\mathbb{C}_p$, the completion of the algebraic closure of $\mathbb{Q}_p$.

2. **Chapter II: p-adic Interpolation.** In this chapter the Kubota-Leopoldt p-adic L-function is defined. I am following Iwasawa's red book [Iwa72] for the classic construction.

3. **Chapter III: Stickelberger Elements and p-adic L-Functions.** Here the second construction is presented. The main technical tool is Theorem 4.3.1 which relates a power series to an element of a group algebra. The p-adic L-function will arise in this way.

4. **Chapter IV: The Compact-Open Topology.** This chapter is mainly technical. The main tool is the p-adic maximum principle treated in the first section and the rest of the chapter I follow [Col79]. In Theorem 5.3.2 I give a useful interpretation of Coleman's continuity criterium for the cyclotomic case.

5. **Chapter V: Coleman Local Theory.** In this chapter I follow [Col79] and [Col79]. It deals with power series modules such as $K((T))_1, \mathcal{O}_K[[T]], \mathfrak{M}_K$ and Galois actions defined on them. I define the norm and trace, give their basic properties and construct the Coleman homomorphism.

6. **Chapter VI: Coleman-Iwasawa-Tsuji Characterization of the p-adic L-functions** I present the third construction here. I follow [Tsu99] to obtain a power series via the Coleman homomorphism and then proving that it has the interpolation property, therefore it must be the p-adic L-function.

Chapter 2

Formal Power Series

2.1 Some generalities about Power Series

In this section let R a commutative ring with 1 and $R[[T]]$ the topological ring of formal powers series with the T-adic topology.

Definition 2.1.1 *For $N \in \mathbb{N}$, we define the* N**-th truncation map** *as*

$$\begin{array}{rccc} P_N : & R[[T]] & \longrightarrow & R[T] \\ & \sum a_n T^n & \longmapsto & \sum_{n<N} a_n T^n \end{array}$$

Let $f = \sum_{n \in \mathbb{N}} a_k T^k \in R[T]$ and $g \in TR[[T]]$. For simplicity let's denote $f_N = P_N(f)$ and $f_N(g) = \sum_{n \leq N} a_n g^n \in R[[T]]$, then for $N \geq M$ we have $f_N(g) \equiv f_M(g) \bmod T^M$ therefore $\big(f_N(g)\big)_{N \in \mathbb{N}}$ is a Cauchy sequence in $R[[T]]$ with respect to the T-adic topology.

Definition 2.1.2 *For $f \in R[[T]]$ and $g \in TR[[T]]$ we define the power series $f(g)$ as the the limit $f(g) = \lim_{N \to \infty} P_N(f)(g)$.*

Remark 2.1.1

1. *By definition $f(g)$ is the unique series in $R[[T]]$ such that $f(g) \equiv P_N(f)(g) \bmod T^N$ for all $N \in \mathbb{N}$, and this property characterizes $f(g)$.*
2. *Let $g_N = P_N(g)$, then $f_N(g) \equiv f_N(g_N) \bmod T^N$ and $f(g) \equiv f_N(g_N) \bmod T^N$.*

Proposition 2.1.1 *The map $R[[T]] \times T\,R[[T]] \longrightarrow R[[T]]$ defined as $(f, g) \longmapsto f(g)$, is continuous with respect to the T-adic topology.*

Proof. Let $F, f \in R[[T]]$ and $G, g \in T\,R[[T]]$ such that $F \equiv f \bmod T^N$ and $G \equiv g \bmod T^N$, then it is enough to prove that $F(G) \equiv f(g) \bmod T^N$. Now the congruences imply that $F_N = f_N$ and $G_N = g_N$ and last remark $F(G) \equiv F_N(G_N) = f_N(g_N) \equiv f(g) \bmod T^N$.

Corollary 2.1.1 *1. For $g \in T\,R[[T]]$ fixed, we have that $g_* : R[[T]] \longrightarrow R[[T]]$ defined as $g_*(f) = f(g)$ is a R-algebra homomorphism.*

2. Let $f \in R[[T]]$ and $g, h \in T\,R[[T]]$ then $\big(f(g)\big)(h) = f\big(g(h)\big)$.

Proof. Both parts follow by continuity since they are true for polynomials. $\square$

Definition 2.1.3 *We define $R((T))$, the ring of Laurent series with coefficients in R, as $R[[T]]_T$ i.e. the localization of $R[[T]]$ at the multiplicative set of powers of T.*

Definition 2.1.4 *$f = \sum a_n T^n \in R((T))$, we define the order of f as*

$$\operatorname{ord} f = \min\{n \in \mathbb{Z} \mid a_n \neq 0\}.$$

Lemma 2.1.1 *$R[[T]]^\times$ is the set of $f = \sum a_n T^n \in R[[T]]$ such that $a_0 \in R^\times$.*

Proof. Let $f = \sum a_n T^n, g = \sum b_n T^n \in R[[T]]$, then $fg = 1$ if and only if $a_0 b_0 = 1$ and for $n \geq 1$, $\displaystyle\sum_{k=0}^{n} a_k b_{n-k} = 0$. That means that if $a_0 \in R^\times$ and taking $b_0 = a_0^{-1}$, for $n \geq 1$ we have $b_n = -a_0^{-1} \displaystyle\sum_{k=0}^{n-1} b_k a_{n-k}$. Therefore when $a_0 \in R^\times$ we can inductively construct $g \in R[[T]]$ such that $fg = 1$. $\square$

Definition 2.1.5 *$f = \sum a_n T^n \in R((T))$, we define the order of f as*

$$\operatorname{ord} f = \min\{n \in \mathbb{Z} \mid a_n \neq 0\}.$$

Lemma 2.1.2 *$R[[T]]^\times$ is the set of $f = \sum a_n T^n \in R[[T]]$ such that $a_0 \in R^\times$.*

Proof. Let $f = \sum a_n T^n, g = \sum b_n T^n \in R[[T]]$, then $fg = 1$ if and only if $a_0 b_0 = 1$ and for $n \geq 1$, $\displaystyle\sum_{k=0}^{n} a_k b_{n-k} = 0$, that means that if $a_0 \in R^\times$, taking $b_0 = a_0^{-1}$ and for $n \geq 1$, $b_n = -a_0^{-1} \displaystyle\sum_{k=0}^{n-1} b_k a_{n-k}$ we can inductively construct $g \in R[[T]]$ such that $fg = 1$. $\square$

Remark 2.1.2

1. *Every $f \in R[[T]]$ not 0 factors as $f = T^N g$ with $N = \operatorname{ord}(f)$ and $g(0) \neq 0$.*
2. *If R is a field in last factorization, by lemma 2.1.2, we have that $g \in R[[T]]^\times$.*
3. *If R is a field, by the last remarks, $R((T))$ is the fraction field of $R[[T]]$.*

2.2 Formal Derivatives

In this section we will restrict to study formal power series over a field K of 0 characteristic. As usual, we define the formal derivative $\frac{d}{dT} : K[[T]] \longrightarrow K[[T]]$ as

$$\frac{d}{dT}(\sum a_n T^n) = (\sum a_n T^n)' = \sum n a_n T^{n-1}.$$

Here some other useful properties:

Remark 2.2.1

1. *By definition, $f' = 0$ if and only if $f \in K$.*
2. *$\frac{d}{dT}$ is linear and continuous with respect to the T-adic topology.*
3. *We have a product formula: for $f, g \in K[[T]]$, $(fg)' = f'g + g'f$. Indeed, since it is true for polynomials, it follows by continuity.*

Lemma 2.2.1 *Let $f, g \in K[[T]]$. If $g \in T\,K[[T]]$ or $f \in K[T]$ then $(f(g))' = f'(g)g'$.*

Proof. By induction is easy to get $(g^n)' = ng^{n-1}g'$ so the conclusion is true for $f = T^n$, by linearity it is true for any $f \in K[T]$. If $g \in T\,K[[T]]$, $f(g)$ is a limit of series $f_n(g)$ where f_n are polynomials, then it follows by continuity. □

Definition 2.2.1 *We define the* **Exponential and Lambda series** *respectively as*

$$\exp = \sum_{n=0}^{\infty} \frac{T^n}{n!} \in K[[T]]^{\times} \text{ and } \lambda = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{T^n}{n} \in T\,K[[T]].$$

Remark 2.2.2

1. *Is easy to see that $\exp = \exp'$ and $\lambda' = (1+T)^{-1}$.*
2. *$\exp$ and is the only series $f \in \mathbb{C}_p[[T]]$ such that $f' = f$ and $f(0) = 1$ (Because for $f = \sum a_n T^n$, $f' = f$ imply that $a_{n+1} = (n+1)a_n$).*
3. *For $f \in T\,K[[T]]$, $F = \exp(f)$ is well defined, $F(0) = 1$ (so $F \in K[[T]]^{\times}$) and by Lemma 2.2.1 $F' = \exp(f)f'$, then $F'/F = f'$.*

Definition 2.2.2 *For $f \in K[[T]]^{\times}$ we define its logarithmic derivative as $\delta(f) = f'/f$.*

Notice that if $h \in K[[T]]^{\times}$ then $\delta(h) \in K[[T]]$, and by the product formula for derivatives, if $f, g \in K((T))^{\times}$ then $\delta(fg) = \delta(f) + \delta(g)$.

Lemma 2.2.2 *Let $f, g \in K[[T]]^{\times}$. $\delta(f) = \delta(g)$ if and only if $f/g \in K^{\times}$.*

Proof. Let $h = f/g \in K[[T]]^\times$, then $\delta(f) = \delta(gh) = \delta(g) + \delta(h)$ therefore we have equivalences: $\delta(f) = \delta(g) \iff \delta(h) = 0 \iff h' = 0 \iff h \in K^\times$. □

Remark 2.2.3
From last lemma we can conclude that for $G \in K[[T]]^\times$ and $f \in T\,K[[T]]$ we have: $\delta(G) = \delta(\exp(f))$ if and only if $G = G(0)\exp(f)$.

Theorem 2.2.1 *The power series* $\exp$ *satisfy the following relations:*

1. *For $n \in \mathbb{N}$, $\exp(n\lambda) = (1+T)^n$. In particular $\exp(\lambda) = T + 1$.*

2. *For $f, g \in T\,K[[T]]$, $\exp(f+g) = \exp(f)\exp(g)$.*

3. *For $f, g \in T\,K[[T]]$, $\lambda(f[+]g) = \lambda(f) + \lambda(g)$, where $f[+]g = (1+f)(1+g) - 1$.*

Proof. (1) Note that for $f = \exp(n\lambda)$ we have $\delta(f) = n\lambda' = \delta\big((1+T)^n\big)$. Hence, by last lemma $f = (1+T)^n$.
(2) Let $H = \exp(f+g), F = \exp(f)$ and $G = \exp(g)$. Clearly they are well defined and lie in $K[[T]]^\times$. Now by last remark $\delta(H) = f + g = \delta(F) + \delta(G) = \delta(FG)$, therefore $H = FG$.
(3) Let $F = \lambda(f), G = \lambda(g) \in T\,K[[T]]$. Since

$$\exp(f+g) = \exp(f)\exp(g) = (1+f)(1+g) = (f[+]g) + 1,$$

we get $\lambda(f[+]g) = \lambda\big(\exp(f+g)+1\big)$. It is enough to show that $\lambda(exp - 1) = T$, but it follows from the fact that $\big(\lambda(\exp -1)\big)' = \exp' / \exp = 1$. □

Remark 2.2.4
As well as for power series, for $f = \sum_{n\in\mathbb{Z}} a_n T^n \in K((T))$ we can define a formal derivative $f' = \sum_{n\in\mathbb{Z}} n a_n T^{n-1}$ which also is K-linear, continuous and satisfies the usual product formula i.e. for $f, g \in K((T))$, $(fg)' = f'g + g'f$.

2.3 Convergence

From now on, let p a fix odd prime, v the p-adic valuation on $\overline{\mathbb{Q}}_p$ and $\overline{\mathbb{Q}}_p$, the algebraic closure of $\mathbb{Q}_p$. As is well known that the p-adic valuation can be extended in a unique way to $\mathbb{Q}_p^\times$ and $v(\mathbb{Q}_p^\times) = \mathbb{Q}$, where v denotes such extension. Since $\overline{\mathbb{Q}}_p$ is not complete, we define:

Definition 2.3.1 *We define $\mathbb{C}_p$ as the completion of $\overline{\mathbb{Q}}_p$.*

Let v and $|\ |$ denote the unique extensions on $\mathbb{C}_p$ of the p-adic valuation and the corresponding absolute normalized value. For any positive real number r, we define the following sets:

$$B_r = \{\zeta \in \mathbb{C}_p \mid |\zeta| < r\},$$
$$B'_r = \{\zeta \in \mathbb{C}_p \mid 0 < |\zeta| < r\}.$$

Let $p^{\mathbb{Q}} = \{p^q \mid q \in \mathbb{Q}\}$. Since it coincides with the set of absolute values of elements of $\mathbb{C}_p^{\times}$, if $r \in \mathfrak{p}^{\mathbb{Q}}$ we can define

$$S_r = \{\zeta \in \mathbb{C}_p \mid |\zeta| = r\}.$$

Definition 2.3.2 *$f = \sum_{n=0}^{\infty} a_k T^k \in \mathbb{C}_p[[T]]$ converges at $\xi \in \mathbb{C}_p$ if $\sum_{n=0}^{\infty} a_k \xi^k$ converges. In such case, as usual, we will denote $f(\xi) = \sum_{k=0}^{\infty} a_k \xi^k$.*

It is well known that this happens if and only if $|a_k \xi^k| \to 0$. Also, if A converges at some $\xi \neq 0$ if and only if A has a positive radius of convergence (which may be infinite).

Definition 2.3.3 *Let K a complete subfield of $\mathbb{C}_p$.*
We define $K[[T]]_r$ as the set of $f \in K[[T]]$ which are convergent at every point of B_r.

Lemma 2.3.1 *Let $f = \sum a_k T^k \in \mathbb{C}_p[[T]]_r$. The associated function defined on B_r, $f : \zeta \longmapsto f(\zeta)$, is continuous.*

Proof. Let $\zeta_n, \zeta \in B_r$ such that $\zeta_n \longrightarrow \zeta$. Note that for $a, b \in \mathbb{C}_p$, $|a|, |b| < s$ we have

$$|a^{k+1} - b^{k+1}| \leq |a - b| \max_{0 \leq j \leq k} |a^j b^{k-j}| \leq |a - b| s^k.$$

Now since $\zeta_m \longrightarrow \zeta$ we can take $s > 0$, $|\zeta| < s < 1$ and $N \in \mathbb{N}$ such that for $n \geq N$, $|\zeta_m| < s$ then

$$\left|\sum a_k \zeta_m^k - \sum a_k \zeta^k\right| \leq \sup_{k \in \mathbb{N}} |a_k||\zeta_m^k - \zeta^k| \leq \frac{1}{s}\left(\sup_{k \in \mathbb{N}} |a_k| s^k\right)|\zeta_m - \zeta|.$$

Since $s < R$ the supremum is finite, therefore $\lim_{n \to \infty} f(\zeta_n) = f(\zeta)$. □

Lemma 2.3.2 *Let $f = \sum a_n T^n \in \mathbb{C}_p[[T]]$ be convergent on B_r. If $f(\xi_n) = 0$ for a sequence $(\xi_n)_{n \in \mathbb{N}} \subseteq \mathbb{C}_p$ such that $0 < |\xi_n| < r$ and $\lim_{n \to \infty} \xi_n = 0$ then $f = 0$.*

Proof. Taking a subsequence if necessary we can assume $|\xi_1| > |\xi_2| > \ldots$. If $f \neq 0$ we can take m minimal such that $a_m \neq 0$ then

$$-a_m = \sum_{k > m} a_k \xi_n^{k-m} = \xi_n \sum_{k > m} a_k \xi_n^{k-m-1},$$

$$|a_m| = |\xi_n| \left| \sum_{k>m} a_k \xi_n^{k-m-1} \right| \leq |\xi_n| \sup_{k>m} |a_k \xi_n^{k-m-1}| \leq |\xi_n| \sup_{k>m} |a_k \xi_1^{k-m-1}|. \tag{2.1}$$

Since $\sum a_k \xi_1^k$ is convergent we have $\sup_{k>m} |a_k \xi_1^{k-m-1}| < \infty$, therefore the last inequality implies that a_m must be 0, which is a contradiction. □

Lemma 2.3.3 (Unicity Lemma) *If $f, g \in \mathbb{C}_p[[T]]$ converges on B_r and $f(\xi_n) = g(\xi_n)$ for a sequence $(\xi_n) \subseteq B_r$ which converges to some $\xi \in B_r$ then $f = g$.*

Proof. If $\xi = 0$, we may apply last lemma to $h = f - g$ taking an appropiate subsequence. If $\xi \neq 0$ we can reduce to the previous case taking $F = f(T+\xi)$ and $G = g(T+\xi) \in \mathbb{C}_p[[T]]$ we have that they are convergent on $B_{r-|\xi|}$ and satisfiy $F(\xi_n - \xi) = G(\xi_n - \xi)$. By the previous case $F = G$, therefore $f = g$. □

Lemma 2.3.4 *λ converges for all $|\zeta| < 1$.*

Let $v(\zeta) > 0$ and $c = p^{v(\zeta)} = 1/|\zeta| < 1$. Since $v(n) < \frac{\ln n}{\ln p}$ and $v(\zeta) = \frac{\ln c}{\ln p}$ we have

$$v\left(\frac{\zeta^n}{n}\right) = nv(\zeta) - v(n) \geq n\frac{\ln c}{\ln p} - \frac{\ln n}{\ln p} = \frac{1}{\ln p} \ln\left(\frac{c^n}{n}\right).$$

That means that $\left|\frac{\zeta^n}{n}\right| \leq \frac{c^n}{n}$, hence $\sum (-1)^n \frac{\zeta^n}{n}$ must be convergent.

Lemma 2.3.5 *For all $n \in \mathbb{N}$ we have,*

$$\frac{n-p}{p-1} - \frac{\log n}{\log p} < v_p(n!) < \frac{n}{p-1}.$$

In particular the exponential series converges for $|\zeta| < p^{-\frac{1}{p-1}}$.

Proof. Since $[n/p^k]$ is the number of multiples of p^k less or equal to n, is easy to see that

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

Now, let $n = a_0 + a_1 p + \ldots + a_p^r$ with $0 \leq a_j < p$, then for $k \leq r$ we have

$$[n/p^k] = a_k + a_{k+1} p + \ldots + a_r p^{r-k}.$$

Therefore

$$v_p(n!) = \sum_{k=1}^{r} [n/p^k] = \sum_{k=1}^{r} \sum_{j=k}^{r} a_j p^{j-k} = \sum_{j=1}^{r} a_j \sum_{i=0}^{j-1} p^i = \frac{1}{p-1} \sum_{j=0}^{r} a_j (p^j - 1) < \frac{n}{p-1}.$$

For the other inequality, note that since $n/p^k - 1 < [n/p^k]$ we have

$$v_p(n!) \geq \sum_{k=1}^{r} \left(\frac{n}{p^k} - 1\right) = \frac{n}{p-1} - \frac{np^{-r}}{p-1} - r > \frac{n-p}{p-1} - \frac{\log n}{\log p}.$$

□

Chapter 3

p-adic Interpolation

From now on p is a fixed prime, assumed odd.

3.1 Dirichlet Characters

Definition 3.1.1 (Dirichlet Characters) *Let n and integer, $n \geq 1$. A map*

$$\chi : \mathbb{N} \longrightarrow \mathbb{C}$$

is called a **Dirichlet Character to the modulus** n *if*

1. *$\chi(a)$ depends only upon the residue class of $a \bmod n$.*
2. *χ is compleatly multiplicative i.e. for all $a, b \in \mathbb{N}$ we have $\chi(ab) = \chi(a)\chi(b)$.*
3. *$\chi(a) \neq 0$ if and only if a is prime to n.*

Remark 3.1.1

1. *Let $n \in \mathbb{Z}$, $n \geq 1$. There is a one to one correspondence between the Dirichlet character to modulus n and the usual characters of the multiplicative group $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$. Therefore there are exactly $\varphi(n)$ Dirichlet characters to the modulus n.*
2. *If $m \mid n$,* any *$\widehat{\chi} \in \mathrm{Hom}\big(\left(\mathbb{Z}/m\mathbb{Z}\right)^{\times}, \mathbb{C}^{\times}\big)$ induces another homomorphism one has by composition with the canonical homomorphism,*

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times} \longrightarrow \left(\mathbb{Z}/m\mathbb{Z}\right)^{\times} \xrightarrow{\widehat{\chi}} \mathbb{C}^{\times}$$

Definition 3.1.2 *A Dirichlet character χ to a modulus n is called* **primitive** *if it is not induced by any character to a modulus m with $m < n$. The integer n is the called the conductor of χ and is denoted by f_{χ}.*

For n prime to p we have the following isomorphisms:

$$\left(\mathbb{Z}/m_0 p^{n+1}\mathbb{Z}\right)^\times = \left(\mathbb{Z}/m_0\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^\times$$

Definition 3.1.3 *Let χ a Dirichlet Character. The character χ is said to be of* **first kind** *if the p-th part of f_χ is 1 or p and of* **second kind** *if f_χ is a power of p.*

Proposition 3.1.1 *Every Dirichlet character χ has a unique factorization $\chi = \theta\psi$ where θ is of first kind and ψ is of second kind.*

3.2 Generalized Bernoulli Numbers

Classically the Bernoulli numbers B_n and Bernoulli polynomials $B_n(X)$ are defined by their generating functions $F(T) = \dfrac{Te^T}{e^T - 1}$ and $F(T, X) = F(T)e^{TX}$ respectively. For a Dirichlet character χ, with conductor $f = f_\chi$, the formal power series $F_\chi(T)$ and $F_\chi(T, X)$ are defined as

$$F_\chi(T) = \sum_{a=1}^{f} \chi(a)\frac{Te^{aT}}{e^{fT} - 1} \quad \text{and} \quad F_\chi(T, X) = F_\chi(T)e^{TX} = \sum_{a=1}^{f} \chi(a)\frac{Te^{(a+X)T}}{e^{fT} - 1}.$$

Definition 3.2.1 *The generalized Bernoulli numbers $B_{n,\chi}$ and generalized Bernoulli polynomials $B_{n,\chi}(X)$ respect the character χ are defined as*

$$F_\chi(T) = \sum_{n=0}^{\infty} B_{n,\chi}\frac{T^n}{n!} \quad \textit{and} \quad F_\chi(T, X) = \sum_{n=0}^{\infty} B_{n,\chi}(X)\frac{T^n}{n!}.$$

Proposition 3.2.1 *The Bernoulli polynomials satisfy by the formulas:*

1. $B_{n,\chi}(X) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k,\chi}X^k$, *in particular* $B_{n,\chi}(0) = B_{n,\chi}$.

2. $\sum_{a=1}^{kf} \chi(a)a^n = \dfrac{1}{n+1}\left\{B_{n+1,\chi}(kf) - B_{n+1,\chi}\right\}.$

Proof. The first part is a consequence of the standard product formula for series. Let us prove the second one:

$$F_\chi(T, X + f) - F_\chi(T, X) = F_\chi(T)(e^{(X+f)T} - e^{XT}) = \sum_{a=1}^{f} \chi(a)Te^{(a+X)T},$$

looking at the coefficients corresponding to T^{n+1} we get

$$B_{n+1,\chi}(X+f) - B_{n+1,\chi}(X) = (n+1)\sum_{a=1}^{f} \chi(a)(a+X)^n.$$

Finally evaluating at $X = jf$ for $j = 0, \ldots, k$ and summing,

$$\begin{aligned} B_{n+1,\chi}(kf) - B_{n+1,\chi}(0) &= (n+1)\sum_{j=0}^{k-1}\sum_{a=1}^{f} \chi(a)(a+jf)^n \\ &= (n+1)\sum_{a=1}^{kf} \chi(a)a^n. \end{aligned}$$

□

The previous proposition can be used to characterize p-adically the Bernoulli numbers. Let

$$S_{n,\chi}(X) = \frac{1}{n+1}\big(B_{n+1,\chi}(X) - B_{n+1,\chi}\big),$$

therefore, by the previous proposition,

$$S_{n,\chi}(kf) = \frac{1}{n+1}\big(B_{n+1,\chi}(kf) - B_{n+1,\chi}\big) = \sum_{a=1}^{kf} \chi(a)a^n. \tag{3.1}$$

Corollary 3.2.1 *As an element of* $\mathbb{Q}_p(\chi)$*,*

$$B_{n,\chi} = \lim_{h\to\infty} \frac{1}{fp^h} S_{n,\chi}(fp^h).$$

Proof. By Proposition 3.2.1, $B_{n+1,\chi}(X) = B_{n+1,\chi} + (n+1)B_{n,\chi}X \bmod X^2$, then

$$S_{n,\chi}(fp^h) = \frac{1}{n+1}\big(B_{n,\chi}(fp^h) - B_{n,\chi}\big) \equiv B_{n,\chi} \bmod p^{2h}.$$

□

3.3 The Normed space P_K

For any power series $A = \sum a_k T^k \in K[[T]]$ set $\|A\| = \sup |a_k|$.

Definition 3.3.1 *Let* P_K *denote the set of* $A \in K[[T]]$ *such that* $\|A\| < \infty$*.*

Remark 3.3.1

Let $A, B \in P_K$ and $a \in K$*, then:*

1. $\|A\| \geq 0$ *and* $\|A\| = 0$ *if and only if* $A = 0$*.*

2. $\|A + B\| \leq \max\{\|A\|, \|B\|\}$ *and* $\|aA\| = |a|\|A\|$*.*

3. $\|AB\| \leq \|A\|\|B\|$*.*

4. *P_K is a subalgebra of $K[[T]]$ and $K[T] \subseteq P_K$.*

1 and 2 and 3 are trivial and for 4 taking m, n such that $|a_m| = \|A\|$ and $|b_n| = \|B\|$, if $AB = \sum c_r T^r$ then

$$|c_r| \leq \max_{s+t=r} |a_s||b_t| \leq |a_n||b_m| = \|A\|\|B\|.$$

Proposition 3.3.1 *The K-algebra P_K is complete respect to $\| \|$.*

Let $(A_n) \subseteq P_K$ be a Cauchy sequence with respect to $\| \|$ say $A_n = \sum a_{nk} T^k$. Let us split the remaining of the proof in 3 steps:

i) For each $k \in \mathbb{N}$, the sequence $(a_{n,k}) \subseteq K$ is convergent.

ii) If $a_k = \lim_{n\to\infty} a_{n,k}$ then $A = \sum a_k T^k \in P_K$.

iii) Finally, A_n converges to A.

Proof.

i) Taking any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $n, m \geq N$ implies that $\|A_n - A_m\| < \varepsilon$, in particular $|a_{n,k} - a_{m,k}| < \varepsilon$. That means that, for fixed k, $(a_{n,k}) \subseteq K$ is Cauchy, hence convergent.

ii) Since $(A_n)_{n\in\mathbb{N}}$ is Cauchy, it is bounded, say by $C > 0$. Then for all n and all k, $|a_{n,k}| \leq \|A_n\| \leq C$, therefore $|a_k| \leq C$ so $A \in P_K$.

iii) For $\varepsilon > 0$ and N such that $n, m \geq N$, $\|A_n - A_m\| < \varepsilon$ for any $k \in \mathbb{N}$ $|a_{n,k} - a_{m,k}| \leq \|A_n - A_m\| < \varepsilon$ so fixing k and taking limit when n goes to infinity we get that for $m \geq N$, $|a_k - a_{mk}| \leq \varepsilon$ hence $\|A - A_m\| < \varepsilon$. Since this happens for any $\varepsilon > 0$ means that A_n converges to A. □

Definition 3.3.2 *We define the combinatorial polynomials $\binom{T}{n}$ as*

$$\binom{T}{n} = \frac{1}{n!} \prod_{k=0}^{n-1} (T - k).$$

Clearly we have that $\|\binom{T}{n}\| \leq |\frac{1}{n!}|$. By Lemma 2.3.5 we have the

$$\left|\frac{1}{n!}\right| = \left(\frac{1}{p}\right)^{v(n!)} \leq p^{-\frac{1}{p-1}}. \tag{3.2}$$

Given any sequence $(b_n) \subseteq K$, there exists a unique sequence (c_n) such that

$$e^{-T} \sum b_n \frac{T^n}{n!} = \sum c_n \frac{T^n}{n!}.$$

This means that,

$$\frac{c_n}{n!} = \sum_{i=0}^{n} \frac{b_i}{i!} \frac{(-1)^{n-i}}{(n-i)!} \quad \text{and} \quad \frac{b_n}{n!} = \sum_{i=0}^{n} \frac{c_i}{i!} \frac{1}{(n-i)!},$$

therefore

$$c_n = \sum_{i=0}^{n} \binom{n}{i} b_i (-1)^{n-i} \quad \text{and} \quad b_n = \sum_{i=0}^{n} \binom{n}{i} c_i.$$

With these notations we have:

Lemma 3.3.1 (Interpolation) *Let $0 < r < |p|^{\frac{1}{p-1}}$ and $|c_n| \leq Cr^n$ for some $C > 0$. Then there exists a unique $A \in P_K$ convergent for $|\xi| < \delta = |p|^{\frac{1}{p-1}}/r$ such that for all $n \in \mathbb{N}$,*

$$A(n) = b_n$$

Proof. Let $A_k(T) = \sum_{i=0}^{k} \binom{T}{i} c_i$. Clearly $A_k(n) = b_n$ and using lemma 2.3.5

$$\left\| c_i \binom{T}{i} \right\| \leq |c_i| \left| \frac{1}{i!} \right| \leq |c_i| p^{\frac{-i}{p-1}} \leq C \left(|p|^{\frac{-1}{p-1}} \right)^i = C\delta^{-i}.$$

For $j \geq k$,

$$\|A_j - A_{k-1}\| \leq \max_{k \leq i \leq j} \left\| c_i \binom{T}{i} \right\| \leq C\delta^{-k}, \tag{3.3}$$

since $\delta < 1$ this means that (A_k) is Cauchy, then exists $A \in P_K$ such that $A_k \to A$ respect to $\|\ \|$. Let $A = \sum a_j T^j$ and $A_k = \sum a_{jk} T^j$, as we have seen $a_{jk} \to a_k$ as j increases, in the other hand since $\deg(A_{k-1}) \leq k-1$ we have $a_{k,k-1} = 0$ then for $j \geq k$ using the bound (3.3) we get

$$|a_{j,k}| = |a_{j,k} - a_{k,k-1}| \leq \|A_j - A_{k-1}\| \leq C\delta^{-k},$$

taking limit as j increases we obtain

$$|a_k| \leq C\delta^{-k}. \tag{3.4}$$

This means that $A(\xi)$ converge for $|\xi| < \delta$, in particular in the integers.

Claim: For a fix element $\xi \in \mathbb{C}_p$ such that $|\xi| < \delta$, $A_k(\xi) \to A(\xi)$.
Let $b_{j,k} = a_j - a_{j,k}$, then $A(\xi) - A_k(\xi) = \sum b_{j,k}\xi^j$. Is enough to prove that $\sup_j |b_{j,k}\xi^j| \to 0$ as $k \to \infty$. For $j > k$, using the bound (3.4)

$$|b_{j,k}\xi^j| = |a_j \xi^j| \leq C(\delta^{-1}|\xi|)^j \leq C(\delta^{-1}|\xi|)^k$$

and for $j \leq k$, (using the bound (3.3))

$$|b_{j,k}\xi^j| \leq \|A - A_k\||\xi|^j \leq C\delta^{-(k+1)}|\xi|^j \leq \begin{cases} C\delta^{-k} & \text{if } |\xi| \leq 1, \\ C(\delta^{-1}|\xi|)^k & \text{if } |\xi| > 1. \end{cases}$$

Therefore if we call $m = \max\{\delta^{-1}, (\delta^{-1}|\xi|)\} < 1$ then

$$|A(\xi) - A_k(\xi)| = \sup_j |b_{j,k}\xi^j| \leq Cm^k,$$

this means that $A_k(\xi) \to A(\xi)$ as $k \to \infty$. □

3.4 p-adic L-function: Classical Approach

Let χ a Dirichlet character of conductor f and $K = \mathbb{Q}_p(\chi)$ i.e. $K = \mathbb{Q}(\chi(1), \chi(2), \ldots)$.Consider $\omega : \mathbb{Z} \longrightarrow \mathbb{C}$ be a fixed embedding of the Teichmüller character in $\mathbb{C}$.

Definition 3.4.1 *The twisted characters of χ are the Dirichlet characters χ_n induced by $\chi\omega^{-n}$ i.e. for a prime to p,*

$$\chi_n(a) = \chi(a)\omega^{-n}(a).$$

Let $p \nmid n$, since ω has conductor p, $f_n = f_{\chi_n}|pf$ but $\chi = \chi_n\omega^n$ hence $f|pf_n$ so in general for any n, $f_n = p^a f$ with $a = 0, 1$. Finally let

$$b_n = \big(1 - \chi_n(p)p^{n-1}\big)B_{n,\chi_n}$$

and

$$c_n = \sum_{i=0}^{n} \binom{n}{i} b_i(-1)^{n-i}.$$

Lemma 3.4.1 *For any $n \geq 0$,*

$$|c_n| \leq \frac{1}{|p^2 f|}|p|^n.$$

Proof. By Corollary 3.2.1 and using the fact that $f_n = p^\alpha f$ and (3.1),

$$B_{n,\chi_n} = \lim_{h\to\infty} \frac{1}{p^h f_n} S_{n,\chi_n}(p^h f_n) = \lim_{h\to\infty} \frac{1}{p^h f} S_{n,\chi_n}(p^h f) = \lim_{h\to\infty} \frac{1}{p^h f} \sum_{a=1}^{p^h f} \chi_n(a)a^n,$$

replacing this limit in the definition of b_n,

$$\begin{aligned} b_n &= \big(1 - \chi_n(p)p^{n-1}\big)B_{n,\chi_n} \\ &= B_{n,\chi_n} - \lim_{h\to\infty} \frac{\chi_n(p)p^{n-1}}{p^{h-1}f} \sum_{a=1}^{p^{h-1}f} \chi_n(a)a^n \\ &= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{c=1}^{p^h f} \chi(c)c^n - \lim_{h\to\infty} \frac{1}{p^h f} \sum_{a=1}^{p^{h-1}f} \chi_n(ap)(ap)^n. \end{aligned}$$

Eliminating the repeated terms and using that $\chi_n(a)a^n = \chi(a)\langle\, a\,\rangle^n$,

$$b_n = \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1,\\(a,p)=1}}^{p^h f} \chi_n(a)a^n = \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1,\\(a,p)=1}}^{p^h f} \chi(a)\langle\, a\,\rangle^n. \tag{3.5}$$

Now, replacing (3.5) in the definition of c_n

$$\begin{aligned} c_n &= \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1,\\(a,p)=1}}^{p^h f} \chi(a)\langle\, a\,\rangle^i \\ &= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1,\\(a,p)=1}}^{p^h f} \chi(a) \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} \langle\, a\,\rangle^i \\ &= \lim_{h\to\infty} \frac{1}{p^h f} \sum_{\substack{a=1,\\(a,p)=1}}^{p^h f} \chi(a)\big(\langle\, a\,\rangle - 1\big)^n = \lim_{h\to\infty} \frac{1}{p^h f} c_n(h), \end{aligned}$$

where $c_n(h) = \displaystyle\sum_{\substack{a=1,\\(a,p)=1}}^{p^h f} \chi(a)\big(\langle\, a\,\rangle - 1\big)^n$, clearly is an integral element of K.

Claim. For all $n \in \mathbb{N}$, $c_n(h) \equiv 0 \bmod p^{n+h-2}$.

Since $\langle\, a\,\rangle \equiv 1 \bmod p$ then $\big(\langle\, a\,\rangle - 1\big)^n \equiv 0 \bmod p^n$ hence $c_n(1) \equiv 0 \bmod p^n$. Let us proceed by induction on h. The case $h = 1$ is done, if $h \geq 1$ let us assume that $c_n(h) \equiv 0 \bmod p^{n+h-2}$. By standard division each $1 \leq a \leq p^{h+1}f$ can be uniquely written as $a = u + p^h f v$ where $1 \leq u \leq p^h f$, $0 \leq v \leq p - 1$ and $u \equiv a \bmod p^h f$, then $\omega(u) = \omega(a)$ and

$$\langle\, a\,\rangle = \langle\, u\,\rangle + p^h f \omega(u)^{-1} v,$$

then,

$$\big(\langle\, a\,\rangle - 1\big)^n = \sum_{k=0}^{n} \binom{n}{k} \big(\langle\, u\,\rangle - 1\big)^k (p^h f \omega(u)^{-1} v)^{n-k}.$$

Since $\langle\, u\,\rangle \equiv 1 \bmod p$ the k-th term of last sum is divisible by $p^{k+(n-k)h} f$, now for $n - k \geq 1$, $k + (n-k)h = n + (n-k)(h-1) \geq n + h - 1$, hence

$$\big(\langle\, a\,\rangle - 1\big)^n \equiv \big(\langle\, u\,\rangle - 1\big)^n \bmod p^{n+h-1},$$

and since $a \equiv u \bmod f$, $\chi(a) = \chi(u)$ then

$$\chi(a)\big(\langle\, a\,\rangle - 1\big)^n \equiv \chi(u)\big(\langle\, u\,\rangle - 1\big)^n \bmod p^{n+h-1}.$$

Summing up along $1 \leq a \leq p^{h+1} f$ such that $(a,p) = 1$,

$$\begin{aligned} \sum_{\substack{a=1,\\(a,p)=1}}^{p^{h+1} f} \chi(a)\big(\langle\, a\,\rangle - 1\big)^n &\equiv \sum_{v=0}^{p-1} \sum_{\substack{u=1,\\(u,p)=1}}^{p^h f} \chi(u)\big(\langle\, u\,\rangle - 1\big)^n \bmod p^{n+h-1}, \\ c_n(h+1) &\equiv p c_n(h) \equiv 0 \bmod p^{n+h-1}. \end{aligned}$$

The claim is proved.

Since $c_n(h) = p^{h+n-2}\theta_n(h)$, for some $\theta_n(h)$ with $|\theta_n(h)| \leq 1$, we can conclude

$$|c_n| = \lim_{h\to\infty} \frac{1}{|p^{n+h}f|}|c_n(h)| = \lim_{h\to\infty} \frac{1}{|p^h f|}|p^{n+h-2}\theta_n(h)| \leq \frac{1}{|p^2 f|}|p^n|$$

□

Corollary 3.4.1 *There exists $A_\chi \in K[[T]]$ convergent for $|\zeta| < |p|^{-\frac{p}{p-1}}(> 1)$ such that,*

$$A_\chi(n) = \big(1 - \chi_n(p)p^{n-1}\big)B_{n,\chi_n}.$$

Proof. Taking $r = |p|$ and $C = \frac{1}{|p^2 f|}$, we can apply the interpolation lemma (lemma 3.3.1) for b_n an c_n as above, since the previous lemma says that $|c_n| \leq Cr^n$ and $r = |p| < |p|^{\frac{1}{p-1}}$, hence there exists such $A_\chi \in K[[T]]$ convergent for $|\xi| < |p|^{\frac{1}{p-1}}|p|^{-1} = |p|^{-\frac{p}{p-1}}$ which takes the prescribed values at the non negative integers, $A_\chi(n) = b_n$. □

Theorem 3.4.1 *There exists a unique $p-$adic meromorphic function $L_p(s,\chi)$ on $B(1,r) \subseteq \mathbb{C}_p$, where $r = |p|^{-\frac{p}{p-1}}$, such that:*

1. $L_p(s,\chi) = \dfrac{a_{-1}}{s-1} + \displaystyle\sum_{n=0}^{\infty} a_n(s-1)^n$ *with* $a_1 = \begin{cases} 1 - \dfrac{1}{p} & \text{if } \chi = 1 \\ 0 & \text{if } \chi \neq 1 \end{cases}$.

2. $L_p(s,\chi) = -\big(1 - \chi_n(p)p^{n-1}\big)\dfrac{B_{n,\chi_n}}{n}$.

Proof. Take for A_χ the one of the Corollary 3.4.1 then

$$L_p(s,\chi) = \frac{1}{s-1}A_\chi(1-s),$$

holds the conditions. The unicity follows from Lemma 2.3.3. □

Chapter 4

Stickelberger Elements and p-adic L-Functions

We fix the notation $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C}$. We fix once and for all an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ so that ζ_n is also an element of $\mathbb{C}_p$.

4.1 The Cyclotomic Character

Lemma 4.1.1 *We have isomorphisms*

$$\sigma_n : (\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow \mathrm{Gal}\big(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p\big),$$

given by $\sigma_n(a) : \zeta_{p^n} \longmapsto \zeta_{p^n}^a$.

Proof. Clearly σ_n is a group homomorphism and its kernel consists in the $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ such that $\zeta_{p^n}^a = \zeta_{p^n}$ but by definition of ζ_{p^n} this is equivalent to say that $a = 1 \bmod p^n\mathbb{Z}$, hence σ_n is injective. For the surjectivity take $\sigma \in \mathrm{Gal}\big(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p\big)$ i.e. $\sigma \in Aut\big(\mathbb{Q}_p(\zeta_{p^n})\big)$ and σ acts trivially in $\mathbb{Q}_p$ hence sigma is determined by its value $\sigma(\zeta_{p^n})$ which must be another p^n root of 1 so $\sigma(\zeta_{p^n}) = \zeta_{p^n}^a$ with $a \neq 0 \bmod p$.

Corollary 4.1.1 *For* $1 \leq m < n$ *the Galois isomorphisms*

$$\sigma_{n,m} : \mathbb{Z}/p^{n-m}\mathbb{Z} \longrightarrow \mathrm{Gal}\big(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_{p^m})\big),$$

are given by $\sigma_{n,m}(k) : \zeta_{p^n} \longmapsto \zeta_{p^n}^{1+kp^m} = \zeta_{p^{n-m}}^k \zeta_{p^n}$.

Proof. Let $\sigma \in \mathrm{Gal}\big(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p(\zeta_{p^m})\big)$, $\sigma(\zeta_{p^n}) = \zeta_{p^n}^a$ with $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Since $(\zeta_{p^n})^{p^{n-m}} = \zeta_{p^m}$ must be fixed, $a \equiv 1 \bmod p^m$ so $a = 1 + kp^m \bmod p^n$ where k runs through $\mathbb{Z}/p^m\mathbb{Z}$. □

Let $\mathbb{Q}_p(\zeta_{p^\infty}) = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_p(\zeta_{p^n})$ and $G = \mathrm{Gal}\big(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p\big)$ then we have the following canonical isomorphisms

$$G \cong \varprojlim \mathrm{Gal}\big(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p\big) \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times .$$

Definition 4.1.1 *We define the canonical character* $\kappa : G \xrightarrow{\simeq} \mathbb{Z}_p^\times$.

Let $\mu_n \subseteq \mathbb{Q}_p(\zeta_{p^n})$ be the group of p^n-roots of 1 and $N_n = N_{\mathbb{Q}_p(\zeta_{p^n})|\mathbb{Q}_p(\zeta_{p^{n-1}})}$. Since $N_n(\zeta_{p^n}) = \prod_{\zeta^p=1} \zeta\zeta_{p^n} = \zeta_{p^{n-1}}$ we have an inverse system $\{N_n : \mu_n \longrightarrow \mu_{n-1}\}$.

Definition 4.1.2 *We define the Tate Module as* $\mathbb{Z}_p(1) = \varprojlim \mu_n$.

By construction $\mathbb{Z}_p(1)$ is naturally a $\mathbb{Z}_p$-module ($\mathbb{Z}_p$ acting by exponentiation) and admit a generator namely the sequence $\zeta = (\zeta_{p^n})$.

4.2 The Preparation Theorem

Let (K, v) be a finite extension of $(\mathbb{Q}_p, v_p)$ in $\mathbb{C}_p$, with valuation ring $\mathcal{O}$ and maximal $\mathfrak{p} = (\pi)$. For $f \in \mathcal{O}[[T]]$ say $f = \sum a_n T^n$ we can define the so called μ and λ invariants as

$$\mu(f) = \min\{v(a_n) | n \in \mathbb{N}\} \text{ and } \lambda(f) = \min\{n \in \mathbb{N} \,|\, v(a_n) = \mu(f)\}.$$

Now, Let us denote $\mathcal{O}[T]_N$ the set of polynomials of degree less than N in $\mathcal{O}[T]$.

Lemma 4.2.1 (Division lemma) *Let $f, g \in \mathcal{O}[[T]]$, with $\mu(f) = 0$ and $\lambda = \lambda(f)$. Then we have a decomposition*

$$g = qf + r$$

where $q \in \mathcal{O}[[T]]$ and $r \in \mathcal{O}[T]_{\lambda(f)}$. Further such decomposition is unique.

Proof. By hypothesis $f = f_0 + T^\lambda u$ where $u \in \mathcal{O}[[T]]^\times$ and $f_0 \in \pi\mathcal{O}[T]_\lambda$. Now $g = h_0 T^\lambda + r_0$ with $r_0 \in \mathcal{O}_\lambda[T]$ so by taking $q_0 = h_0 u^{-1}$ and reducing $\bmod \pi$, we get

$$\overline{g} = \overline{q}_0 \overline{u} T^\lambda + \overline{r_0} = \overline{f}\overline{q_0} + \overline{r_0}.$$

That means that for some $g_1 \in \mathcal{O}[[T]]$ we have

$$g = q_0 f + r_0 + \pi g_1,$$

applying the same argument to g_1 we obtain $r_1 \in \mathcal{O}[T]_\lambda$ and $q_1, g_2 \in \mathcal{O}[[T]]$ such that $g_1 = q_1 f + r_1 + \pi g_2$, therefore

$$g = (q_0 + \pi q_1)f + (r_0 + \pi r_1) + \pi^2 g_2.$$

Repeating the process we obtain $(q_n) \subseteq \mathcal{O}[[T]]$, $(r_n) \subseteq \mathcal{O}_\lambda[[T]]$ such that $q = \sum q_n \pi^n$, $r = \sum g_n \pi^n$ are convergent, $r \in \mathcal{O}[T]_\lambda$ and $g = qf + r$. □

Definition 4.2.1 *A polynomial $P \in \mathcal{O}[T]$ is said to be distinguished if $P = T^n + a_{n-1}T^{n-1} + \ldots + a_0$ with $a_i \in \mathfrak{p}$ i.e. P is monic and $P - T^{degf} \in \mathfrak{p}[T]$.*

Theorem 4.2.1 (p-adic Weierstrass Preparation theorem) *Let $f \in \mathcal{O}[[T]]$ not zero, $\mu = \mu(f)$ and $\lambda = \lambda(f)$. We may factor f uniquely as*

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

where $P \in \mathcal{O}[T]$ is distinguished of degree λ and $u \in \mathcal{O}[[T]]^\times$.

Proof. Dividing f by π^μ, it is enough to check the case when $\mu(f) = 0$. Now, we can apply the division lemma to T^λ and f we get $g \in \mathcal{O}[[T]]$ and $r \in \mathcal{O}[T]_\lambda$ such that $T^\lambda = gf + r$. By reduction $\bmod\, \mathfrak{p}$ we get

$$\overline{r} = T^\lambda - \overline{g}\overline{f},$$

but by hypothesis $\overline{f}$ is divisible by T^λ, then so does $\overline{r}$. Since $\deg \overline{r} \leq \deg r < \lambda$, we have that $\overline{r} = 0$ i.e. $r = 0 \bmod \mathfrak{p}$. Now set $P = T^\lambda - r(T)$, clearly it is distinguished and since $T^\lambda = \overline{g}\overline{f}$ the constant term of g cannot be $0 \bmod \mathfrak{p}$ so $g \in \mathcal{O}[[T]]^\times$. Taking $u = 1/g$ we obtain $f = P(T)u(T)$ as was to be shown. □

Remark 4.2.1

1. *For $f \in \mathcal{O}_K[[T]]$ not zero, the factorization $f = \pi^\mu P(T)u(T)$ with $P \in \mathcal{O}[T]$ distinguished and $u \in \mathcal{O}[[T]]^\times$ is called the* **Weierstrass Factorization** *of f and P the* **Weierstrass Polynomial** *of f.*

2. *If $u \in \mathcal{O}[[T]]^\times$ then $|u(\zeta)| = 1$ for all $\zeta \in B_1$ (by Lemma 2.1.2 $u(0) \in \mathcal{O}^\times$ i.e. $|u(0)| = 1$, then for $\zeta \in B_1$ we must have $|u(z) - u(0)| \leq |\zeta| < 1$ therefore $|u(\zeta)| = 1$).*

Corollary 4.2.1 *If $f \in \mathcal{O}[[T]]$ is not zero then it has the same zeros of P in B_1, and each zero has the same multiplicity.*

Proof. By the preparation theorem $f = \pi^\mu P(T)u(T)$ with P a polynomial and $u \in \mathcal{O}[[T]]^\times$. By part 2 of Remark 4.2.1 the zeros of f in B_1 are zeros of P. Pick $a \in B_1$

among the zeros of f and set $g \in \mathcal{O}_K[[T]]$ such that $f = (T-a)^m g$ with $g(a) \neq 0$ and $g = \pi^\mu Q(T)v(t)$ the Weierstrass factorization of g. Since $Q(a) \neq 0$ and $(T-a)^m Q/P \in \mathcal{O}_K[[T]]^\times$, this quotient cannot have zeros neither poles therefore $P = (T-a)^m Q$ i.e. m is the common multiplicity of a as zero of f as well as zero of P. □

Last Corollary gives us another proof of the uniqueness Principle:

Corollary 4.2.2 *Let $f, g \in \mathcal{O}[[T]]$. If $f(\zeta) = g(\zeta)$ for infinitely many $\zeta \in B_1$ then $f = g$.*

Proof. Let $h = f - g$. If $h \neq 0$ by last corollary it must have at most finitely many zeros since they are the zeros of its Weierstrass polynomial. But this contradicts the hypothesis, therefore $h = 0$ i.e. $f = g$. □

Let $[p^n] = (T+1)^{p^n} - 1$. Clearly these polynomials are distinguished. For any $f \in \mathcal{O}[[T]]$, by the division lemma (Lemma 4.2.1) there exists $q_n \in \mathcal{O}[[T]]$ and $f_n \in \mathcal{O}[T]_{p^n}$ such that $f = q_n[p^n] + f_n$, hence there are well define K-algebra morphisms

$$\begin{array}{rccc} \varphi_n : & \mathcal{O}[[T]] & \longrightarrow & \mathcal{O}[T]/[p^n] \\ & f & \longmapsto & f_n \bmod [p^n]. \end{array}$$

Since $[p^n]$ is a factor of $[p^{n+1}]$, the canonical protections $\mathcal{O}[T]/[p^{n+1}] \longrightarrow \mathcal{O}[T]/[p^n]$ constitute an inverse system and induces a K-algebra morphism

$$\mathcal{O}[[T]] \longrightarrow \varprojlim \mathcal{O}[T]/\big((1+T)^{p^n} - 1\big).$$

Both sides have natural topologies, $\mathcal{O}[[T]]$ the one induced by the maximal ideal (p, T) and $\varprojlim \mathcal{O}[T]/[p^n]$ the one induced by the inverse limit. The following result can be found in [Was97, p. 114]

Theorem 4.2.2 *The last morphism is an algebraic and topological isomorphism.*

Proof. This morphism is surjective because for every coherent sequence in the inverse limit, we may take a sequence of representatives of each term $(f_n)_{n\in\mathbb{N}}$ and by definition it must be a cauchy sequence of polynomials so must have limit $f \in \mathcal{O}[[T]]$ and the coherence implies that $f \equiv f_n \bmod [p^n]$. For the injectivity note that any element of its kernel must be divisible for every $[p^n]$, hence must be 0. □

4.3 Group rings and Power Series

Let d prime to p. For each $n \in \mathbb{N}$ set $q_n = dp^{n+1}$, $K_n = \mathbb{Q}(\zeta_{q_n})$ and $\Gamma_n = \mathrm{Gal}\big(K_n/K_0\big)$ and $\Delta = \mathrm{Gal}\big(K_0/\mathbb{Q}\big)$. Since $K_0/\mathbb{Q}$ is tame at p the restriction map $\mathrm{Gal}\big(K_n/\mathbb{Q}\big) \longrightarrow \mathrm{Gal}\big(K_0/\mathbb{Q}\big)$

induce a canonical split exact sequence

$$1 \longrightarrow \mathrm{Gal}\big(K_n/K_0\big) \longrightarrow \mathrm{Gal}\big(K_n/\mathbb{Q}\big) \underset{i}{\rightleftarrows} \mathrm{Gal}\big(K_0/\mathbb{Q}\big) \longrightarrow 1\ ,$$

Hence we get a canonical isomorphism $\mathrm{Gal}\big(K_n/\mathbb{Q}\big) \cong \Gamma_n \times \Delta$, which fits in the diagram:

$$\begin{array}{ccc} \mathrm{Gal}\big(K_n/\mathbb{Q}\big) & \xrightarrow{\ \cong\ } & \Gamma_n \times \Delta \\ \sigma_n \uparrow & & \uparrow \gamma_n \times \delta \\ \big(\mathbb{Z}/q_n\mathbb{Z}\big)^\times & \longrightarrow & \overline{U}_n \times \big(\mathbb{Z}/pd\mathbb{Z}\big)^\times \end{array} \tag{4.1}$$

where $\overline{U}_n = \big\{a \bmod q_n \mid a \equiv 1 \bmod pd\big\}$, $\gamma_n = \sigma_n|_{\overline{U}_n}$ and σ_n, δ are given by

$$\sigma_n(a) : \zeta_{q_n} \longmapsto \zeta_{q_n}^a \text{ and } \delta(b) : \zeta_{pd} \longmapsto \zeta_{pd}^b.$$

Let $K_\infty = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(\zeta_{q_n})$ and $\Gamma = \mathrm{Gal}\big(K_\infty/K_0\big)$. We have topological isomorphisms:

$$\Gamma = \varprojlim \Gamma_n \cong \varprojlim \overline{U}_n \cong 1 + pq\mathbb{Z}_p = (1+pd)^{\mathbb{Z}_p}.$$

Let $\gamma : (1+pd)^{\mathbb{Z}_p} \longrightarrow \Gamma$ such isomorphism, then it is totaly characterize by its action

$$\gamma(a) : \zeta_{q_n} \longrightarrow \zeta_{q_n}^{a \bmod q_n\mathbb{Z}}.$$

From diagram (4.1) we get

$$\begin{array}{ccc} \mathrm{Gal}\big(K_\infty/\mathbb{Q}\big) & \xrightarrow{\ \cong\ } & \Gamma \times \Delta \\ \sigma \uparrow & & \uparrow \gamma \times \delta \\ \mathbb{Z}_p^\times & \longrightarrow & (1+pd\mathbb{Z}_p) \times \big(\mathbb{Z}/pd\mathbb{Z}\big)^\times \end{array}$$

Note that $\gamma_0 = \gamma(1+pd)$ is a topological generator of Γ i.e. $\Gamma = \gamma_0^{\mathbb{Z}_p}$.

Lemma 4.3.1 *The Groups* $\mathrm{Gal}\big(K_\infty/K_n\big) = \Gamma^{p^n} = \gamma_0^{p^n\mathbb{Z}_p}$ *and* $\Gamma_n = \langle\, \gamma_n(1+pd)\,\rangle$.

Proof. Note that $\mathrm{Gal}\big(K_\infty/K_n\big)$ has index p^n in Γ. Since the only subgroup of index p^n of $\mathbb{Z}_p$ is $p^n\mathbb{Z}_p$, then the corresponding subgroup of Γ must be Γ^{p^n}, hence

$$\mathrm{Gal}\big(K_n/K_0\big) = \Gamma^{p^n} = \gamma_0^{p^n\mathbb{Z}_p}.$$

Now, canonically $\Gamma_n \cong \Gamma/\Gamma^{p^n} = \langle\, \gamma_0\Gamma^{p^n}\,\rangle$, therefore $\Gamma_n = \langle\, \gamma_n(1+pd)\,\rangle$. □

For F a finite extension of $\mathbb{Q}_p$, consider the group algebras $\mathcal{O}_F[\Gamma_n]$ with the topology induced by $\mathcal{O}_F$. Note that the canonical homomorphisms $\{\Gamma_n \longrightarrow \Gamma_m\}_{m\le n}$ induce an inverse system of topological algebras $\big\{\mathcal{O}_F[\Gamma_n] \longrightarrow \mathcal{O}_F[\Gamma_m]\big\}_{m\le n}$.

Definition 4.3.1 *We define $\mathcal{O}_F[[\Gamma]]$ as the topological $\mathcal{O}_F$-algebra $\varprojlim \mathcal{O}_F[\Gamma_n]$.*

Clearly the morphisms $\mathcal{O}_F[\Gamma] \longrightarrow \mathcal{O}_F[\Gamma_n]$ induced by the canonical projections are coherent with the inverse system, therefore we get a canonical morphism

$$\mathcal{O}_F[\Gamma] \longrightarrow \mathcal{O}_F[[\Gamma]].$$

By the same argument that we will use in Lemma 6.3.1 we have that last morphism is a dense immersion therefore we may consider $\mathcal{O}_F[\Gamma]$ as a dense subgroup of $\mathcal{O}_F[[\Gamma]]$ doing the identification:

$$\gamma(a) \leftrightarrows \big(\gamma_n(a \bmod p^n)\big)_{n\in\mathbb{N}}.$$

Theorem 4.3.1 *There exists a unique isomorphism of compact $\mathcal{O}_F$-algebras*

$$\mathcal{O}_F[[T]] \cong \mathcal{O}_F[[\Gamma]],$$

such that the isomorphism sends $1+T \longmapsto \gamma_0 = \gamma(1+pd)$.

Proof. Consider the algebra-morphism $\mathcal{O}_F[T] \longrightarrow \mathcal{O}_F[\Gamma_n]$ given by $1+T \longmapsto \gamma_n(1+pd)$. By Lemma 4.3.1 they are surjective and $\gamma_n(1+pd)$ has order p^n in Γ_n, hence monic polynomial $[\,p^n\,] = (1+T)^{p^n} - 1$ is in the kernel and has minimal degree, therefore it is a generator of such kernel and we get an isomorphism

$$\theta_n : \mathcal{O}_F[T]/[\,p\,] \xrightarrow{\cong} \mathcal{O}_F[\Gamma_n].$$

Such isomorphisms are clearly compatible with corresponding inverse systems, then they induce an isomorphism

$$\varprojlim \mathcal{O}_F[T]/[\,p\,] \xrightarrow{\cong} \varprojlim \mathcal{O}_F[\Gamma_n].$$

which sends $\big(1+T \bmod [\,p^n\,]\big)_{n\in\mathbb{N}} \longmapsto \big(\gamma_n(1+pd)\big)$ therefore by Theorem 4.3.1

$$\mathcal{O}_F[[T]] \cong \varprojlim \mathcal{O}_F[T]/[\,p^n\,] \cong \varprojlim \mathcal{O}_F[\Gamma_n] = \mathcal{O}_F[[\Gamma]],$$

and the resulting isomorphism sends $1+T \longmapsto \gamma(1+pd)$. $\square$

4.4 p-adic L-Functions: Iwasawa's Approach

Let p be an odd prime and d an integer prime to p such that $d \neq 2 \bmod 4$. In this section we will continue with the notation: $q_n = p^{n+1}d$, $K_n = \mathbb{Q}(\zeta_{q_n})$, $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$ and the groups $G = \mathrm{Gal}\big(K_\infty/\mathbb{Q}\big)$, $G_n = \mathrm{Gal}\big(K_n/K_0\big)$, $\Gamma = \mathrm{Gal}\big(K_\infty/K_0\big)$, $\Gamma_n = \mathrm{Gal}\big(K_n/K_0\big)$, $\Delta = \mathrm{Gal}\big(K_0/\mathbb{Q}\big)$. We let σ_a, for a prime to q_0, denote the element in $\mathrm{Gal}\big(K_\infty/\mathbb{Q}\big)$ which sends each $\zeta_{q_m} \longmapsto \zeta_{q_m}^a$ as well as its restrictions in $\mathrm{Gal}\big(K_n/\mathbb{Q}\big)$.

Definition 4.4.1 (Stickelberger Element) *The Stickelberger element θ_n is defined as*

$$\xi_n = \frac{1}{q_n} \sum_{\substack{a=1,\\(a,q_0)=1}}^{q_n} a\,\sigma_a^{-1}|_{K_n} = \sum_{a \in W_n} \left\{\frac{a}{q_n}\right\} \sigma_a^{-1}|_{K_n} \in \mathbb{Q}_p[G_n], \tag{4.2}$$

where $W_n \subseteq \mathbb{Z}$ is any set of representative of $\big(\mathbb{Z}/q_n\mathbb{Z}\big)^\times$.

Now consider the inverse system of algebras $\{\mathbb{Q}_p[G_n] \longrightarrow \mathbb{Q}_p[G_m]\}_{m \le n}$ where the maps are the induced by the respective restrictions.
Corresponding to the decomposition $\mathrm{Gal}\big(K_n/\mathbb{Q}\big) \cong \Gamma_n \times \Delta$, we write:

$$\sigma_a = \delta(a)\gamma_n(a), \text{ with } \delta(a) \in \Delta, \gamma_n(a) \in \Gamma_n.$$

We will use the same notation σ_a indistinctly as an element of $\mathrm{Gal}\big(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}\big)$ as well as its canonical image in $\mathrm{Gal}\big(K_\infty/\mathbb{Q}(\zeta_f)\big)$.
It is well known [Was97, pp. 93] that for c prime to q_n we have

$$(1 - c\sigma_c^{-1})\theta_n \in \mathbb{Z}_p[\mathrm{Gal}\big(K_n/\mathbb{Q}\big)].$$

An adaptation of the same argument gives as:

Lemma 4.4.1 *Let c prime to q_0. We have that,*

$$\eta_n = -(1 - c\gamma_n(c)^{-1})\xi_n \in \mathbb{Z}_p[\Delta \times \Gamma_n].$$

Proof. With the previous notation,

$$\xi_n = \frac{1}{q_n} \sum_{\substack{a=1,\\(a,q_0)=1}}^{q_n} a\,\delta(a)^{-1}\gamma_n(a)^{-1}. \tag{4.3}$$

Since c is prime to q_0 we may consider in the sum (4.3) the change of summing index $a \equiv bc \bmod q_n$, then $\dfrac{a}{q_n} = \left\{\dfrac{bc}{q_n}\right\}$ and $\delta(a) = \delta(b)$, hence

$$\xi_n = \sum_{\substack{b=1,\\(b,q_0)=1}}^{q_n} \left\{\frac{bc}{q_n}\right\} \delta(bc)^{-1}\gamma_n(bc)^{-1} = \sum_{\substack{b=1,\\(b,q_0)=1}}^{q_n} \left\{\frac{bc}{q_n}\right\} \delta(b)^{-1}\gamma_n(b)^{-1}\gamma_n(c)^{-1}.$$

Then:

$$\eta_n = -\sum_{\substack{a=1,\\(a,q_0)=1}}^{q_n} \left(\left\{\frac{ac}{q_n}\right\} - c\left\{\frac{a}{q_n}\right\}\right)\delta(a)^{-1}\gamma_n(a)^{-1}\gamma_n(c)^{-1} \in \mathbb{Z}_p[\Delta \times \Gamma_n],$$

since: $\left\{\dfrac{ac}{q_n}\right\} + \left[\dfrac{ac}{q_n}\right] = \dfrac{ac}{q_n} = c\left\{\dfrac{a}{q_n}\right\} + c\left[\dfrac{a}{q_n}\right].$ □

Let us fix $c_0 = 1 + pd$ and $\theta^* = \omega\theta^{-1}$. Consider the idempotent:

$$\varepsilon_{\theta^*} = \frac{1}{|\Delta|}\sum_{\delta\in\Delta}\theta^*(\delta)\delta^{-1} \in K_\theta[\Delta]$$

where $K_\theta = \mathbb{Q}_p(\theta)$ Let us define

$$\begin{aligned}
\xi_n(\theta) &= -\frac{1}{q_n}\sum_{\substack{a=1,\\(a,q_0)=1}}^{q_n} a\,\theta\omega^{-1}(a)^{-1}\gamma_n(a)^{-1},\\
\eta_n(\theta) &= \sum_{\substack{a=1,\\(a,q_0)=1}}^{q_n}\left(c_0\left\{\frac{a}{q_n}\right\} - \left\{\frac{ac_0}{q_n}\right\}\right)\theta\omega^{-1}(a)\gamma_n(a)^{-1}\gamma_n(c_0)^{-1} \in \mathcal{O}_\theta[\Gamma_n].
\end{aligned}$$

By definition, $\varepsilon_{\theta^*}\xi_n = \xi_n(\theta)\varepsilon_{\theta^*}$ and $\varepsilon_{\theta^*}\eta_n = \eta_n(\theta)\varepsilon_{\theta^*}$.

In [Was97, pp.119] is proven that or $m \geq n$, the restriction map $K_\theta[\Gamma_m] \longrightarrow K_\theta[\Gamma_n]$ sends

$$\xi(\theta)_n \longmapsto \xi_m(\theta) \text{ and } \eta_n(\theta) \longmapsto \eta_m(\theta).$$

Since both sequences are coherent and, by Theorem (4.3.1), we are able to associate them power series:

$$\begin{aligned}
\big(\xi_n(\theta)\big)_{n\in\mathbb{N}} &\longmapsto f(T,\theta) \text{ for } \theta \neq 1,\\
\big(\eta_n(\theta)\big)_{n\in\mathbb{N}} &\longmapsto g(T,\theta),\\
\big(1 - c_0\gamma_n(c_0)^{-1}\big)_{n\in\mathbb{N}} &\longmapsto h(T,\theta).
\end{aligned}$$

Theorem 4.4.1 *Let $\chi = \theta\psi$ an even Dirichlet character with θ of first kind and ψ of second kind, and let $\zeta_\psi = \psi(c_0)^{-1} = \chi(1+q_0)^{-1}$, then*

$$L_p(s,\chi) = f(\zeta_\psi(1+q_0)^s - 1, \theta).$$

Proof. See [Was97, pp.123]. □

Chapter 5

The Compact-open Topology

5.1 Zeros of Power Series and the p-adic Maximum Principle

In this section K is a complete extension of $\mathbb{Q}_p$ in $\mathbb{C}_p$ and $f = \sum a_n T^n \in K[[T]]$ convergent for $|\zeta| < R$. Since for $|\zeta| < R$, $|a_n \zeta^n| \longrightarrow 0$, then $\sup_{n\in\mathbb{N}} |a_n\zeta^n|$ is really a maximum and

$$|f(\zeta)| \leq \max_{n\in\mathbb{N}} |a_n\zeta^n|.$$

Definition 5.1.1 1. *For $0 \leq r < R$ we define $M_f(r) = \max_{n\in\mathbb{N}} |a_n|r^n$ and the* **growth function** *associated to f, $M_f : r \longmapsto M_f(r)$.*

2. *$r < R$, is called* **regular** *if $M_f(r) = |a_m|r^m$ for only one $m \in \mathbb{N}$ and it is called* **critical** *if its not regular.*

3. *For each $r < R$ the coefficients a_m such that $M_f(r) = |a_m|r^m$ are called* **dominant** *for the radius r.*

4. *For f with $R > 1$ we define the extreme indexes of f as*

$$\lambda(f) = \min\{n \in \mathbb{N} \,|\, |a_n| = M_f(1)\} \text{ and } \nu(f) = \max\{n \in \mathbb{N} \,|\, |a_n| = M_f(1)\}.$$

In the following let us denote for $r \in |\mathbb{C}_p|$, S_r and B_r the sets of $\zeta \in \mathbb{C}_p$ such that $|\zeta| = r$ and $|\zeta| < r$ respectively.

Remark 5.1.1

1. *The growth function is always non decreasing.*

2. *For a series convergent for $|\zeta| \leq 1$, $M_f(1) = \sup_{n\in\mathbb{N}} |a_n| = \|f\|$ (as in the first chapter).*

3. *For $|\zeta| = r$, $|f(\zeta)| \leq M_f(r)$ and the equality $|f(\zeta)| = M_f(r)$ holds for any regular radii, hence the zeros of f lie on the critical radii.*

4. *The condition $R > 1$ guaranties that the extreme indexes are finite hence we can define the number $\Delta(f) = \nu(f) - \lambda(f)$.*

5. *$M_f(1) \leq 1$ if and only if $f \in \mathcal{O}_K[[T]]$ and $\|f\| < 1$ if and only if $f \in \mathfrak{p}_K[[T]]$. Further if $f \in \mathcal{O}_K[[T]]$ with $R > 1$ and $\|f\| = 1$ the extreme indexes has the following interpretation: If $\widetilde{f} = f \bmod \mathfrak{p}$, then $\widetilde{f} \in \kappa[T]$ and the extreme indexes are $\lambda(f) = \mathrm{ord}_0(\widetilde{f})$, $\nu(f) = \deg(\widetilde{f})$.*

Lemma 5.1.1 *Let $f = \sum a_n T^n \in K[[T]]$. Then critical radii from a discrete sequence $0 \leq r_1 < r_2 < \ldots < R$.*

Proof. Let $0 < r < R$, since $|a_n|r^n \longrightarrow 0$ there is $N \in \mathbb{N}$ such that for $n > N$, $|a_n|r^n < M_f(r)/2$. So there must be a $m \leq N$ such that $M_f(r) = |a_m|r^m$. Now for $n > N$ and $0 < s < r$, we have:

$$|a_n|r^n \leq |a_m|r^m \Longrightarrow s^{n-m} < r^{n-m} \leq |a_m|/|a_n| \Longrightarrow |a_n|s^n < |a_m|s^m.$$

Then if $s < r$ is critical radius must satisfy $|a_i|s^i = M_s(f) = |a_j|s^j$ for $1 \leq i < j \leq N$ i.e. it must satisfy one of the equations $s^{j-i} = |a_i|/|a_j|$, $0 \leq i < j \leq N$ so there are only finitely many choices for s. □

Let $r < R$ and consider $f_r(T) = f(rT)$ then f_r is convergent for $|\zeta| < R/r$. Since $1 < R/r$ we can define $\lambda_r(f) = \lambda(f_r)$, $\nu_r(f) = \nu(f_r)$ then

$$\lambda_r(f) = \min\{n \in \mathbb{N} \,|\, |a_n|r^n = M_f(r)\},$$
$$\nu_r(f) = \max\{n \in \mathbb{N} \,|\, |a_n|r^n = M_f(r)\}.$$

Let us fix $f = \sum a_n T^n \in K[[T]]$ and denote $\lambda_r(f) = \lambda_r$ and $\nu_r(f) = \nu_r$.

Lemma 5.1.2 *If $r < t$ are two consecutive critical radii and $r < s < t$ then*

$$\nu_r = \lambda_s = \nu_s = \lambda_t.$$

Proof. Let $N \in \mathbb{N}$ be such that for any $n \geq N$, $|a_n|t^n < M_f(r)$. Then for $r \leq s \leq t$ and $n \geq N$, $|a_n|s^n < M_f(r)(s/t)^n < M_f(s)$. This means that for each radius in $]r, t[$ the dominant terms always have indexes less or equal to N. Consider the dominant term $|a_m|s^m = M_f(s)$ i.e. for $m \neq n \leq N$ $|a_n|s^n < |a_m|s^m$. By continuity there is a $\varepsilon > 0$ such that for $m \neq n \leq N$ and $|s - t| < \varepsilon$ we have $|a_n|t^n < |a_m|t^m$. Now for each $n \in \mathbb{N}$ set

$$A_n = \{s \in]r, t[\,|\, a_m \text{ is dominant for the radius } s\} \subseteq]r, t[,$$

by the previous these sets are open and $]r,t[=\bigcup_{n\in\mathbb{N}} A_n$. In particular the complement of A_m is also therefore, and since $]r,t[$ is connected, $A_m =]r,t[$ i.e. all the radii $s \in]r,t[$ have the same dominant term. Finally, note that for $m < n \leq N$ and $s \in]r,r'[$ we have

$$|a_n|r^n = |a_n|s^n(r/s)^n < |a_m|s^m(r/s)^n < |a_m|r^m(r/s)^{n-m},$$

hence $m = \nu_r$. An analogous argument shows that $m = \lambda_t$. □

Let $0 \leq r_0 < r_1 < r_2 < \ldots \leq R$ be a increasing sequence stoping at some N with $r_N = 1$ or infinite such that $\lim r_n = R$. For such sequences we have:

Proposition 5.1.1 *Let $\rho : [0,R[\longrightarrow \mathbb{R}$ continuous function such that all its restrictions $\rho_n = \rho|_{[r_n,r_{n+1}]}$ are convex and continuously differentiable in their respective domains. If for all $n \in \mathbb{N}$ we have that $\rho'_-(r_n) \leq \rho'_+(r_n)$ then ρ is convex.*

Proof. Let $g : [0,R[\longrightarrow \mathbb{R}$ defined as

$$g(t) = \begin{cases} \rho'(t) & \text{if } t \neq r_n \text{ for all } n \in \mathbb{N}, \\ \rho'_-(r_n) & \text{if } t = r_n \text{ for some } n \in \mathbb{N}. \end{cases}$$

By definition g is increasing and for each $x \in [0,R[$, the function g only has finitely many discontinuities in $[0,x]$ and $\rho = \displaystyle\int_0^x g(t)dt$. Fix $x_0, x_1 \in [0,R]$ with $x_0 < x_1$ and $t \in (0,1)$. With these constants consider $y : [x_0,x_1] \longrightarrow [x_0,x_1]$ defined as $y(s) = x_0 + t(s - x_0)$. We must show that:

$$\rho(y(x_1)) \leq \rho(x_0) + t(\rho(x_1) - \rho(x_0)). \tag{5.1}$$

Note that $y(x_0) = x_0$, $y(s) < s$ and $y' = t$. Inequality (5.1) is equivalent to the following:

$$\int_{y(x_0)}^{y(x_1)} g(s)ds \leq t \int_{x_0}^{x_1} g(s)ds. \tag{5.2}$$

Let $w : [y(x_0), y(x_1)] \longrightarrow [x_0,x_1]$ be the inverse function of y and $\widetilde{g} = g \circ y$, then

$$\frac{1}{t}\int_{y(x_0)}^{y(x_1)} g(s)ds = \int_{y(x_0)}^{y(x_1)} \widetilde{g}(w(s))w'ds = \int_{x_0}^{x_1} \widetilde{g}(\eta)d\eta.$$

Since g is increasing, for each $s \in [0,1]$ we have that $\widetilde{g}(s) = g(y(s)) \leq g(s)$ i.e. $\widetilde{g} \leq g$. Therefore comparing the integrals of g and $\widetilde{g}$ we obtain (5.2). □

Corollary 5.1.1 *The function $M_f : [0,R[\longrightarrow \mathbb{R}$ is continuously convex and smooth expect at the critical radii.*

Proof. Let $\rho = M_f$, $r_1 < r < r_2$ consecutive critical radii and $m = \lambda_r < n = \nu_r$. Since r is critical we have $\rho(r) = |a_m|r^m = |a_n|r^n$. By the last lemma for $s \in]r_1, r[$ and $t \in (r, r_2)$ we get $\rho(s) = |a_m|s^m$ and $\rho(t) = |a_n|t^n$. Since a_m and a_n are dominant coefficients for the radius r, M_f is continuous in $]r_1, r_2[$. Clearly the f is smooth in $]s, r[$, $]r, t[$ and looking at the derivatives at s, t we have

$$\rho'_-(r) = m|a_m|r^{m-1} \leq n|a_n|r^{n-1} = \rho'_+(r), \tag{5.3}$$

therefore by Proposition 5.1.1 ρ is convex. □

Lemma 5.1.3 *Let $g = \sum b_n T^n \in \mathcal{O}_K[[T]]$. Then g has exactly $\lambda = \lambda(g)$ zeros in B_1, counting multiplicities.*

Proof. Without loss of generality we may take $g/\|g\|$ instead of g in order to get $\|g\| = 1$. By the preparation theorem (theorem 4.2.1) there exists $P \in \mathcal{O}_K[T]$ distinguished of degree λ and a unit $u = \sum u_n T^n$ such that $g = P(T)u(T)$. By part 2 of Remark 4.2.1 g and P share the same zeros in B_1 (with the same multiplicities). Now, P have λ zeros in $\mathbb{C}_p$ (counting multiplicities) and since it is distinguished $P = T^\lambda + \sum_{i<\lambda} c_i T^i$ with $|c_i| < 1$. For each zero ζ of P we have that:

$$|\zeta|^\lambda = \big|\sum_{i<\lambda} c_i \zeta^i\big| \leq \max_{i<\lambda} |c_i||\zeta|^i < \max_{i<\lambda} |\zeta|^i,$$

but it happens if and only if $|\zeta| < 1$ (because for $|\zeta| \geq 1$, $|\zeta|^\lambda \geq |\zeta|^i$ for $\lambda \geq i$). Therefore P, as well as f, has λ zeros in B_1. □

Corollary 5.1.2 *For $|\zeta| < R$ and $r < R$, f has exactly λ_r zeros in the ball B_r.*

Proof. Taking $g(T) = f(rT)$, it converges for $|\zeta| < R/r$. Since $1 < R/r$ the coefficients of g are bounded so we can assume $g \in \mathcal{O}_K[[T]]$ then the result follows from the previous, since by definition $\lambda_r(f) = \lambda(g)$. □

Theorem 5.1.1 (Zeros in critical radius) *If $r < R$ is a critical radius of f then f has exactly $\nu_r - \lambda_r$ zeros in the sphere $|\zeta| = r$.*

Proof. Let $r < R$ be a critical radius and $r < t < R$ be the next one. By the corollary f has exactly λ_r and λ_t zeros at the balls B_r and B_t respectively. Since the radii $s \in]r, t[$ are all regular, f must have $\lambda_t - \lambda_r$ zeros in the sphere $|\zeta| = r$, and by Lemma 5.1.2 $\lambda_t = \nu_r$ therefore f has exactly $\nu_r - \lambda_r$ zeros in S_r. □

Corollary 5.1.3 *Let $r < R$ be critical and $\xi \in \mathbb{C}_p$ satisfying one of the following conditions: (i) $|\xi| < M_f(r)$. (ii) $|\xi| = M_f(r)$ and $|\xi - f(0)| = M_f(r)$.*
Then there exists $\zeta \in S_r$ such that $f(\zeta) = \xi$.

Proof. Let $h = \sum_{n\geq 1} a_n T^n$ and $g = f - \xi = (f(0) - \xi) + h$. Note that f takes the value ξ in S_r if and only if g has a zero in it too. By last theorem it happens when r is critical with respect to g i.e. when g has more that one dominant term for such radius. Since r is critical with respect to f we have that $M_h(r) = M_f(r)$ then

$$M_h(r) \leq M_g(r) = \max\{|f(0) - \xi|, M_h(r)\}.$$

Now, conditions (i) and (ii) imply that $|f(0) - \xi| \leq M_f(r)$, therefore

$$M_g(r) = M_h(r) = M_f(r).$$

Last equality implies that f and g will share the same dominant terms of positive degree. If the constant term of f is not dominant then f must have at least two dominant terms of higher degree then so does g; If not we must have $|f(0)| = M_f(r)$ and f must have at least another dominant term wish shares with h and g, hence in both cases the constant term of g is dominant and shares the other dominant terms of f. □

Corollary 5.1.4 *Let r is a critical radius of f. For every $t \in \mathbb{R}$ such that $t = |\xi| \leq M_r(f)$ for some $\xi \in \mathbb{C}_p$, there exists $\zeta \in S_r$ such that $|f(\zeta)| = t$.*

Proof. If $t = 0$ it is just last theorem. If $t > 0$ then $t \in p^{\mathbb{Q}} \cap]0, M_r(f)]$, so choose $\xi \in S_t$ according the following cases:

1. If $t < M_f(r)$: Take any $\xi \in S_t$, trivially we get $|\xi| < M_f(r)$.
2. If $|a_0| < t = M_f(r)$: Take any $\xi \in S_t$, we always get $|\xi - a_0| = M_f(r)$.
3. If $|a_0| = t = M_f(r)$: Take $\xi = -a_0$, then we have that $|\xi - a_0| = |2||a_0| = M_f(r)$.

In each case the ξ chosen fulfills the conditions of Corollary 5.1.3 therefore there exists $\zeta \in S_r$ such that $|f(\zeta)| = |\xi| = t$. □

Theorem 5.1.2 (The Maximum Principle) *Let $r < R$, $r \in p^{\mathbb{Q}}$ then*

$$M_f(r) = \sup_{|\zeta|<r} |f(\zeta)| = \sup_{|\zeta|\leq r} |f(\zeta)| = \max_{|\zeta|=r} |f(\zeta)|.$$

Proof. Let $|\zeta| \leq r$, then $|f(\zeta)| \leq M_f(|\zeta|) \leq M_f(r)$ which implies

$$\sup_{|\zeta|<r} |f(\zeta)| \leq \sup_{|\zeta|\leq r} |f(\zeta)| \leq M_f(r).$$

Now fix $\zeta \in S_r$. We may choose a sequence $(\zeta_n)_{n\in\mathbb{N}} \subseteq B_r$ such that

(i) The sequence $r_n = |\zeta_n|$ is a decreasing sequence of regular radii.

(ii) $\lim\limits_{n\to\infty} \zeta_n = \zeta$.

By (ii) we get $\lim\limits_{n\to\infty} r_n = r$ and by regularity $|f(\zeta_n)| = M_f(r_n)$. As M_f is continuous (Corollary 5.1.1) we get

$$M_f(r) = \lim_{n\to\infty} M_f(r_n) = \lim_{n\to\infty} |f(\zeta_n)| \leq \sup_{|\zeta|<r} |f(\zeta)|.$$

Finally, if r is regular we have $|f(\zeta)| = M_f(r)$ for any $\zeta \in S_r$ and if it is critical, by Corollary 5.1.4 there exists $\zeta \in S_r$ such that $|f(\zeta)| = M_f(r)$. □

5.2 $K((T))_1$ and the compact-open Topology

Let $B' = \{\zeta \in \mathbb{C}_p \,|\, 0 < |\zeta| < 1\}$. Recall that $K((T))_1$ is the subring of $K((T))$ constituted by Laurent series of finite order pole that converge at every point of B'. Put

$$p^{\mathbb{Q}^-} := \{|\zeta| = p^{v(\zeta)} \mid \zeta \in B'\} = \{p^q \mid q \in \mathbb{Q} \text{ and } q < 0\}.$$

For $\varepsilon > 0$ and $0 < a < b$ consider the family $\mathcal{N}_K$ of sets

$$N(\varepsilon, a, b) = \big\{f \in K((T))_1 \mid \text{ for } a \leq |\zeta| \leq b,\, |f(\zeta)| < \varepsilon\big\}.$$

This family of sets satisfies the conditions of a system of neighborhoods of 0 therefore they allows to define a topology in $K((T))_1$. (see [Wil98]).

Definition 5.2.1 *We define the* **compact-open topology** *as the topology induced by the system $\mathcal{N}_K$ of neighborhoods of 0.*

Remark 5.2.1

1. *The compact-open topology has basis*

$$\{f + N(\varepsilon, a, b) \,|\, f \in K((T))_1, \varepsilon > 0 \text{ and } 0 < a < b < 1\}.$$

2. *The compact-open topology turns $K((T))_1$ into a topological ring.*

3. *The natural immersion of K into $K((T))_1$ is continuous.*

Lemma 5.2.1 *Let $f = \sum_{n\in\mathbb{Z}} a_n T^n \in K((T))_1$. For $r \in p^{\mathbb{Q}^-}$ let*

$$\|f\|_r = \sup_{|\zeta|=r} |f(\zeta)|.$$

1. *For* $r \in p^{\mathbb{Q}^-}$, $\|f\|_r = \sup_{n\in\mathbb{Z}} |a_n| r^n$.

2. *For* $0 < r' < r \in p^{\mathbb{Q}^-}$, $\sup_{r'\leq|\zeta|\leq r} |f(\zeta)| = \max\{\|f\|_{r'}, \|f\|_r\}$.

Proof. (1) Since $f \in K((T))_1$ for some $N \in \mathbb{N}$ we have $T^N f = \sum_{n\in\mathbb{N}} b_n T^n \in K[[T]]$ then $b_n = a_{n-N}$ and $r^N \|f\|_r = M_{T^N f}(r) = \sup_{n\in\mathbb{N}} |b_n| r^n$, hence

$$\|f\|_r = \sup_{n\in\mathbb{N}} |a_{n-N}| r^{n-N} = \sup_{n\in\mathbb{Z}} |a_n| r^n.$$

(2) Let $\rho : (0,1) \longrightarrow \mathbb{R}$ defined as $\rho(r) = \|f\|_r$. Let $g \in K[[T]]^\times$ such that $f = T^N g$ and $r_1 < r < r_2$ be consecutive critical radii of g. By definition there exists $c_1, c_2 > 0$ and $n_1 < n_2 \in \mathbb{Z}$ such that for every $s \in]r_1, r[$ we have $\rho(s) = c_1 s^{n_1}$ as for every $t \in]r, r_2[$ we have $\rho(t) = c_2 t^{n_2}$. Since r is critical $c_1 r^{n_1} = \rho(r) = c_2 r^{n_2}$, therefore

$$\rho'_-(r) = n_1 c_1 r^{n_1 - 1} \leq n_2 c_2 r^{n_2 - 1} = \rho'_+(r).$$

We have that ρ is convex because it satisfies the conditions of Proposition 5.1.1, in particular for every $s \in]r', r[$ we have $\|f\|_s \leq \max\{\|f\|_{r'}, \|f\|_r\}$ and it is equivalent to have $\sup_{r'\leq|\zeta|\leq r} |f(\zeta)| = \max\{\|f\|_{r'}, \|f\|_r\}$. □

Corollary 5.2.1 *1. For* $r \in p^{\mathbb{Q}^-}$ *and* $\varepsilon > 0$, *the sets*

$$V(r,\varepsilon) = \{f \in K((T))_1 \mid \textit{ For all } \zeta \in S_r \textit{ we have } |f(\zeta)| < \varepsilon\},$$

are open and constitute system of neighborhoods of 0 for the compact-open topology.

2. *The ring* $K((T))_1$ *with the compact-open topology is a second-countable topological ring i.e. every point admits a countable system of neighborhoods.*

3. *A sequence in* $K((T))_1$ *converges if and only if it converges uniformly in each sphere* S_r *with* $r \in p^{\mathbb{Q}^-}$.

Proof. (1) Clearly the sets $V(r,\varepsilon)$ are open and by part 2 of Lemma 5.2.1 $V(a,b,\varepsilon) = V(a,\varepsilon) \cap V(b,\varepsilon)$, hence any neighborhood of 0 must contain one of them.
(2) It follows from part 1 and the fact that $p^{\mathbb{Q}^-}$ is countable because $\{V(r,q) \mid r \in p^{\mathbb{Q}^-}$ with $q \in \mathbb{Q}^+\}$ gives a countable system of neighborhoods of 0.
(3) Since for a fixed $r \in p^{\mathbb{Q}^-}$ the family $\{V(r,\varepsilon) \mid \varepsilon > 0\}$ is a system of neighborhoods of 0 for the topology of uniform convergence on S_r, (3) follows directly from part (1).

Definition 5.2.2 *We define* $K[[T]]_1$ *as the ring* $K[[T]] \cap K((T))_1$ *endowed with the relative topology with respect to open-compact topology of* $K((T))_1$.

Theorem 5.2.1 *The compact-open topology turns $K[[T]]_1$ into a complete topological ring.*

Proof. The only non trivial part is the completeness. Let $(f_n)_{n\in\mathbb{N}} \subseteq K[[T]]_1$ be a Cauchy sequence, $f_n = \sum a_{n,k}T^k$. Fix $r \in p^{\mathbb{Q}^-}$ and pick $t > r$ also in $p^{\mathbb{Q}^-}$, then:

i) For $j \in \mathbb{N}$, $\|f_n - f_m\|_r = \sup |a_{n,k} - a_{m,k}|r^k \geq r^j|a_{n,j} - a_{m,j}|$ which means that each $(a_{n,j})_{n\in\mathbb{N}} \subseteq K$ is Cauchy. Since K is complete, it has a limit $a_j \in K$, so that we may consider a power series $f = \sum a_kT^k$.

ii) Since $(f_n)_{n\in\mathbb{N}}$ is Cauchy, $(\|f_n\|_t)_{n\in\mathbb{N}}$ is bounded, say by $C > 0$. Not that for all n and all j, $|a_{n,j}|t^j \leq \|f_n\|_t \leq C$, therefore $|a_j|t^j \leq C$ and this implies that $\lim\limits_{n\to\infty} |a_j|r^j = 0$ because
$$|a_j|r^j = |a_j|t^j\left(\frac{r}{t}\right)^j \leq C\left(\frac{r}{t}\right)^j.$$
Since $r \in p^{\mathbb{Q}^-}$ can be chosen arbitrarily we must have that $f \in K[[T]]_1$.

iii) For $\varepsilon > 0$, $N \in \mathbb{N}$ such that $n, m \geq N$, $\|f_n - f_m\|_r < \varepsilon$ and for any $k \in \mathbb{N}$ we have $|a_{n,k} - a_{m,k}|r^k \leq \|f_n - f_m\|_r < \varepsilon$ then fixing j and taking limit when n goes to infinity we get that for $m \geq N$, $|a_j - a_{mj}| \leq \varepsilon$ hence $\|f - f_m\|_r < \varepsilon$. Since $r \in p^{\mathbb{Q}^-}$ as well as $\varepsilon > 0$ are arbitrary, we get $\lim\limits_{n\to\infty} f_n = f$. □

Definition 5.2.3 *For $f \in K((T))_1$ we define V_f, the set of* **series dominated by** *f, as the set of $g \in K((T))_1$ such that $|g(\zeta)| \leq \|f\|_{|\zeta|}$ for all $\zeta \in B'$.*

Lemma 5.2.2 *1. For $f \in K((T))_1$ and $g \in V_f$, $\operatorname{ord} g \geq \operatorname{ord} f$.*

2. V_f is a complete subspace of $K((T))_1$.

3. For $r \in p^{\mathbb{Q}^-}$, if $\|f\|_r < \varepsilon$ then $V_f \subseteq V(r, \varepsilon)$.

4. For $\varepsilon > 0$ and $r \in p^{\mathbb{Q}^-}$ exists $N \in \mathbb{N}$ such that
$$V_f \cap T^N K[[T]]_1 \subseteq V(r, \varepsilon).$$

Proof. (1) Let $f = \sum_{n\geq -N} a_nT^n$ and $g = \sum b_nT^n \in V_f$. Since the critical radii of f are isolated we may find $r > 0$ such that every $s \in (0, r)$ is regular with respect to f, then $\lambda_s = \nu_s = k \geq -N$ for some fixed k. It will be enough to show that for $j < -N$ we have $b_j = 0$. For this note that for every $s \in]0, r[$, $|b_j|s^j \leq \|g\|_s \leq \|f\|_s = |a_k|s^k$ then $|b_j| \leq |a_k|s^{k-j}$. Then for any $j < k$, taking limit when s goes to 0, we get $b_j = 0$.
(2) Let $\operatorname{ord}(f) = N$ by the previous part, $V_f \subseteq T^N K[[T]]_1$ which is complete, then it is enough to show that V_f is closed. For this take $(g_n) \subseteq V_f$ converging to $g \in K((T))_1$ and pick any $r \in p^{\mathbb{Q}^-}$. Then for any $\zeta \in S_r$ we have $|g_n(\zeta)| \leq \|f\|_r$, therefore $|g(\zeta)| =$

$\lim_{n\to\infty} |g_n(\zeta)| \le \|f\|_r$. Since r is arbitrary we must have that $g \in V_f$.
(3) Taking $g \in V_f$ and any $|\zeta| = r$, $|g(\zeta)| \le \|f\|_r < \varepsilon$ then $g \in V(r,\varepsilon)$.
(4) Fix $s \in p^{\mathbb{Q}^-}$, $s > r$ and $R > \|f\|_s$ by part 2, $V_f \subseteq V(s,R)$ then

$$V_f \cap T^N K[[T]]_1 \subseteq V(s,R) \cap T^N K[[T]]_1 \subseteq V\big(r, R(r/s)^N\big). \tag{5.4}$$

For the second inclusion take $g \in V(s,R)$ such that $g = T^N h$ with $h \in K[[T]]_1$. Applying the maximum principle (Theorem 5.1.2) to h we get $\|g\|_r r^{-N} = \|h\|_r \le \|h\|_s = \|g\|s^{-N}$, then $\|g\|_r \le \|g\|_s (r/s)^N$. From (5.4) for a fixed N, as soon as it is big enough, we get $V_f \cap T^N K[[T]]_1 \subseteq V(r,\varepsilon)$. □

As in Definition 2.1.1 set the N-th truncation map $P_N : K((T))_1 \longrightarrow K((T))_1$ as

$$P_N\left(\sum_{n\in\mathbb{Z}} a_n T^n\right) = \sum_{n<N} a_n T^n,$$

Remark 5.2.2

1. *P_N is continuous, since for any $r \in p^{\mathbb{Q}^-}$ and $f = \sum a_n T^n \in K((T))_1$, by part 1 of Lemma 5.2.1 $\|P_N(f)\|_r = \sup_{n<N} |a_n| r^n \le \sup_{n\in\mathbb{Z}} |a_n| r^n = \|f\|_r$.*
2. *$P_N(V_f) \subseteq V_f$, since for $g \in V_f$ and $\zeta \in B'$ we have*

$$|P_N(g)(\zeta)| \le |g(\zeta)| \le \|f\|_{|\zeta|}.$$

The following proposition gives us a useful criterium for convergence in $K((T))_1$.

Proposition 5.2.1 *Let $g \in K((T))_1$ and $(g_n)_{n\in\mathbb{N}} \subseteq V_f$. Then (g_n) converges to g if and only if for all $N \in \mathbb{Z}$, $\big(P_N(g_n)\big)_{n\in\mathbb{N}}$ converges to $P_N(g)$.*

Proof. Since the truncations P_N are continuous, the sufficiency is clear. For the other implication, by linearity of P_N, it is enough to check the case $g = 0$. For this fix $\varepsilon > 0$ and $r \in p^{\mathbb{Q}^-}$. Since $g_n \in V_f$ then $g_n - P_N(g_n) \in V_f \cap T^N K[[T]]_1$. By part 4 of Lemma 5.2.2 for a fixed N, big enough, we have $g_n - P_N(g_n) \in V(r, \varepsilon/2)$. Now, since $\lim_{n\to\infty} P_N(g_n) = 0$, for n big enough we have that $P_N(g_n) \in V(r,\varepsilon/2)$, therefore $g_n \in V(r,\varepsilon)$. □

5.3 The Compact-Open topology in $\mathcal{O}_K[[T]]$

In $O_K[[T]]$ we can consider two topologies: the compact-open topology, as a subspace of $K[[T]]_1$ and the (p,T)-adic topology. The following theorem relates both topologies:

Theorem 5.3.1 *In $\mathcal{O}_K[[T]]$ the (p,T)-adic topology and the compact-open topology coincide. In particular $\mathcal{O}_K[[T]]$ is compact with respect to the compact-open topology.*

Proof. Since both topologies, the (p,T)-adic and compact-open are given by systems of neighborhoods of 0, $\{(p,T)^N \mid N \in \mathbb{N}\}$ and $\{V(r,\varepsilon) \cap \mathcal{O}_K[[T]] \mid r \in p^{\mathbb{Q}^-}, \varepsilon > 0\}$ respectively, it will be enough to prove the following claims:

Claim 1: For $\varepsilon > 0$ and $r \in p^{\mathbb{Q}^-}$ exists $N \in \mathbb{N}$ such that $(p,T)^N \subseteq V(r,\varepsilon)$.
Let $f \in (p,T)^N$. By definition $f = \sum_{k=0}^{N} g_n p^k T^{N-k}$ with $g_k \in \mathcal{O}_K[[T]]$, then for $\zeta \in S_r$

$$|f(\zeta)| \leq \max_{0 \leq k \leq N} |g_k(\zeta)| \frac{1}{p^k} r^{N-k} \leq \|g\|_r \max\left\{\frac{1}{p^N}, r^N\right\}.$$

Since $g \in \mathcal{O}_K[[T]]$ implies that $\|g\|_r \leq 1$, we have that $f_r \leq \max\{\frac{1}{p^N}, r^N\}$. Therefore taking N big enough we get $\|f\|_r < \varepsilon$.

Claim 2: For all $N \in \mathbb{N}$ we have $V(1/p, 1/p^N) \cap \mathcal{O}_K[[T]] \subseteq (p,T)^N$.
Let $f \in V(1/p, 1/p^N) \cap \mathcal{O}_K[[T]]$. Since $f \in \mathcal{O}_K[[T]]$ we have

$$f \equiv \sum_{k=0}^{N-1} a_k T^k \bmod (T,p)^N.$$

Now, since $\|f\|_{1/p} < \frac{1}{p^N}$ for $k < N$ we have that $|a_k/p^{N-k}| < 1$. In particular $a_k = \alpha_k p^{N-k}$ for some $\alpha_k \in \mathcal{O}_K$. Therefore for $k < N$ we have $a_k T^k = \alpha_k p^{N-k} T^k \in (p,T)^N$, so $f \in (p,T)^N$. □

As in the end of Section 4.2, set $[\,p^n\,] = (1+T)^{p^n} - 1$.

Definition 5.3.1 *For $m \in \mathbb{N}$ we define Ω_m as the set of roots of $[p^{m+1}]$ in $\mathbb{C}_p$ and $\Omega'_m = \Omega_m \setminus \{0\}$. Also we define $\Omega = \bigcup_{m \in \mathbb{N}} \Omega_m$ and $\Omega' = \Omega \setminus \{0\}$.*

Remark 5.3.1

1. *Each $\Omega_m = \{\zeta^a_{p^{m+1}} - 1 \mid 0 \leq a < p^{m+1}\}$ and $\Omega_1 \subseteq \Omega_2 \subseteq \Omega_3 \subseteq \ldots \subseteq \Omega$.*

2. $\prod_{u \in \Omega'} u = \prod_{n=1}^{\infty} \prod_{\substack{(a,p)=1,\\ a \leq p^{n+1}}} (\zeta^a_{p^n} - 1) = 0$. *Indeed let $\Phi_n \in \mathbb{Z}[T]$ be the p^nth-cyclotomic polynomial i.e. $\Phi_{n+1}(T) = \prod_{\substack{(a,p)=1,\\ a \leq p^{n+1}}} (T - \zeta^a_{p^{n+1}})$. Since for $n \geq 1$, $\Phi_{n+1}(T) = \Phi_n(T^p)$ we have $\prod_{\substack{(a,p)=1,\\ a \leq p^{n+1}}} (\zeta^a_{p^n} - 1) = \Phi_{p^{n+1}}(1) = p$, which implies that $\prod_{u \in \Omega'} u = 0$.*

3. *Each* $f \in K[T]/[p^{m+1}]$ *induces a well defined map* $f : \Omega_m \longrightarrow \mathcal{O}_K$*, so for such* f*'s we may define a norm* $\|f\|_m = \sup_{u \in \Omega_m} |f(u)|$.

4. *Let* $(f_n)_{n\in\mathbb{N}}$ *and* f *be in* $K[T]/[p^{m+1}]$*. Since* Ω_m *is finite we get:* $(f_n)_{n\in\mathbb{N}}$ *converges to* f *with respect to* $\| \, \|_m$ *if and only if for all* $u \in \Omega_m$, $\big(f_n(u)\big)_{n\in\mathbb{N}}$ *converges to* $f(u)$.

5. *For* $f = \sum a_k T^k \in K[T]/[p^{m+1}]$*, we may consider the norm* $\|f\|_K = \sup_{0 \le k < p^{m+1}} |a_k|$ *which is well defined by the uniqueness of the Euclidean division in* $K[T]$.

6. $K[T]/[p^{m+1}]$ *with respect* $\| \, \|_K$ *is homeomorphic to* $K^{p^{m+1}}$ *via the following map*

$$\begin{array}{ccc} K^{p^{m+1}} & \longrightarrow & K[T]/[p^{m+1}] \\ (a_0, a_1, \dots) & \longmapsto & a_0 + a_1 T + \dots \end{array} \tag{5.5}$$

7. $\| \, \|_K$ *and* $\| \, \|_m$ *are equivalent since* K *is complete and* $K[T]/[p^{m+1}]$ *is a finite dimensional* K *vector space [Neu99, p.132], therefore they induce the same topology.*

8. *The map (5.5) sends* $\mathcal{O}_K^{p^{m+1}}$ *to* $\mathcal{O}_K[T]/[p^{m+1}]$*. In particular* $\mathcal{O}_K[T]/[p^{m+1}]$ *is compact with respect the* $\| \, \|_m$ *topology.*

Consider the canonical commutative diagram:

$$\begin{array}{ccc} \mathcal{O}_K[[T]] & \xrightarrow{\ \varphi\ } & \varprojlim \mathcal{O}_K[T]/[p^{n+1}] \\ & \overset{\varphi_n}{\searrow} & \big\downarrow \pi_n \\ & & \mathcal{O}_K[T]/[p^{m+1}] \end{array}$$

Theorem 5.3.2 (Convergence Criterium) *Let* $f_n, f \in \mathcal{O}_K[[T]]$*. Then:*
$(f_n)_{n\in\mathbb{N}}$ *converges to* f *if and only if for all* $u \in \Omega'$, $\big(f_n(u)\big)_{n\in\mathbb{N}}$ *converges to* $f(u)$.

Proof. The first implication is clear. For the converse, note that by Remark 5.3.1 the hypothesis implies that for each $m \ge N$, $\lim_{n\to\infty} \varphi_m(f_n) = \varphi_m(f)$ and since $\varphi_m = \pi_m \varphi$,

$$\lim_{n\to\infty} \pi_m\big(\varphi(f_n)\big) = \pi_m\big(\varphi(f)\big).$$

But by definition of the product topology this implies that $\lim_{n\to\infty} \varphi(f_n) = \varphi(f)$ then the conclusion follows from the continuity of φ^{-1}. □

Remark 5.3.2
If $\lim_{n\to\infty} g_n = g$ *in* $\varprojlim \mathcal{O}_K[T]/[p^{n+1}]$*, taking* $f_n = \varphi^{-1}(g_n), f = \varphi^{-1}(g)$ *and* $u \in \Omega'$ *we have*

$$f_n(u) = \varphi_m(f_n)(u) = \pi_m(g_n)(u) \longrightarrow \pi_m(g)(u) = \varphi_m(f)(u) = f(u).$$

Therefore the last convergence criterium is equivalent the continuity of the inverse of the map

$$\mathcal{O}_K[[T]] \xrightarrow{\varphi} \varprojlim \mathcal{O}_K[T]/[p^{n+1}].$$

Definition 5.3.2 *A testing sequence is a sequence $(a_i)_{i\in\mathbb{N}} \subseteq B'$ with all its terms different such that for any sequence $(g_n)_{n\in\mathbb{N}} \subseteq \mathcal{O}_K[[T]]$ we have that $\lim_{n\to\infty} g_n = 0$ if and only if for all $i \in \mathbb{N}$, $\lim_{n\to\infty} g_n(a_i) = 0$.*

Theorem 5.3.2 says that Ω' is a testing sequence, the following result from [Col79] characterizes such sequences.

Theorem 5.3.3 *Let $(a_i)_{i\in\mathbb{N}} \subseteq B'$. (a_i) is a testing sequence if and only if $\lim_{m\to\infty} \prod_{i=1}^{m} a_i = 0$.*

Proof. Suppose that (g_n) does not converge to zero. We claim that without loss of generality exists a $\delta > 0$ such that $|g_n(0)| > \delta$ for all $n \geq 1$. Indeed, since $g_n \in \mathcal{O}_K[[T]]$ there must be a $k \in \mathbb{N}$ such that the k-th coefficients of g_n does not converges to 0 i.e. if we define $h_n = T^{-k}(g_n - P_k(g_n))$ has a subsequence such that $|h_n(0)| > \delta$ for some $\delta > 0$ as we claimed, and if for any $a \in B'$ such that $g_n(a) \longrightarrow 0$, $h_n(a) \longrightarrow 0$. Now set $A_1 = |a_1|$ and for $m \geq 1$ $A_m = \prod_{i=1}^{m} |a_i| \prod_{j<i}^{m} |a_i - a_j|$ The lemma will follow from the following assertion:

Claim: Let $f = \sum b_j T^j \in \mathcal{O}_K[[T]]$. If $|f(a_i)| < A_m$ for $1 \leq i \leq m$, the we have that $|f(0)| < \prod_{i=1}^{m} |a_i|$.

If $m = 1$ then $|a_1| = A_1 > |f(a_1)|$, then

$$|f(0)| \leq \max\big\{|f(a_1) - f(0)|, |f(a_1)|\big\} \leq |f(a_1)| < |a_1|.$$

(in general for $\zeta \in B'$, $|f(\zeta) - f(0)| \leq |\zeta|$) Now, suppose that the assertion is true for $m \geq 1$, since $f - f(a_{m+1}) = (T - a_{m+1})g$ for some $g \in \mathcal{O}_{\mathbb{C}_p}[[T]]$ then $f(a_i) - f(a_{m+1}) = (a_i - a_{m+1})g(a_i)$, now using the hypothesis that $|f(a_i)| < A_{m+1}$ for $1 \leq i \leq m+1$ we find

$$|a_i - a_{m+1}||g(a_i)| \leq \max\big\{|f(a_i)|, |f(a_{m+1})|\big\} < A_{m+1}$$

for $1 \leq i \leq m$. then

$$|g(a_i)| < A_{m+1}|a_i - a_{m+1}|^{-1} = |a_{m+1}|A_m < A_m,$$

for $1 \leq i \leq m$. By induction $|g(0)| < \prod_{i=1}^{m} |a_i|$, therefore

$$|f(0)| = |f(a_{m+1}) - a_{m+1}g(0)| < \prod_{i=1}^{m+1} |a_i|,$$

as we asserted.

Now in our case take $m \in \mathbb{N}$ such that $\delta > |A_m| > 0$, since $g_n(a_i) \longrightarrow 0$ for each i, and exists $N \in \mathbb{N}$ such that for $0 \leq i \leq m$ and $n \geq N$, $|g_n(a_i)| < |A_m|$ by the claim $|g_n(0)| < |A_m| < \delta$, which is a contradiction. □

5.4 Continuity with respect to the compact open topology

Proposition 5.4.1 *The map $K((T))_1 \times B_1 \longrightarrow \mathbb{C}_p$, $(f, \zeta) \longmapsto f(\zeta)$ is continuous with respect to the product and the p-adic topologies.*

Proof. Take (f_n, ζ_n) converging to (f, ζ) in $K((T))_1 \times B_1$, then there are $0 < s < r < 1$ such that $s < |\zeta_n|, |\zeta| < r$ for all n. Now we have that

$$|f_n(\zeta_n) - f(\zeta)| \leq \max\{|f_n(\zeta_n) - f(\zeta_n)|, |f(\zeta_n) - f(\zeta)|\},$$

and by the maximum principle

$$|f_n(\zeta_n) - f(\zeta)| \leq \max\{\|f - f_n\|_r, \|f - f_n\|_s, |f(\zeta_n) - f(\zeta)|\}.$$

Therefore $f_n(\zeta_n)$ converges to $f(\zeta)$. □

Consider the n-th coefficient function $c_n : K[[T]] \longrightarrow K$ characterized by the equality

$$h = \sum c_n(h) T^n,$$

for all $h \in K[[T]]$. Let $f = \sum a_k T^k \in K[[T]]$ and $g \in TK[[T]]$. As in Definition 2.1.2, there is a well defined series $f(g) \in K[[T]]$ such that $f(g) \equiv f_N(g) \bmod T^{N+1}$ where f_N denotes the truncation $P_N(f)$. Last congruence implies that $c_k(f) = c_k(f_N)$ for all $k \leq N$.

Lemma 5.4.1 *Let $f \in K[[T]]$, $g \in T\,K[[T]]$ and $R, r > 0$ such that f, g converges in B_R and B_r respectively, then:*

1. *For $0 < s < \alpha < r$ if $\beta = \|g\|_\alpha < R$ then $|c_N\big(f(g)\big)| s^N \leq \|f\|_\beta (s/\alpha)^N$. In particular $f(g)$ converges in B_r.*

2. *If $R = \infty$ or $R > \sup_{s<r} \|g\|_s$ then for $s < r$ and $\zeta \in B_s$ we have*

$$\big(f(g)\big)(\zeta) = f(g(\zeta)).$$

3. *If $g \in T\,\mathcal{O}_K[[T]]^\times$ then for any $f \in K((T))_1$, $f(g) \in V_f$.*

Proof. Let us call $h = f(g)$ and $h_n = f_n(g) = \sum_{k\leq n} a_k g^k$, then:

(1) Since $c_N(h_N) = \sum_{k\leq N} a_k c_N(g^k)$ we have $|c_N(h_N)| \leq \sup |a_k||c_N(g^k)|$, but $|c_N(h)| = |c_N(h_N)|$ and $|c_N(g^n)|\alpha^N \leq \|g^n\|_\alpha \leq \|g\|_\alpha^n$, then

$$|c_N(h)|\alpha^N \leq \max_{k\leq N} |a_k|\|g\|_\alpha^k \leq \|f\|_\beta.$$

Hence $|c_N(h)|s^N \leq \|f\|_\beta (s/\alpha)^N$ as we stated.

(2) Let $\zeta \in S_s$ such that $s < r$, and fix α, β as in part 1, then for $k, N \in \mathbb{N}$ and $k > N$, $|c_k(h)|s^k \leq \|f\|_\beta \leq (s/\alpha)^N$. Since $c_k(h) = c_k(h_N)$ for $k \leq N$ we have that $h(\zeta) - h_N(\zeta) = \sum_{k>N} c_k(h)\zeta^k - \sum_{k>N} c_k(h_N)\zeta^k$, then

$$|h(\zeta) - h_N(\zeta)| \leq \max_{k>N}\{|c_k(h)|s^k, |c_k(h_N)|s^k\} \leq \max\{\|f\|_\beta, \|f_N\|_\beta\}(s/\alpha)^N$$

since $\|f_N\|_\beta \leq \|f\|_\beta$ we get $|h(\zeta) - h_N(\zeta)| \longrightarrow 0$, so we obtain

$$\big(f(g)\big)(\zeta) = \lim_{n\to\infty} \big(f_n(g)\big)(\zeta) = \lim_{n\to\infty} f_n\big(g(\zeta)\big).$$

Finally for $\xi = g(\zeta)$, by definition $f(\xi) = \lim_{n\to\infty} f_n(\xi) = f(g)(\zeta)$.

(3) Since $g = Tu(T)$ with $u \in \mathcal{O}_K[[T]]^\times$ by part 2 of Remark 4.2.1 we have that $|g(\zeta)| = |\zeta|$ then $\big|\big(f(g)\big)(\zeta)\big| = |f\big(g(\zeta)\big)| \leq \|f\|_{|g(\zeta)|} = \|f\|_{|\zeta|}$. □

Proposition 5.4.2 *The map $\mathcal{O}_K[[T]] \times T\,\mathcal{O}_K[[T]] \longrightarrow \mathcal{O}_K[[T]]$ defined as $(f,g) \longrightarrow f(g)$ is continuous with respect to the compact open topology.*

Proof. Let (f_n, g_n) converges to (f,g) in $\mathcal{O}_K[[T]] \times T\,\mathcal{O}_K[[T]]$ and $\eta \in \Omega'$. By Proposition 6.5 the evaluation is continuous, then we have $\lim_{n\to\infty} g_n(\eta) = g(\eta)$ and $\lim_{n\to\infty} f_n(g_n(\eta)) = f(g(\eta))$. Now taking $|\eta| < r < 1$ we have that $\|g\|, \|g_n\|_r \leq r < 1$, then by last lemma $\lim_{n\to\infty} \big(f_n(g_n)\big)(\eta) = \big(f(g)\big)(\eta)$ hence by our convergence criterium (Theorem 5.3.2) we can conclude that $\lim_{n\to\infty} f(g_n) = f(g)$. □

Corollary 5.4.1 *Let $f \in K((T))_1$. The map $f_* : T\,\mathcal{O}_K[[T]] \longrightarrow K((T))_1$, $g \longmapsto f(g)$, is continuous with respect the open compact topology.*

Proof. First, note that for $g \in T\,\mathcal{O}_K[[T]]$ and $\zeta \in B'$, $|g(\zeta)| \leq |\zeta|$ hence we have

$$|\big(f(g)\big)(\zeta)| = |f\big(g(\zeta)\big)| \leq \|f\|_{|\zeta|},$$

therefore $f(g) \in V_f$. Let $g_n \longrightarrow g$ in $T\,\mathcal{O}_K[[T]]$, by Theorem 5.3.2 is enough to show that for all $N \in \mathbb{N}$, $\lim_{n\to\infty} P_N(f(g_n)) = P_N(f(g))$. For this fix N and set $f_N = P_N(f)$, note that there is a $c_N \in K$ such that $f_N \in c_N\mathcal{O}_K[[T]]$ hence by the previous proposition $\lim_{n\to\infty} f_N(g_n) = f_N(g)$, then by continuity of P_N we get $P_N\big(f(g_n)\big) = P_N\big(f_N(g_n)\big) \longrightarrow P_N\big(f_N(g)\big) = P_N\big(f(g)\big)$. □

Corollary 5.4.2 *The map* $\lambda_* : T\,\mathcal{O}_K[[T]] \longrightarrow K[[T]]$ *is continuous.*

Proof. By Lemma 2.3.4, the map $\lambda \in K[[T]]_1$, hence λ_* must be continuous. □

Lemma 5.4.2 *Let* $s < r < t$ *all in* $p^{\mathbb{Q}^-}$. *There exists* $C > 0$ *such that for any* $f \in K((T))_1$ *we have*

$$\|f'\|_r \leq \frac{C}{r}\max\{\|f\|_s, \|f\|_t\}. \tag{5.6}$$

Proof. Let $f = \sum_{n\in\mathbb{Z}} a_n T^n$ so $f' = \sum_{n\in\mathbb{Z}} n a_n T^{n-1}$. Now for $n \geq 1$,

$$\begin{aligned} n|a_n|r^{n-1} &= r^{-1}n|a_n|t^n\left(\frac{r}{t}\right)^n \leq \frac{C_1}{r}\|f\|_t\,, \\ n|a_{-n}|r^{-n-1} &= r^{-1}n|a_{-n}|s^{-n}\left(\frac{s}{r}\right)^n \leq \frac{C_2}{r}\|f\|_s\,, \end{aligned}$$

where $C_1 = \sup\limits_{n\geq 1} n(r/t)^n$ and $C_2 = \sup\limits_{n\geq 1} n(s/r)^n$. Then $C = \max\{C_1, C_2\}$ satisfies 5.6. □

Proposition 5.4.3 *The Formal derivative on* $K((T))_1$ *is continuous with respect to the compact-open topology.*

Proof. It is clear from Lemma 5.4.2 □

Chapter 6

Coleman Local Theory

6.1 Generalities and Notation

In this chapter we will study several Galois action associated to a finite abelian unramified extension of $\mathbb{Q}_p$, on several rings on power series. Let us recall the definition:

Definition 6.1.1 *A Galois extension $E/\mathbb{Q}_p$ is unramified if*

$$[E : \mathbb{Q}_p] = [k_E : \mathbb{F}_p].$$

Let $E/\mathbb{Q}_p$ any finite Galois extension and $n = [E : \mathbb{Q}_p]$. Here are some general remarks:

Remark 6.1.1

1. *We will use the usual notation $\mathcal{O}_E$ for the ring of integral elements over $\mathbb{Z}_p$ of E, $\mathfrak{p}_E$ for its maximal ideal and $k_E = \mathcal{O}_E/\mathfrak{p}_E$, its residual field.*

2. *It is well known that $n = ef$ where e is the ramification index and f the inertia degree, given by $p\mathcal{O}_E = \mathfrak{p}_E^e$ and $f = [k_E/\mathbb{F}_p]$ (See [Neu99]). By definition in the unramified case $n = f$ and $e = 1$, in particular p is a uniformizer for E.*

3. *Consider the canonical surjective homomorphism $\mathrm{Gal}(E/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(k_E/\mathbb{F}_p)$ [Neu99, p. 56]. It is an isomorphism if and only if $E/\mathbb{Q}_p$ is unramified.*

4. *k_E is a finite extension of $\mathbb{F}_p$ therefore it is a finite field with p^f elements and has a* **Frobenius automorphism** *φ_E defined as $\varphi_E(a) = a^p$ for all $a \in k_E$ which fixes $k_E^{\varphi_E} = \mathbb{F}_p$.*

5. *The automorphism $\varphi_E \in \mathrm{Gal}(k_E/\mathbb{F}_p)$ has a unique lift $\varphi \in \mathrm{Gal}(E/\mathbb{Q}_p)$, which is a generator of $\mathrm{Gal}(E/\mathbb{Q}_p)$, and is called the Frobenius element of $\mathrm{Gal}(E/\mathbb{Q}_p)$.*

Let us fix the notation for this chapter:

Let K an unramified finite Galois extension of $\mathbb{Q}_p$ in a fixed algebraic closure $\mathbb{C}_p$, with $f = [K/\mathbb{Q}_p]$, $\Delta = \mathrm{Gal}\big(K/\mathbb{Q}_p\big)$ and Frobenius element φ. By the previous discussion

$$\Delta = \langle\, \varphi \,\rangle = \{1, \varphi, \cdots, \varphi^{f-1}\}.$$

Let $K_n = K[\zeta_p^{n+1}]$, $K_\infty = \bigcup K_n$ and $G_n = \mathrm{Gal}\big(K_n/K\big)$, $G_\infty = \mathrm{Gal}\big(K_\infty/K\big) = \varprojlim G_n$. As K is unramified we have $G_\infty \cong \mathrm{Gal}\big(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p\big) \cong \mathbb{Z}_p^\times$ as topological groups, given canonically by the cyclotomic character $\kappa : G_\infty \xrightarrow{\simeq} \mathbb{Z}_p^\times$ defined by its action on p-th roots of unity, $\sigma(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^{\kappa(\sigma)}$.

6.2 The multiplicative $\mathbb{Z}_p$-action on $\mathfrak{M}_K$

Let $\mathfrak{M}_K$ be the set of units of $\mathcal{O}_K[[T]]$ and $\mathfrak{M}_K$ be the set of principal units of $\mathcal{O}_K[[T]]$ i.e. the set of $f \in \mathfrak{M}_K[[T]]$ such that $f(0) \equiv 1 \bmod \mathfrak{p}_K$.

Remark 6.2.1

1. *Since $\mathcal{O}_K[[T]]$ and $U_K = 1 + p\mathcal{O}_K$ are compact and the sum is continuous, $\mathfrak{M}_K = U_K + T\mathcal{O}_K[[T]]$ is compact.*

2. *$\mathfrak{M}_K = \mathcal{O}_K^\times \mathfrak{M}_K$ and since $\mathcal{O}_K^\times$ is compact, then $\mathfrak{M}_K$ is compact.*

The multiplicative group $\mathfrak{M}_K$ admits a natural $\mathbb{Z}$-action given by exponentiation i.e. $(n, f) \in \mathbb{Z} \times \mathfrak{M}_K \longmapsto f^n$. The aim of this section is to extend this natural action to a $\mathbb{Z}_p$-action.

Lemma 6.2.1 *For $\alpha \in \mathbb{Z}_p$ there is a well defined series $(1+T)^\alpha \in \mathbb{Z}_p[[T]]$ such that for every sequence $(\alpha_n)_{n\in\mathbb{N}} \subseteq \mathbb{N}$, $\alpha_n \longrightarrow \alpha$ we have that $(1+T)^{\alpha_n} \longrightarrow (1+T)^\alpha$.*

Proof. Let $\tau : \mathbb{Z}_p \longrightarrow TK[[T]]$, $\tau(\alpha) = \alpha\lambda$ and $\varepsilon = \exp(\tau)$ i.e. $\varepsilon : \mathbb{Z}_p \longrightarrow \mathfrak{M}_K$, $\varepsilon(\alpha) = \exp(\alpha\lambda)$. By Proposition 5.4.2 the map ε is continuous since $\exp^*$ and τ are continuous. By Theorem 2.2.1, for $n \in \mathbb{N}$ $(1+T)^n = \exp(n\lambda) = \varepsilon(n)$, therefore for $\alpha \in \mathbb{Z}_p$ the power series $\varepsilon(\alpha)$ has the desired property i.e. can be taken as $(1+T)^\alpha$. □

Corollary 6.2.1 *There is a unique continuous $\mathbb{Z}_p$-action on U_K which extends the natural $\mathbb{Z}$-action given by $(n, u) \in \mathbb{Z} \times U_K \longmapsto u^n \in U_K$.*

Proof. Since for $\alpha \in \mathbb{Z}_p$, $(1+T)^\alpha \in \mathbb{Z}_p[[T]]$ it must converges in B_1, then we can define $u = 1 + \zeta \in U_K$, $u^\alpha = (1+T)^\alpha(\zeta)$. Let $\varepsilon_K : \mathbb{Z}_p \times U_K \longrightarrow U_K$ given by $\varepsilon_K(\alpha, 1+\zeta) =$

$(1+T)^\alpha(\zeta)$. By Lemma 2.3.1 ε_K is continuous, hence by continuity it is a well define $\mathbb{Z}_p$-action on U_K totaly determined by its restriction over $\mathbb{Z} \times U_K$. □

Theorem 6.2.1 *There is $\mathbb{Z}_p$ continuous action on the multiplicative group $\mathfrak{M}_K$ that extends the natural $\mathbb{Z}$-action.*

Proof. For $f \in \mathfrak{M}_K$ we can write $f = f(0)(1+g)$ where $g \in T\,\mathcal{O}_K[[T]]$ and clearly this decomposition is continuous. By the previous lemmas we have a continuous map

$$(\alpha, f) \in \mathbb{Z}^p \times \mathfrak{M}_K \longmapsto f(0)^\alpha (1+g)^\alpha = f(0)^\alpha \big((1+T)^\alpha\big)_*(g) \in \mathfrak{M}_K.$$

By continuity, it is a well defined $\mathbb{Z}_p$-action on $\mathfrak{M}_K$ and it is totaly determined by its restriction over $\mathbb{Z} \times \mathfrak{M}_K$. □

Definition 6.2.1 *We define the exponential $\mathbb{Z}_p$-actions on U_K and $\mathfrak{M}_K$ as the unique $\mathbb{Z}_p$ actions that extends the respective natural $\mathbb{Z}$-actions given by exponentiation.*

Now, for $\alpha \in \mathbb{Z}_p$, let us consider the power series $[\alpha] = (1+T)^\alpha - 1$.

Remark 6.2.2

For $\alpha, \beta \in \mathbb{Z}_p$, we have $[\alpha]\big([\beta]\big) = [\alpha\beta] = [\beta]\big([\alpha]\big)$. This is clear by continuity of the exponentiation since it is true for $\alpha, \beta \in \mathbb{Z}$.

6.3 Galois Structures on $K((T))_1$

Remark 6.3.1

1. *Since each $\mathcal{O}_K[G_n]$ is an $\mathcal{O}_K$ free module of finite rank we can endowed them with the canonical Topology induced by $\mathcal{O}_K$.*

2. *The product $\prod_{n\in\mathbb{N}} \mathcal{O}_K[G_n]$ is a compact topological space with respect to the product topology. Further it is a topological $\mathcal{O}_K$-algebra (with term-to-term operations).*

3. *The product topology in $\prod_{n\in\mathbb{N}} \mathcal{O}_K[G_n]$ has as basis:*

$$\{U_1 \times U_2 \times \ldots \mid U_n \subseteq \mathcal{O}_K[G_n] \text{ are open and } U_n = \mathcal{O}_K[G_n] \text{ for } n \text{ big enough}\}$$

Note that for $m \leq n$ the restrictions $G_n \longrightarrow G_m$ induce ring homomorphisms on the group algebras $\pi_{m,n} : \mathcal{O}_K[G_n] \longrightarrow \mathcal{O}_K[G_m]$. This constitute an inverse system of rings, so we can consider its inverse limit $\varprojlim \mathcal{O}_K[G_n]$ as the subset of $\prod_{n\in\mathbb{N}} \mathcal{O}_K[G_n]$.

Definition 6.3.1 *We define the* **Iwasawa Ring** *$\mathcal{O}_K[[G_\infty]]$ as $\varprojlim \mathcal{O}_K[G_n]$ endowed with the inverse-limit topology i.e. the topology induced by the product topology.*

Each $\mathcal{O}_K[G_n]$ acts on K_n naturally extending the action of G_n by linearity i.e. for $x \in K_n$ and $\theta = \sum_{j=1}^N a_j\sigma_j \in \mathcal{O}_K[G_n]$, $\theta \cdot x = \sum a_j\sigma_j(x)$,

$$|\theta \cdot x| \leq \max_{j\leq N} |a_j||\sigma_j x| \leq |x|$$

which means that these actions are continuous. Also these actions are compatible with respect to restrictions and we can extend them to an action of $\mathcal{O}_K[[G_\infty]]$ on K_∞ in the following way: for $x \in K_\infty = \bigcup\limits_{n\in\mathbb{N}} K_n$ and $\theta = (\theta_n)_{n\in\mathbb{N}} \in \mathcal{O}_K[[G_\infty]]$, since $x \in K_m$ for some m, we can define $\theta \cdot x = \theta_m \cdot x$ (which is well define by compatibility). For $G_\infty = \varprojlim G_n$, let us consider $\mathcal{O}_K[G_\infty]$ with its natural action on K_∞ i.e. the linear extension of the action of G_∞.

Lemma 6.3.1 *$\mathcal{O}_K[G_\infty]$ is densely immersed in $\mathcal{O}_K[[G_\infty]]$ in a canonical way such that the actions on K_∞ are compatible.*

Proof. First note that the natural projections $G_\infty \longrightarrow G_n$ extend to algebra morphisms $\mathcal{O}_K[G_\infty] \xrightarrow{\varphi_n} \mathcal{O}_K[G_n]$ in a compatible way with respect to restrictions, then by the universal property we have a map $\mathcal{O}_K[G_\infty] \xrightarrow{\varphi} \mathcal{O}_K[[G_\infty]]$ such that $\pi_n\varphi = \varphi_n$ i.e. the following diagram commutes:

$$\begin{array}{ccc} \mathcal{O}_K[G_\infty] & \xrightarrow{\varphi} & \mathcal{O}_K[[G_\infty]] \\ & {\scriptstyle\varphi_n}\searrow & \downarrow{\scriptstyle\pi_n} \\ & & \mathcal{O}_K[G_n] \end{array}$$

φ has dense image because the arrows φ_n are surjective. For the injectivity of φ take $\theta \in \ker\varphi$, $\theta = \sum\limits_{j=1}^N a_j\sigma_j$ with $\sigma_j \in G_\infty$ all different, then there must be a $m \in \mathbb{N}$ such that $\sigma_j|_{K_m}$ are all different so by Dedekind's independence lemma ([Mil08, pp.52]) the $\sigma_j|_{K_m}$ must be linearly independent. Then

$$0 = \varphi_n(\theta) = \sum_{j=1}^N a_j\big(\sigma_j|_{K_m^\times}\big) \Longrightarrow a_1 = \ldots = a_N = 0 \Longrightarrow \theta = 0.$$

Finally, the actions are compatible because both coincide on $\mathcal{O}_K[G_n]$. □

From now on we will consider $\mathcal{O}_K[G_\infty]$ as a topological subring of $\mathcal{O}_K[[G_\infty]]$.

Remark 6.3.2

1. *By Lemma 6.2.1 for $\sigma \in G_\infty$ there we can consider the power series:*

$$[\kappa(\sigma)] = (1+T)^{[\kappa(\sigma)]} - 1 \in T\mathcal{O}_K[[T]],$$

therefore for any $f \in K((T))_1$ there is a well defined power series

$$\sigma \cdot f = f([\kappa(\sigma)]) \in K((T))_1.$$

2. *For $u \in \Omega$ i.e. $u = \zeta_{p^{n+1}}^{a} - 1$ and $\sigma \in G_\infty$ we have*

$$(\sigma \cdot f)(u) = f([\kappa(\sigma)](u)) = f(\zeta_{p^{n+1}}^{au} - 1) = \sigma(f(u)).$$

3. *For $\sigma \in G_\infty$ and $f \in K[[T]]_1$ we have that $(\sigma \cdot f)\big([\alpha]\big) = \sigma \cdot f([\alpha])$. This is a consequence of Remark 6.2.2 since $(\sigma \cdot f)\big([\alpha]\big) = f([\kappa(\sigma)\alpha]) = f([\alpha] \circ [\kappa(\sigma)]) = \sigma \cdot f([\alpha])$.*

Theorem 6.3.1 *There is a unique continuous structure of $\mathcal{O}_K[[G_\infty]]$-module on $K((T))_1$ which extends the K-module structure such that for all $f \in K((T))_1$ and $\sigma \in G_\infty$, we have*

$$\sigma \cdot f = f\big([\kappa(\sigma)]\big) = f\big((1+T)^{\kappa(\sigma)} - 1\big).$$

Proof. Let $\sigma \in G_\infty$ and $[\kappa(\sigma)] \in T\mathcal{O}_K[[T]]$. By part 3 of Lemma 5.4.1 for $f \in K((T))_1$ we have that $f([\kappa(\sigma)]) \in V_f$ then by linearity for any $\theta \in \mathcal{O}_K[G_\infty]$ we have that $\theta \cdot f \in V_f \subseteq K((T))_1$. In particular we have an $\mathcal{O}_K[G_\infty]$-module structure on $K((T))_1$. For extending the action of $\mathcal{O}_K[G_\infty]$ to an action of $\mathcal{O}_K[[G_\infty]]$, by Lemma 6.3.1, it is enough to prove that it is continuous on $\mathcal{O}_K[G_\infty]$. For this purpose take $(\theta_n, f_n) \in \mathcal{O}_K[G_\infty] \times K((T))_1$ such that $(\theta_n, f_n) \longrightarrow (\theta, f)$. Note that

$$\theta_n \cdot f_n - \theta \cdot f = \theta_n \cdot (f_n - f) + (\theta_n - \theta) \cdot f.$$

Now taking $\varepsilon > 0$, $0 < r < 1$ and $g_n = f_n - f$, for n big enough we have $g_n \in V(r, \varepsilon)$, then $\theta_n \cdot g_n \in V_{g_n} \subseteq V(r, \varepsilon)$ which means that $\lim_{n\to\infty} \theta_n \cdot g_n = 0$. For the remanning case we need:

Lemma 6.3.2 *For $(\theta_n)_{n\in\mathbb{N}} \subseteq \mathcal{O}_K[G_\infty]$ such that $\lim_{n\to\infty} \theta_n = 0$ and $f \in K((T))_1$ we have that $\lim_{n\to\infty} \theta_n \cdot f = 0$ with respect to the compact-open topology.*

Proof. Suppose first that $f \in \mathcal{O}_K((T))$. Since $\mathcal{O}_K[[G_\infty]]$ acts continuously on K_∞ for any $x \in K_\infty$, $\lim_{n\to\infty} \theta_n(x) = 0$. Now using part 2 of Remark 6.3.2 we have that for any $\theta \in \mathcal{O}_K[G_\infty]$ we get $(\theta \cdot f)(u) = \theta(f(u))$ then for $u \in \Omega$, $\lim_{n\to\infty} (\theta_n \cdot f)(u) = \lim_{n\to\infty} \theta_n(f(u)) = 0$. By Theorem 5.3.2 we may conclude that $\theta_n \cdot f = 0$ as we wanted. For the general case, taking $f \in K((T))_1$ we have that the truncations $P_m(f) \in a_m\mathcal{O}_K((T))$ for some $a_m \in K^\times$ and since for any $\theta \in \mathcal{O}_K[G_\infty]$, $P_m(\theta \cdot f) = P_m\big(\theta \cdot P_m(f)\big)$ we have that $\lim_{n\to\infty} P_m(\theta_n \cdot f) = 0$ for any $m \in \mathbb{N}$. Therefore by Proposition 5.2.1 we get $\lim_{n\to\infty} \theta_n \cdot f = 0$. $\square$

6.4 The Norm Operator

Let $\mathcal{O}_n, \mathfrak{p}_n$ denote the ring of integral elements of K_n and its maximal ideal respectively and $\Omega_n = \{\zeta_{p^{n+1}}^{a} - 1 \,|\, a \in \mathbb{Z}\}$ i.e. the set of non zero roots of $[p^{n+1}]$. For $f \in \mathcal{O}_K[[T]]$ and

$u \in \mathcal{O}_K$ let us denote $u[+]T = (1+u)(1+T)-1$ and

$$f_u(T) = f(u[+]T) = f((1+u)(1+T)-1) \in \mathcal{O}_K[[T]].$$

We will say that $f \in \mathcal{O}_K[[T]]$ is Ω_n invariant if $f_u = f$ for all $u \in \Omega_n$ i.e. if for $1 \leq a < p^{n+1}$ we have $f(T) = f(\zeta_{p^{n+1}}^a(1+T)-1)$, for example $[p^{n+1}]$ is always Ω_n invariant.

Lemma 6.4.1 *If $f \in \mathcal{O}_K[[T]]$ is Ω_0-invariant there exists a unique $g \in \mathcal{O}_K[[T]]$ such that $f = g\big([\,p\,]\big)$.*

Proof. Uniqueness: if $g([p]) = h([p])$, g and h coincide in $\bigcup_{n\in\mathbb{N}} \Omega_n$, since $[\,p\,](\Omega_{n+1}) = \Omega_n$ we have that $h|_\Omega = g|_\Omega$, therefore by the unicity lemma, Lemma 2.3.3, we get $g = h$.
Existence: Let us suppose that for $0 \leq i \leq n-1$, we have $a_i \in \mathcal{O}_K$ such that

$$f = \sum_{i=0}^{n-1} a_i[\,p\,]^i + [\,p\,]^n f_n, \tag{6.1}$$

for some $f_n \in O_K[[T]]$ (for $n = 0$ such presentation is trivial) and consider $g_n = f_n - f_n(0)$. By the preparation theorem (Theorem 4.2.1) for g_n exists $\mu \in \mathbb{N}$, $u \in \mathcal{O}_K[[T]]^\times$ and $P \in \mathcal{O}_K[T]$ distinguished such that $g_n = p^\mu P(T)u(T)$. On the other hand since f and $[\,p\,]$ are Ω_0-invariants, by equation (6.1) f_n must be Ω_0 invariant. But then P vanishes in Ω_0, so it is divisible by $[\,p\,]$ (because it is divisible by T and the minimal polynomial of $\zeta_p - 1$). Taking $a_n = f_n(0)$ we have that $f_n = a_n + [\,p\,]f_{n+1}$ therefore we get $f = \sum_{i=0}^{n} a_i[\,p\,]^i + [\,p\,]^n f_{n+1}$. In this way we construct a sequence $(a_n) \subseteq K$ such that

$$f - \sum_{i=0}^{\infty} a_i[\,p\,]^i \in \bigcap_{n\geq 0} [\,p\,]^n \mathcal{O}_K[[T]] = 0.$$

Setting $g = \sum_{i=0}^{\infty} a_i T^i$ we have $f = g\big([p]\big)$. □

Let $K[[T]]_1^{\Omega_0}$ and $\mathcal{O}_K[[T]]^{\Omega_0}$ be the subrings of $K[[T]]_1$ and $\mathcal{O}_K[[T]]$ respectively of Ω_0-invariant power series. Last lemma implies that $[\,p\,]^* : \mathcal{O}_K[[T]] \longrightarrow \mathcal{O}_K[[T]]^{\Omega_0}$ is an algebraic ring isomorphism.

Lemma 6.4.2 1. *For $u \in \Omega$ the maps from $K((T))_1$ to itself: $f \longmapsto f_u$ are continuous ring homomorphisms with respect to the compact-open topology.*

2. *The ring isomorphism $[\,p\,]^* : \mathcal{O}_K[[T]] \longrightarrow \mathcal{O}_K[[T]]^{\Omega_0}$ is a topological isomorphism with respect to the compact-open topology.*

Proof. (1) Since the maps $f \longmapsto f_u$ are ring homomorphisms, they are continuous if and only if they are continuous at 0. For this let $\lim_{n\to\infty} f_n = 0$ in $K((T))_1$ and $u' \in \Omega$ then for any $u' \in \Omega'$ we have $\lim_{n\to\infty} (f_n)_u(u') = \lim_{n\to\infty} f_n(u[+]u') = 0$. Since u' is arbitrary in Ω' by Theorem 5.3.2 we have get $\lim_{n\to\infty} (f_n)_u = 0$.

(2) Let $\lim_{n\to\infty} f_n = 0$ in $\mathcal{O}_K[[T]]$. For any $u \in \Omega'$, $\lim_{n\to\infty} f_n\big([p](u)\big) = 0$ but $[p](\Omega) = \Omega$ hence, by Theorem 5.3.2, $\lim_{n\to\infty} f_n\big([p]\big) = 0$. Lemma 6.4.1 says that $[p]^*$ is a bijection, hence a continuous isomorphism, but by Corollary 5.3.1 $\mathcal{O}_K[[T]]$ is compact, then $[p]^*$ must be a topological isomorphism. □

Theorem 6.4.1 *The ring homomorphism*

$$\begin{array}{rccc} [p]^* : & K[[T]]_1 & \longrightarrow & K[[T]]_1^{\Omega_0} \\ & f & \longmapsto & f\big([p]\big) \end{array}$$

is a topological isomorphism with respect to the compact-open topology.

Proof. By Corollary 5.4.1 $[p]^*$ is continuous and it is clearly and homomorphism. Let $K \cdot \mathcal{O}_K[[T]] = \{\alpha f \mid (\alpha, f) \in K \times \mathcal{O}_K[[T]]\}$ and $K \cdot \mathcal{O}_K[[T]]^{\Omega_0} = K \cdot \mathcal{O}_K[[T]] \cap K[[T]]_1^{\Omega_0}$. By Lemma 6.4.1 it is easy to see that $[p]^*$ maps $K \cdot \mathcal{O}_K[[T]]$ onto $K \cdot \mathcal{O}_K[[T]]^{\Omega_0}$. Since both sets are dense respectively in $K[[T]]_1$ and $K[[T]]_1^{\Omega_0}$, then $[p]^*$ is surjective. We only need to prove that $[p]^*$ has continuous inverse in $K \cdot \mathcal{O}_K^{\Omega_0}$, since by continuity it can be extended to a continuous map defined in $K[[T]]_1^{\Omega_0}$ and it will be the inverse of $[p]^*$. For this we will need the following claim:

Claim: Let $h \in K[[T]]_1$, $r \in p^{\mathbb{Q}^-}$, $p^{-\frac{p}{p-1}} < r < 1$ and $t = r^{1/p}$. Then $\|h\|_r = \|h\big([p]\big)\|_t$. Let $\zeta \in S_t$ i.e. $|\zeta| = t$, then $[p](\zeta) = (1+\zeta)^p - 1 = \displaystyle\sum_{k=1}^{p} \binom{p}{k} \zeta^k$. Note that

$$\left| \binom{p}{k} \zeta^k \right| = \begin{cases} |\zeta|^p & \text{if } k = p \\ \frac{1}{p}|\zeta|^k & \text{if } 1 \le k \le p-1. \end{cases}$$

Since $p^{-\frac{1}{p-1}} < |\zeta|$ we have that for $1 \le k \le p-1$: $\frac{1}{p}|\zeta|^k < \frac{1}{p}|\zeta| < |\zeta|^p$ therefore r is a regular radius for $[p]$ and $[p](S_t) \subseteq S_r$, in particular $\|h([p])\|_t \le \|h\|_r$. Now by Theorem 5.1.2 there exits $\xi \in S_r$ such that $\|h\|_r = |h(\xi)|$. Now taking ζ a root of $[p] - \xi$ we have $\big|[p](\zeta)\big| = r$, since $M_{[p]}$ is strictly increasing we must have that $|\zeta| = t$, therefore

$$\|h\|_r = |h(\xi)| = \big|h\big([p](\zeta)\big)\big| \le \|h([p])\|_t \le \|h\|_r.$$

Returning to our case by part 2 of Lemma 6.4.2 $\big([p]^*\big)^{-1}$ is well defined in $K \cdot \mathcal{O}_K^{\Omega_0}$ and by linearity we only need to check continuity at 0. For that purpose let us prove that for any $f_n \in K \cdot \mathcal{O}_K[[T]]$ such that $\lim\limits_{n\to\infty} f_n([\,p\,]) = 0$ we have $\lim\limits_{n\to\infty} f_n = 0$. By last claim for any r, $p^{-\frac{p}{p-1}} < r < 1$ we have $\|f_n\|_r = \|f_n([\,p\,])\|_{r^{1/p}}$, but for any $s \in p^{\mathbb{Q}^-}$ we have $\lim\limits_{n\to\infty} \|f_n\|_s = 0$, therefore $\lim\limits_{n\to\infty} f_n = 0$. $\square$

Theorem 6.4.2 *There exists unique map* **Norm** $\mathrm{Nr}_K : \mathcal{O}_K[[T]] \longrightarrow \mathcal{O}_K[[T]]$ *such that*

$$\mathrm{Nr}_K(f)\big([\,p\,]\big) = \prod_{u\in\Omega_0} f_u. \tag{6.2}$$

Further, this map is continuous and multiplicative i.e. $\mathrm{Nr}_K(fg) = \mathrm{Nr}_K(f)\,\mathrm{Nr}_K(g)$.

Proof. Let $F : \mathcal{O}_K[[T]] \longrightarrow \mathcal{O}_K[[T]]$ defined as $F(f) = \prod\limits_{u\in\Omega_0'} f_u$. Clearly F is multiplicative and, by part 1 of Lemma 6.4.2, continuous. For $f \in \mathcal{O}_K[[T]]$, since $(f_u)_{u'} = f_{u[+]u'}$, $F(f) \in \mathcal{O}_K[[T]]^{\Omega}$. Therefore by Lemma 6.4.1 we can define a continuous map $\mathrm{Nr}_K = F \circ ([\,p\,]^*)^{-1}$ which satisfies (6.2).

Remark 6.4.1

1. $\mathrm{ord}\big(\mathrm{Nr}_K(f)\big) = \mathrm{ord}(f)$. *Since* $F = \mathrm{Nr}_K(f)([\,p\,]) = \prod\limits_{u\in\Omega_0} f_u$ *we have that* $\mathrm{ord}\,F = p\,\mathrm{ord}\,f = \sum\limits_{u\in\Omega_0} \mathrm{ord}\,f_u$, *on the other hand for* $u \in \Omega_0$, $\mathrm{ord}\,f_u = \mathrm{ord}\,f$, *therefore we may conclude.*

2. *Let* $\eta_n = \zeta_{p^{n+1}} - 1$, *since* $[\,p\,](\eta_{n+1}) = u_n$ *we have* $\mathrm{Nr}_K(f)(\eta_n) = \mathrm{Nr}_K\, kn + 1n\big(f(\eta_{n+1})\big)$, *further by induction we get*

$$\mathrm{Nr}_K^k(f)(\eta_n) = \mathrm{Nr}_K\, kn + kn\big(f(\eta_{n+k})\big).$$

Let $\Lambda_K = \varprojlim \mathbb{Z}_p[G_n]$ (respect the canonical restrictions), since the inclusions $\mathbb{Z}_p[G_n] \hookrightarrow \mathcal{O}_K[G_n]$ are compatible with the Lemma 6.3.1 for the case $K = \mathbb{Q}_p$,we get that $\mathbb{Z}_p[G_\infty]$ is canonically densely immersed in Λ_K.
Now by Lemma 6.2.1 for $f \in \mathfrak{M}_K$ and $a \in \mathbb{Z}_p$ then $(a, f) \longrightarrow f^a$ is a well defined and continuous action, and it is easy to see that for $f \in \mathfrak{M}_K$, $\sigma \cdot f \in \mathfrak{M}_K$. Hence we have a structure of $\mathbb{Z}_p[G_\infty]$-module on the multiplicative abelian group $\mathfrak{M}_K$. For this action we will use the following notation: For $\theta = \sum a_k\sigma_k \in \mathbb{Z}_p[G_\infty]$ and $f \in \mathfrak{M}_K$ we will denote

$$f^\theta = f^{\sum a_k\sigma_k} = \prod (\sigma_k \cdot f)^{a_k}.$$

Lemma 6.4.3 *There is a unique* $\mathbb{Z}_p[G_\infty]$*-homomorphism* $\log : \mathfrak{M}_K \longrightarrow K[[T]]$ *such that*

$$\exp_* \log = Id_{\mathfrak{M}_K}$$

Proof. Note that for $g \in \mathfrak{M}_K$ we have the factorization $g = u(1+f)$ and the map $g \longmapsto (u, f) \in U_K^1 \times T\,\mathcal{O}_K$ is continuous. Therefore we can define

$$\log g = \log_K u + \lambda_* f,$$

which is continuous by the continuity of $\lambda_\star$ in $T\mathcal{O}_K[[T]]$ and the continuity of $\log_K$ in U_K^1. Now since K is unramified the exponential map $\exp_K : p\mathcal{O}_K \longrightarrow U_K^1$ is the inverse of $\log_K$ and by part 1 of Theorem 2.2.1 we have $\exp(\lambda_*(f)) = 1 + f$, therefore

$$\exp(\log g) = \exp(\log_K u) + \exp(\lambda_*(f)) = u(1+f) = g.$$

By part 2 of Theorem 2.2.1 for $1+f, 1+g \in 1 + T\mathcal{O}_K$ we have that

$$\log\big((1+f)(1+g)\big) = \lambda(f[+]g) = \lambda(f) + \lambda(g) = \log(1+f) + \log(1+g).$$

In particular for $n \in \mathbb{N}$, $\log\big((1+f)^n\big) = n \log(1+f)$, therefore by continuity we get $\log\big((1+f)^\alpha\big) = \alpha \log(1+f)$ for any $\alpha \in \mathbb{Z}_p$, hence log is a $\mathbb{Z}_p$-homomorphism. Now for $\alpha \in \mathbb{Z}_p$, $[\alpha] \in T\,K[[T]]$, by Corollary 2.1.1 part 2 we have for any $h \in T\,K[[T]]$ that

$$\lambda\big(h([\alpha])\big) = \big(\lambda(h)\big)([\alpha]).$$

Then for $f \in \mathfrak{M}_K$ and $\sigma \in G_\infty$ we have

$$\log(\sigma \cdot f) = \log\big(f([\kappa(\sigma)])\big) = \big(\log(f)\big)([\kappa(\sigma)]) = \sigma \cdot \log(f).$$

Then log is a $\mathbb{Z}_p[G_\infty]$-homomorphism. □

Theorem 6.4.3 *The set $\mathfrak{M}_K$ has a unique structure of continuous Λ_K-module which extends the $\mathbb{Z}_p[G_\infty]$ action i.e. $f \in \mathfrak{M}_K$, $a \in \mathbb{Z}_p$ and $\sigma \in G_\infty$ we have*

$$a \cdot f = f^a \text{ and } \sigma \cdot f = f([\kappa(\sigma)]).$$

Proof. As in Theorem 6.3.1 (since $\mathbb{Z}_p[G_\infty]$ is dense is Λ_K) the continuity of the action of $\mathbb{Z}_p[G_\infty]$ is enough to get an extension to a unique continuous action of Λ_K on $\mathfrak{M}_K$. For this, let $(\theta_n, f_n) \in \mathbb{Z}_p[G_\infty] \times \mathfrak{M}_K$ such that $\theta_n \longrightarrow \theta$ and $f_n \longrightarrow f$. Notice that

$$(f_n)^{\theta_n} = \big(f_n f^{-1}\big)^{\theta_n} f^{\theta_n} \tag{6.3}$$

Let us prove that $(f_n)^\theta \longrightarrow f^\theta$: Take $u \in \Omega'$, for any $g \in \mathfrak{M}_K$ and $\theta = \sum a_k \sigma_k$, by Lemma 2.3.1 and Remark 6.3.2, we have that

$$g^\theta(u) = \prod (\sigma \cdot g)^{a_k}(u) = \prod g\big(\sigma(u)\big)^{a_k}.$$

Now since $f_n(\sigma(u)) \longrightarrow f(\sigma(u))$ and using the continuity of $\mathbb{Z}_p$ multiplicative action we have that

$$(f_n)^\theta(u) = \prod f_n(\sigma(u))^{a_k} \longrightarrow \prod f(\sigma(u))^{a_k} = f^\theta(u),$$

then by Theorem 5.3.2 we have $f^{\theta_n} \longrightarrow f^\theta$. By equation (6.3) it is enough to show that if $g_n \longrightarrow 1$ then $g_n^{\theta_n} \longrightarrow 1$, but since log is continuous we have $\log(g_n) \longrightarrow 0$ and by Theorem 6.3.1 and Lemma 6.4.3 $\log(g_n^{\theta_n}) = \theta_n \cdot \log(g_n) \longrightarrow 0$, therefore using Lemma 6.4.3 we get

$$g_n^{\theta_n} = \exp_*\big(\log(g_n^{\theta_n})\big) \longrightarrow 1,$$

as we wanted to prove. □

Remark 6.4.2

1. *If $\sigma \in G_\infty$, $f \in K((T))_1$ and $u \in B'$ then we have $(\sigma \cdot f)_u = f_u\big([\kappa(\sigma)]\big) = \sigma \cdot f_u$. Note that $(\sigma \cdot f)_u = f\big([\kappa(\sigma)]\big)_u = f\big([\kappa(\sigma)](u[+]T)\big)$, therefore*

$$(\sigma \cdot f)_u = f\big((1+u)^{[\kappa(\sigma)]}(1+T)^{[\kappa(\sigma)]} - 1\big) = f_u\big([\kappa(\sigma)]\big).$$

Proposition 6.4.1 *The map Nr_K leaves invariant $\mathfrak{M}_K$ and $\mathfrak{M}_K$, further Nr_K restricts to a Λ_K endomorphism of $\mathfrak{M}_K$ i.e. for all $\theta \in \Lambda_K$ and $f \in \mathfrak{M}_K$,*

$$\mathrm{Nr}_K(\theta \cdot f) = \theta \cdot \mathrm{Nr}_K(f).$$

Proof. Since Nr_K is multiplicative, it leaves invariant $\mathfrak{M}_K$ and since it preserve $\mathcal{O}_K[[T]]$ we have $\mathrm{Nr}_K(\mathfrak{M}_K) \subseteq \mathcal{O}_K[[T]] \cap \mathfrak{M}_K$. Now since $\mathrm{Nr}_K = F\big([p]^*\big)^{-1}$ (see Theorem 6.4.2) the first coefficient of $\mathrm{Nr}_K(f)$ is the p-th power of the first coefficient of f, then $\mathrm{Nr}_K(\mathfrak{M}_K) \subseteq \mathfrak{M}_K$. Since Nr_K is multiplicative it does commute with the $\mathbb{Z}$-action on $\mathfrak{M}_K$, therefore by continuity it must commute with the extended action of $\mathbb{Z}_p$. Now, by last lemma we have

$$\big(\mathrm{Nr}_K(\sigma \cdot f)\big)\big([p]\big) = \prod_{u \in \Omega_0} (\sigma \cdot f)_u = \prod_{u \in \Omega_0} f_u\big([\kappa(\sigma)]\big) = \big(\sigma \cdot \mathrm{Nr}_K(f)\big)\big([p]\big),$$

hence $\mathrm{Nr}_K(\sigma \cdot f) = \sigma \cdot \mathrm{Nr}_K(f)$. We have proven that the norm commutes with the $\mathbb{Z}_p[G_\infty]$-action therefore by continuity of the norm it must commute with the Λ_K-action i.e. the norm must be a Λ_K-endomorphism. □

Theorem 6.4.4 *There exists unique map $\mathrm{Tr}_K : K[[T]]_1 \longrightarrow K[[T]]_1$ such that*

$$\mathrm{Tr}_K(f)\big([p]\big) = \sum_{u \in \Omega_0} f_u. \tag{6.4}$$

further it is a continuous $\mathcal{O}_K[[G_\infty]]$-homomorphism.

Proof. Let $S : K[[T]]_1 \longrightarrow K[[T]]_1$, $S(f) = \sum_{u\in\Omega_0'} f_u$. By part 1 of Lemma 6.4.2, S is a continuous ring homomorphism and as in the case of the norm is Ω_0 invariant, then by Theorem 6.4.1 we can take $\mathrm{Tr}_K = S \circ ([p]^*)^{-1}$, which is a continuous endomorphism of $\mathcal{O}_K[[T]]$ satisfying (6.4). By part 3 of Remark 6.3.2 and Remark 6.4.2 we have that

$$\big(\sigma \cdot \mathrm{Tr}_K f\big)([p]) = \big(\mathrm{Tr}_K f([p])\big)([\kappa(\sigma)]) = \left(\sum_{u\in\Omega_0} f_u\right)[\kappa(\sigma)] = \sum_{u\in\Omega_0} \sigma\cdot(f_u) = \sum_{u\in\Omega_0} (\sigma\cdot f)_u.$$

Therefore $\big(\sigma \cdot \mathrm{Tr}_K f\big)([p]) = \big(\mathrm{Tr}_K(\sigma\cdot f)\big)([p])$ hence $\sigma\cdot \mathrm{Tr}_K f = \sigma\cdot(\mathrm{Tr}_K f)$. □

Remark 6.4.3

1. *Since* Tr_K *leaves* $\mathcal{O}_K[[T]]$ *is invariant,* Tr_K *is a continuous* $\mathcal{O}_K[[G_\infty]]$*-endomorphism of* $\mathcal{O}_K[[T]]$.

2. *Let* $\eta_n = \zeta_{p^{n+1}} - 1$. *As well as in the case of the norm we have*

   (a) $\mathrm{Tr}_K f(\eta_n) = \mathrm{Tr}_{K_{n+1}/K_n}\big(f(\eta_{n+1})\big)$.

   (b) *For* $f \in \mathcal{O}_K[[T]]$, $\mathrm{Tr}_K^n(f) \equiv 0 \bmod p^n\mathcal{O}_K[T]$.

3. *For* $g(T) \in \mathcal{O}_K[[T]]$ *then* $\mathrm{Tr}_K(g[p]) = p\,g$. *Just note that since* $h = g([p])$ *is* Ω_0 *invariant,* $\mathrm{Tr}_K(h)([p]) = ph$. *Therefore, by definition of* Tr_K, $\mathrm{Tr}_K(h) = p\,g(T)$.

Proposition 6.4.2 *For* $f \in \mathfrak{M}_K$ *we have* $\mathrm{Tr}_K(\log f) = \log(\mathrm{Nr}_K f)$.

Let $f = 1 + g \in \mathfrak{M}_K' = 1 + T\mathcal{O}_K[[T]]$. Then $f([p]) = 1 + g([p])$ and $f_u = 1 + g(u[+]T) \in \mathfrak{M}_K'$, hence by part 2 of Corollary 2.1.1 we have

$$\log(f_u) = \lambda\big(g(u[+]T)\big) = \big(\lambda(g)\big)(u[+]T) = \log(f)_u,$$

$$\log(f[p]) = \lambda\big(g([p])\big) = \big(\lambda(g)\big)([p]) = \log(f)([p]).$$

Therefore

$$\begin{aligned} [p]^*(\log\, \mathrm{Nr}_K f) &= \log\big((\mathrm{Nr}_K f)([p])\big) = \log \prod_{u\in\Omega_0} f_u = \sum_{u\in\Omega_0} \log(f_u) \\ &= \sum_{u\in\Omega_0} (\log f)_u = \big(\mathrm{Tr}_K(\log f)\big)([p]) = [p]^*(\mathrm{Tr}_K \log f), \end{aligned}$$

Since $[p]^*$ is injective we must have that $\mathrm{Tr}_K(\log f) = \log(\mathrm{Nr}_K f)$. Now the general case follows from the fact that $\mathrm{Nr}_K, \mathrm{Tr}_K$ and log are $\mathbb{Z}_p$-homomorphisms. □

Let us consider the extension of the Frobenius $\varphi : K((T))_1 \longrightarrow K((T))_1$ given by its action on coefficients i.e.

$$\varphi\left(\sum a_n T^N\right) = \sum \varphi(a_n) T^N.$$

Remark 6.4.4

1. *φ is a ring homomorphism and $\varphi(f) \equiv f^p \bmod p$.*

2. *Since $\Delta = \mathrm{Gal}\big(K/\mathbb{Q}_p\big) \cong \mathrm{Gal}\big(K_\infty/\mathbb{Q}_{p^\infty}\big)$ (the isomorphism is given by restriction) we can lift $\varphi \in \mathrm{Gal}\big(K_\infty/\mathbb{Q}_{p^\infty}\big)$, which acts as the usual φ on K and trivially on all p-th roots of unity.*

3. *Since for every $a \in \mathcal{O}_K$, $|\varphi(a)| = |a|$ we have that $\|\varphi(f)\|_r = \|f\|_r$ for any $r \in p^{\mathbb{Q}^-}$, in particular φ is continuous.*

4. *φ commutes with evaluations i.e. if $f \in \mathcal{O}_K((T))$ and $g \in T\,\mathcal{O}_K[[T]]$ then $\varphi\big(f(g)\big) = \big(\varphi f\big)(\varphi g)$. This follows by Proposition 5.4.2 and the continuity of φ (since it is true when f, g are polynomials).*

5. *φ commutes with Nr_K. Since φ is a ring isomorphism we have*

$$\varphi\big(\mathrm{Nr}_K(f)([\,p\,])\big) = \prod_{u \in \Omega_0} \varphi(f_u) = \prod_{u \in \Omega_0} \varphi(f)_u = \mathrm{Nr}_K\big(\varphi(f)\big)([\,p\,]),$$

   because $\varphi(f_u) = \varphi(f(u[+]T)) = \varphi(f)(u[+]T) = \varphi(f)_u$. On the other hand

$$\varphi\big(\mathrm{Nr}_K(f)([\,p\,])\big) = \big(\varphi(\mathrm{Nr}_K f)\big)([\,p\,]),$$

   then by Lemma 6.4.2 we have $\mathrm{Nr}_K\,\varphi(f) = \varphi\,\mathrm{Nr}_K(f)$.

Lemma 6.4.4 *Let $n \geq 1$, $g \equiv 1 \bmod p^n\mathcal{O}_K[[T]]$ and $h \in \mathfrak{M}_K$, then:*

1. *Let $f \in \mathcal{O}_K[[T]]$. If $f([\,p\,]) \in p^N\mathcal{O}_K[[T]]$ then $f \in p^N\mathcal{O}_K[[T]]$.*

2. *$\mathrm{Nr}_K(g) \equiv 1 \bmod p^{n+1}\mathcal{O}_K[[T]]$*

3. *$\dfrac{\mathrm{Nr}_K^n(h)}{\varphi\big(\mathrm{Nr}_K^{n-1}(h)\big)} \equiv 1 \bmod p^n\mathcal{O}_K[[T]]$ i.e.*

$$\varphi^{-n}\,\mathrm{Nr}_K^n(f) \equiv \varphi^{-(n-1)}\,\mathrm{Nr}_K^{n-1}(f) \bmod p^k.$$

Proof. (1) Let $f = \sum a_n T^n$. Since $[\,p\,] \equiv T^p \bmod p$, if $f([\,p\,]) \in p\mathcal{O}_K[[T]]$ then $f([\,p\,]) = \sum a_n [\,p\,]^n \equiv \sum a_n T^{np} \equiv 0 \bmod p$, therefore $f \in p\mathcal{O}_K[[T]]$. Now if $f([\,p\,]) \in p^N\mathcal{O}_K[[T]]$, taking $h = \frac{1}{p^{N-1}} f$ we have that $h([\,p\,]) \in p\mathcal{O}_K[[T]]$ then, by the previous case $h \in p\mathcal{O}_K[[T]]$, therefore $f \in p^N\mathcal{O}_K[[T]]$.

(2) By part 1 it is enough to show that $F(g) \equiv 1 \bmod p^{n+1}$. For this take $u \in \Omega_0 \subseteq \mathfrak{p}_0$, then $u[+]T \equiv T \bmod \mathfrak{p}_0$ and $g_u = g(u[+]T) \equiv g \bmod p^n\mathfrak{p}_0$. Therefore $F(g) \equiv g^p \equiv 1 \bmod p^n\mathfrak{p}_0$ but this means that the coefficients of $F(g) - g^p$ lie in $p^n\mathfrak{p}_0 \cap \mathcal{O}_K = p^{n+1}\mathcal{O}_K$ i.e. $F(g) \equiv 1 \bmod p^{n+1}$ and by part 1 $\mathrm{Nr}_K(g) \equiv 1 \bmod p^{n+1}$.

(3) First let us prove the case $n = 1$: Without loss of generality we may suppose that $h = \sum a_n T^n \in \mathcal{O}_K[[T]]$, because if $h = h_0 T^{-N}$ for some $N > 0$ and $h_0, T^N \in \mathcal{O}_K[[T]]$ then with our assumption we have:

$$\frac{\mathrm{Nr}_K(h)}{\varphi(h)} = \left(\frac{\mathrm{Nr}_K(T^N)}{\varphi(T^N)}\right)^{-1} \frac{\mathrm{Nr}_K(h_0)}{\varphi(h_0)} \equiv \frac{\mathrm{Nr}_K(h_0)}{\varphi(h_0)} \bmod p.$$

Now, $\varphi(h) \equiv \sum_n a_n^p T^n$ and $h^p \equiv \sum_n a_n^p T^{np} \bmod p$, then $\varphi(h)(T^p) \equiv h^p \bmod p$. On the other hand $F(h) \equiv h^p \bmod \mathfrak{p}_0$, and since both series have integral coefficients we must have that $F(h) \equiv h^p \bmod p$, then $\mathrm{Nr}_K(h)(T^p) \equiv h^p \bmod p$. Therefore

$$\frac{\mathrm{Nr}_K(h)(T^p)}{\varphi(h)(T^p)} \equiv 1 \bmod p,$$

then, looking at the coefficients, it is easy to see that $\dfrac{\mathrm{Nr}_K(h)}{\varphi(h)} \equiv 1 \bmod p$.

Now let $g_1 = \dfrac{\mathrm{Nr}_K(h)}{\varphi(h)}$ and $g_{n+1} = \mathrm{Nr}_K(g_n)$ for $n > 1$. We have seen that $g_1 \equiv 1 \bmod p$ and since the norm and φ are multiplicative we have that

$$g_n = \frac{\mathrm{Nr}_K^n(h)}{\varphi\big(\mathrm{Nr}_K^{n-1}(h)\big)},$$

then by part 2 is easy to conclude that $g_n \equiv 1 \bmod p^n$. □

From part 3 of last Lemma we have that

$$\varphi^{-k}\,\mathrm{Nr}_K^k(f) \equiv \varphi^{-(k-1)}\,\mathrm{Nr}_K^{k-1}(f) \bmod p^k,$$

hence we are able to define

Definition 6.4.1 *Let us define* $\mathrm{Nr}_K^\infty : \mathfrak{M}_K \longrightarrow \mathfrak{M}_K$ *as* $\mathrm{Nr}_K^\infty(f) = \lim_{n\to\infty} \varphi^{-n}\,\mathrm{Nr}_K^n(f)$ *and* $\mathfrak{M}_K^\varphi$ *as the set of* $f \in \mathfrak{M}_K$ *such that* $\mathrm{Nr}_K(f) = \varphi f$.

Remark 6.4.5

1. *From definition* $\mathrm{Nr}_K\big(\mathrm{Nr}_K^\infty(f)\big) = \varphi\big(\mathrm{Nr}_K^\infty(f)\big)$.
2. *If* $f \in \mathfrak{M}_K^\varphi$ *then* $\mathrm{Nr}_K^\infty f = f$, *therefore* Nr_K^∞ *maps* $\mathfrak{M}_K$ *onto* $\mathfrak{M}_K^\varphi$.
3. *Since* $\mathrm{Nr}_K^\infty(f) \equiv f \bmod p\mathcal{O}_K[[T]]$, *we have that* $\mathfrak{M}_K^\varphi \subseteq \mathfrak{M}_K$.
4. *Since* Nr_K *and* φ *are continuous we have that* $\mathfrak{M}_K^\varphi$ *is closed. Further, since* $\mathfrak{M}_K$ *is compact we have that* $\mathfrak{M}_K^\varphi$ *is compact.*

Proposition 6.4.3 $\mathrm{Nr}_K^\infty : \mathfrak{M}_K \longrightarrow \mathfrak{M}_K^\varphi$ *is a continuous a* Λ_K*-homomorphism.*

Proof. Since Nr_K and φ are Λ_K-homomorphisms and the continuity of the Λ_K-action on $\mathfrak{M}_K$, by definition of N^∞, it is must be a Λ_K-homomorphism. Hence it is enough to check the continuity in 1. For this take a sequence $(f_n)_{n\in\mathbb{N}} \subseteq \mathfrak{M}_K$ convergent to 1, then for $N \in \mathbb{N}$ there exist $n_0 \in \mathbb{N}$ such that for $n \geq n_0$ $f_n \equiv 1 \bmod p^N \mathcal{O}_K[[T]]$ therefore by part 2 of Lemma 6.4.4 and definition of Nr_K^∞ we have that

$$\mathrm{Nr}_K^\infty(f_n) \equiv \varphi^{-N}\,\mathrm{Nr}_K^N(f_n) \equiv 1 \bmod p^N \mathcal{O}_K[[T]].$$

But, this means that $\lim_{n\to\infty} \mathrm{Nr}_K^\infty(f_n) = 1$. □

Proposition 6.4.4 *Let* $\mathfrak{M}'_K = 1 + p\mathcal{O}_K[[T]]$*. The sequence*

$$1 \longrightarrow \mathfrak{M}'_K \longrightarrow \mathfrak{M}_K \underset{i}{\overset{\mathrm{Nr}_K^\infty}{\rightleftarrows}} \mathfrak{M}_K^\varphi \longrightarrow 1$$

is a split exact sequence of topological Λ_K*-modules, where* i *is the inclusion.*

Proof. We only need to prove that $\ker \mathrm{Nr}_K^\infty = \mathfrak{M}'_K 1$. By part 3 of Remark 6.4.5 we have that $\ker \mathrm{Nr}_K^\infty \subseteq \mathfrak{M}'_K$. For the other inclusion take $f \in \mathfrak{M}'_K$. Note that iterating part 2 of Lemma 6.4.4 we get $\mathrm{Nr}_K^k(f) \equiv 1 \bmod p^k \mathcal{O}_K[[T]]$, therefore $\mathrm{Nr}_K^\infty(f) = 1$ i.e. $f \in \ker \mathrm{Nr}_K^\infty$. □

6.5 Local units and the Coleman Homomorphism

Let $U^{(n)}$ be the principal units of K_n i.e. $U^{(n)} = 1 + \mathfrak{p}_n$.

Remark 6.5.1

1. *Notice that for* $m \leq n$, $\mathrm{Nr}_K\, knm(U^{(n)}) \subseteq U_m$*. Further, since for* $l \leq m \leq n$ *we have* $\mathrm{Nr}_K\, kml\, \mathrm{Nr}_K\, knm = \mathrm{Nr}_K\, knl$*, then the principal units constitute an inverse system with respect to norms.*

2. *Each* G_n *acts naturally on* $U^{(n)}$ *and, as in Corollary 6.2.1, we may define in* $U^{(n)}$ *a canonical continuous* $\mathbb{Z}_p$*-action, therefore we have a continuous* $\mathbb{Z}_p[G_n]$*-action.*

3. *Note that the canonical morphisms* $\mathbb{Z}[G_\infty] \longrightarrow \mathbb{Z}[G_n]$ *induce continuous* $\mathbb{Z}_p[G_\infty]$*-action on each* $U^{(n)}$*. Therefore each of them can be extended to a continuous* Λ_K*-actions on the respective* $U^{(n)}$*.*

4. *For* $m \leq n$ *the* $\mathbb{Z}_p[G_\infty]$*-actions on* $U^{(n)}$ *and* U_m *are compatible with* $\mathrm{Nr}_{K_n/K_m} : U^{(n)} \longrightarrow U_m$ *then, by continuity of the norms, they are compatible the respective* Λ_K*-actions, therefore we can induce a canonical topological* Λ_K*-action on* $\varprojlim U^{(n)}$*.*

Definition 6.5.1 *We define the* **group of local units** $\mathscr{U}_K$ *as* $\varprojlim U^{(n)}$ *with the canonical* Λ_K*-module structure.*

Lemma 6.5.1 *Let* $\eta_n = \zeta_{p^{n+1}} - 1$. *For every* $(\alpha_n)_{n\in\mathbb{N}} \in U^1_{K,\infty}$ *there is a unique* $g \in \mathcal{O}_K[[T]]$ *such that* $g(u_n) = \varphi^n(\alpha_n)$.

Proof. The uniqueness follows immediately by the Corollary 4.2.2. For the existence, first note that φ leaves $\mathfrak{p}$ invariant, the $\varphi^n(\alpha_n) \in U^{(n)}$. Now since η_n is prime in $\mathcal{O}_n$, there exists $f_n \in \mathcal{O}_K[[T]]$ such that

$$f_n(\eta_n) = \varphi^n(\alpha_n)$$

Now, for any $n, k \in \mathbb{N}$ by Remark 6.4.1 we have

$$\big(\varphi^{-k}\operatorname{Nr}_K^k f_{n+k}\big)(\eta_n) = \varphi^{-k}\operatorname{Nr}_K kn + kn\big(f_{n+k}(\eta_{n+k})\big) = \varphi^n(\alpha_n). \tag{6.5}$$

Let $g_n = \varphi^{-n}\operatorname{Nr}_K^n(f_{2n})$ and $m = n + j$ with $j \geq 0$, note that by (6.5) we have

$$(\varphi^{-j}\operatorname{Nr}_K^j g_m)(\eta_n) = \varphi^{-m-j}\operatorname{Nr}_K^{m+j} f_{2m}(\eta_n) = \varphi^n(\alpha_n),$$

and by 3 of Lemma 6.4.4

$$\varphi^{-j}\operatorname{Nr}_K^j g_m = \varphi^{-m-j}\operatorname{Nr}_K^{m+j} f_{2m} \equiv \varphi^{-m}\operatorname{Nr}_K^m f_{2m} \bmod p^{m+1},$$

then for $m = n + j$, $\varphi^n(\alpha_n) = (\varphi^{-j}\operatorname{Nr}_K^j g_m)(\eta_n) \equiv g_m(\eta_n) \bmod p^{m+1}$, then

$$|\varphi^n(\alpha_n) - g_m(\eta_n)| \leq \frac{1}{p^{m+1}}. \tag{6.6}$$

Finally, $(g_m)_{m\in\mathbb{N}} \subseteq \mathcal{O}_K[[T]]$ (compact by Corollary 5.3.1) admits an accumulation point $g \in \mathcal{O}_K[[T]]$, then by (6.6) $g(\eta_n) = \varphi^n(\alpha_n)$. □

Theorem 6.5.1 *There is a topological* Λ_K*-isomorphism* $\mathfrak{Col}_K : U^1_{K,\infty} \longrightarrow \mathfrak{M}^\varphi_K$ *such that for* $u = (u_n)_{n\in\mathbb{N}} \in U^1_{K,\infty}$ *we have*

$$\big(\mathfrak{Col}_K(u)\big)(\eta_n) = \varphi^n(u_n).$$

Proof. Let $\phi_n : \mathfrak{M}^\varphi \longrightarrow U^{(n)}$ defined as $\varphi_n(f) = \varphi^{-n} f(\omega_n)$. By part 2 of Remark 6.3.2 the ϕ_n are $\mathbb{Z}_p[G_\infty]$-morphisms and by Proposition and the continuity of φ, they are continuous. Therefore they are topological Λ_K-morphisms. Now iterating part 2 of Remark 6.4.1, we have $\operatorname{Nr}_K^k(f)(\omega_n) = \operatorname{Nr}_{K_{n+k}/K_n} f(\omega_{n+k})$ therefore for $n = m + k$ and $f \in \mathfrak{M}^\varphi_K$ we have

$$\begin{aligned} \phi_m(f)(\omega_m) &= \varphi^{-m}\operatorname{Nr}_K^m \varphi^{-k}\operatorname{Nr}_K^k(f)(\omega_m) = \varphi^{-n}\operatorname{Nr}_K^{m+k}\operatorname{Nr}_{K_{m+k}/K_m}(f)(\omega_{m+k}) \\ &= \operatorname{Nr}_{K_n/K_m}\varphi^{-n}\operatorname{Nr}_K^n(f)(\eta_n) = \operatorname{Nr}_{K_n/K_m}\phi_m(f)(\omega_m), \end{aligned}$$

then the following diagram commutes:

$$\begin{array}{ccc} \mathfrak{M}_K^{\varphi} & \xrightarrow{\phi_n} & U^{(n)} \\ & \searrow^{\phi_m} & \downarrow \mathrm{Nr}_{K_n/K_m} \\ & & U_m \end{array}$$

Then they define a continuous Λ_K-morphism, $\varphi : \mathfrak{M}_K^{\varphi} \longrightarrow U^1_{K,\infty}$ which is injective by the uniqueness lemma (Lemma 2.3.3), surjective by last lemma. Since $\mathfrak{M}_K^{\varphi}$ is compact φ is a topological Λ_K-isomorphism, therefore so does $\Gamma_K = \phi^{-1}$. □

Lemma 6.5.2 *Let* $\Theta : T\mathcal{O}_K[[T]] \longrightarrow K[[T]]_1$ *defined as* $\Theta(f) = f - \dfrac{\Phi(f)}{p}$ *where*

$$\Phi(f) = \varphi(f)\big((1+T)^p - 1\big).$$

For any $f \in T\,O_K[[T]]$ *we have that* $\Theta\big(\lambda(f)\big) \in \mathcal{O}_K[[T]]$.

Proof. Since for each $n \geq 1$ factors uniquely as $n = p^k a$ with $k \geq 0$ and $(a,p) = 1$ we have $\lambda(f) = \sum_{n=1}^{\infty}(-1)^{n+1}\dfrac{f^n}{n} = \sum_{(a,p)=1}(-1)^{a+1}\dfrac{1}{a}\sum_{k=0}^{\infty}\dfrac{(f^a)^{p^k}}{p^k}$, Since $\mathcal{O}_K[[T]]$ is closed, is enough to show that for any $f \in \mathcal{O}_K[[T]]$,

$$\Theta\left(\sum_{k=0}^{\infty}\frac{f^{p^k}}{p^k}\right) \in \mathcal{O}_K[[T]].$$

For this purpose we need the following claim:

Claim: For $f \in \mathcal{O}_K[[T]]$ and $k \in \mathbb{N}$ we have $\Phi(f^{p^k}) \equiv f^{p^{k+1}} \bmod p^{k+1}$.
Let g be defined by $[\,p\,] = T^p + pg$ and $f = \sum a_n T^n$. Since

$$\Phi(f) = \varphi f([\,p\,]) = \sum \varphi(a_p)(T^p + pg)^n \equiv \sum a_n^p T^{np} \equiv f^p \bmod p,$$

the claim is true for $k = 0$. Now, for a $k \geq 0$ assume that $\Phi(f^{p^k}) = f^{p^{k+1}} + p^{k+1}h_k$ with $h_k \in \mathcal{O}_K[[T]]$, therefore

$$\Phi(f^{p^{k+1}}) = \varphi f^{p^{k+1}}([\,p\,]) = \Phi\big(f^{p^k}\big)^p = (f^{p^{k+1}} + p^{k+1}h_k)^p = f^{p^{k+2}} + p^{k+2}h_{k+2},$$

for some $h_{k+2} \in \mathcal{O}_K[[T]]$, hence the claim is true for $k+1$.

We can restate the claim in the following way: for every $k \in \mathbb{N}$ we have that

$$\frac{f^{p^{k+1}}}{p^{k+1}} - \Phi\frac{f^{p^k}}{p^k} \in \mathcal{O}_K[[T]].$$

this means that for each $N \geq 1$ there is a $g_N \in \mathcal{O}_K[[T]]$ such that

$$\Theta\Big(\sum_{k=0}^{N} \frac{f^{p^k}}{p^k}\Big) = \sum_{k=0}^{N} \frac{f^{p^k}}{p^k} - \sum_{k=0}^{N} \Phi \frac{f^{p^k}}{p^k} f = g_N - \Phi \frac{f^{p^N}}{p^N}.$$

Since $\lim_{N \to \infty} \dfrac{f^{p^N}}{p^N} = 0$ and φ and $[\,p\,]$ are continuous we have that Θ is continuous and $\Theta\Big(\sum_{k=0}^{\infty} \frac{f^{p^k}}{p^k}\Big) = \lim_{N \to \infty} \Theta\Big(\sum_{k=0}^{N} \frac{f^{p^k}}{p^k}\Big) = \lim_{N \to \infty} g_N \in \mathcal{O}_K[[T]]$. □

Lemma 6.5.3 *The map $\Theta_\Omega : \mathfrak{M}_K \longrightarrow \mathcal{O}_K[[T]]$ defined as*

$$\Theta_\Omega(f) = \Theta(\log f),$$

is a continuous Λ_K-homomorphism.

Proof. Since log and $[\,p\,]_*$ are continuous Λ_K homomorphism, so it is Θ_Ω. Therefore it only remains to check the integrability of its image. For this let $g \in T\,\mathcal{O}_K[[T]]$, by Lemma 6.5.2 we have that $\Theta_\Omega(1+g) = \Theta(\lambda(g)) \in \mathcal{O}_K[[T]]$. Now for $f \in \mathfrak{M}_K$ we may write $f = a(1+g)$ where $a = 1 + h(p)$ with $h \in T\mathbb{Z}_p[[T]]$ and $g \in T\,\mathcal{O}_K[[T]]$, then

$$\Theta_\Omega(f) = \Theta \log(1 + h(p)) + \Theta \log(1+g) = \Theta\big(\lambda(h)\big)(p) + \Theta\big(\lambda(g)\big) \in \mathcal{O}_K[[T]].$$

□

For the following we will need an integral version of the normal basis theorem:

Lemma 6.5.4 *Let $E/\mathbb{Q}_p$ a finite Galois unramified extension of degree f. Then there exists a $\theta \in \mathcal{O}_E$ such that $\theta, \varphi(\theta), \ldots, \varphi^{f-1}(\theta)$ is a $\mathbb{Z}_p$-basis of $\mathcal{O}_K$.*

Proof. Let $\overline{\theta} \in k_E$ a normal primitive element $k_E/\mathbb{F}_p$ i.e. an element such that $\overline{\theta}, \overline{\theta}^p, \ldots, \overline{\theta}^{p^{f-1}}$ is a $\mathbb{F}_p$ basis of k_E. Fix $\theta \in \mathcal{O}_E$ a lifting of $\overline{\theta}$, then the set

$$R = \{b_1\theta + b_2\varphi(\theta) + \ldots + b_f\varphi^{f-1}(\theta) \mid 0 \leq b_i \leq p-1\},$$

is a system of representative of k_E in $\mathcal{O}_E$. Since p is a uniformizer of $\mathfrak{p}_E$, for each $a \in \mathcal{O}_E$ we have that $a = \sum_{j=0}^{\infty} a_j p^j$ with $a_j \in R$, hence $a_j = \sum_{k=0}^{f-1} b_{j,k}\varphi^k(\theta)$ with $0 \leq b_{j,k} \leq p-1$. Therefore $a = \sum_{k=0}^{f-1}\Big(\sum_{j=0}^{\infty} b_{j,k}p^j\Big)\varphi^k(\theta)$ then

$$\mathcal{O}_K = \mathbb{Z}_p\theta + \mathbb{Z}_p\varphi(\theta) + \ldots + \mathbb{Z}_p\varphi^{f-1}(\theta).$$

Now if $\sum_{k=0}^{f-1} \alpha_k\varphi^k(\theta) = 0$ for $\alpha_k \in \mathbb{Z}_p$ we may assume that at least one $\alpha_k \in \mathbb{Z}_p^\times$, but reducing mod p it contradicts the fact that $\overline{\theta}, \overline{\theta}^p, \ldots, \overline{\theta}^{p^{f-1}}$ are a $\mathbb{F}_p$ basis of k_E, therefore

$\theta, \varphi(\theta) \ldots, \varphi^{f-1}(\theta)$ must be linearly independent over $\mathcal{O}_K$. $\square$

Lemma 6.5.5 *Let $b \in K$ and $n \in \mathbb{Z}$. Consider the equation in K:*

$$b = a - \varphi(a)p^n \tag{6.7}$$

1. *If $n \neq 0$ then the equation has always unique solution.*

2. *If $n = 0$ the equation is solvable if and only if $\mathrm{Tr}_{K/\mathbb{Q}_p}(b) = 0$.*

3. *If $n \neq 0$ the equation has a solution in $\mathbb{Q}_p$ if and only if $b \in \mathbb{Q}_p$.*

Proof. By last lemma there is a $\theta \in K$ such that $\theta, \varphi(\theta) \ldots, \varphi^{f-1}(\theta)$ is a $\mathbb{Z}_p$-basis of $\mathcal{O}_K$, therefore a $\mathbb{Q}_p$-basis of K. Let $b = \sum_{k=0}^{f-1} b_k \varphi^k(\theta)$ and $a = \sum_{k=0}^{f-1} a_k \varphi^k(\theta)$. By linear independence equation (6.7) is equivalent to the system of equations in $\mathbb{Q}_p$

$$b_k = a_k - a_{k-1}p^n \text{ for } 0 \leq k \leq f-1 \text{ where } a_{-1} = a_{f-1}.$$

In matrix notation:

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & -p^n \\ -p^n & 1 & 0 & \cdots & 0 & 0 \\ 0 & -p^n & 1 & \cdots & 0 & 0 \\ 0 & 0 & -p^n & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & -p^n & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{f-1} \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{f-1} \end{pmatrix}$$

(1) Since the matrix of the system has determinant $1 - p^{n(f-1)}$ for $n \neq 0$ the system is always solvable.
(2) For the case $n = 0$ if the equation has solution we must have $\sum_k b_k = 0$ and since the matrix has rank $n - 1$ then the equation has solution if and only if $\sum b_k = 0$. Now, $\mathrm{Tr}_{K/\mathbb{Q}_p}(b) = \sum_{k=0}^{f-1} b_k \mathrm{Tr}_{K/\mathbb{Q}_p}(\theta)$, hence the existence of a solution is equivalent to $\mathrm{Tr}_{K/\mathbb{Q}_p}(b) = 0$.
(3) It follows from the fact that the matrix preserve the space of vectors $(a_0, a_1, \ldots, a_{f-1}) \in \mathbb{Q}_p^f$ such that $a_k = 0$ for $k \neq 0$. $\square$

As before, let $c_1 : K[[T]] \longrightarrow K$ the first coefficient projection i.e. $c_1(f) = f'(0)$.

Lemma 6.5.6 $\Theta(K[[T]]) = \ker(\mathrm{Tr}_{K/\mathbb{Q}_p} \circ c_1)$.

Proof. Note that for $f = \sum a_n T^n \in K[[T]]$ we have

$$\Theta(f) = \sum \Theta(a_k T^k) = \left(a_0 - \frac{\varphi(a_0)}{p}\right) + \big(a_1 - \varphi(a_1)\big)T + \sum_{k\geq 2}\left(a_k T^k - \frac{\varphi(a_k)[\,p\,]^k}{p}\right). \quad (6.8)$$

Note that for $n \geq 2$ the n-th term of $\Theta(f)$ is given by

$$c_n(\Theta(f)) = a_n - \frac{1}{p}\sum_{k\geq 2}\varphi(a_k)c_n\big([\,p\,]^k\big), \quad (6.9)$$

and since $[\,p\,] = \sum_{j=1}^{p-1}\binom{p}{j}T^j$ then $[\,p\,]^k = \sum_{j_1,\dots,j_k=1}^{p-1}\binom{p}{j_1}\cdots\binom{p}{j_k}T^{j_1+\dots+j_k}$ therefore for $k \leq n \leq k(p-1)$ we have

$$c_n\big([\,p\,]^k\big) = \sum_{\substack{j_1+\dots+j_k=p-1\\ 1\leq j_i\leq p-1}}\binom{p}{j_1}\cdots\binom{p}{j_k} = \begin{cases} p^n & \text{if } n = k \\ 0 \bmod p & \text{if } k < n \leq k(p-1)\end{cases}$$

and 0 otherwise. So in equation (6.9) we get for $n \geq 2$:

$$c_n(\Theta(f)) = a_n - \varphi(a_n)p^{n-1} - \frac{1}{p}\sum_{\frac{n}{p-1}\leq k<n}\varphi(a_k)c_n\big([\,p\,]^k\big). \quad (6.10)$$

Now given $g = \sum b_n T^n \in K[[T]]$, for solving the equation $\Theta(f) = g$, with $f = \sum_n a_n T^n$ by (6.8) and (6.10), we need to solved simultaneously the system:

$$b_0 = a_0 - \frac{\varphi(a_0)}{p},\ b_1 = a_1 - \varphi(a_1) \text{ and } b_n' = a_n - \varphi(a_n)p^{n-1} \text{ for } n \geq 2.$$

where $b_n' = b_n + \frac{1}{p}\sum_{\frac{n}{p}\leq k<n}\varphi(a_k)c_n\big([\,p\,]^k\big)$ which is well determined when we know a_k for $k < n$. By Lemma 6.5.5 the only condition we need is that $\mathrm{Tr}_{K/\mathbb{Q}_p}(a_1) = 0$, therefore that $f \in \ker(\mathrm{Tr}_{K/\mathbb{Q}_p}\circ c_1)$. □

Theorem 6.5.2 *The following sequence of topological Λ_K-modules is exact:*

$$1 \longrightarrow \mathbb{Z}_p(1) \xrightarrow{\alpha_K} \mathfrak{M}_K \xrightarrow{\Theta_\Omega} \mathcal{O}_K[[T]] \xrightarrow{\beta_K} \mathbb{Z}_p(1) \longrightarrow 1\ ,$$

where $\alpha_K(a\cdot\zeta) = (1+T)^a$, $\beta_K(f) = \mathrm{Tr}_{K/\mathbb{Q}_p} f'(0)\cdot\zeta$ and $\zeta = (\zeta_{p^{n+1}})_{n\in\mathbb{N}}$.

Proof. It is clear that α_K is injective and β_K is surjective. By Lemma 6.5.2 we have that $\Theta_\Omega(\mathfrak{M}_K) \subseteq \mathcal{O}_K[[T]]$ and by Lemma 6.5.6 its image is exactly $\ker\beta_K$. Then we only need to check exactness at $\mathfrak{M}_K$. Since $\log(1+T)^a = a\lambda$ and $\Theta(a\lambda) = a\Theta(\lambda) = \lambda - \frac{\lambda([\,p\,])}{p} = 0$ we have that $\Theta_\Omega\alpha_K = 0$. It remains to prove the other inclusion. For that take $g = uf \in \mathfrak{M}_K$ with $f \equiv 1 + a_1T \bmod T^2$, then $\log g = \log u + a_1T + \sum_{k=2}^{\infty}a_kT^k$. If $\Theta_\Omega(g) = 0$ by equation (6.8) we have that:

1. $(p-1)\log u = \log u - \dfrac{\log u}{p} = 0$, hence $\log u = 0$ i.e. $u = 1$.
2. $a_1 = \varphi(a_1)$, hence $a_1 \in \mathbb{Z}_p$.
3. For $k \geq 1$, if $a_1, \dots, a_k \in \mathbb{Q}_p$ by equation (6.9) we get $a_{k+1} \in \mathbb{Q}_p$.

Therefore $f = g \in \mathbb{Q}_p[[T]]$. Now let $h = \log f - a_1\lambda$ then $h \equiv 0 \bmod T^2$ and $\Theta(h) = 0$ i.e. $p\,h(T) = h([p])$. Since

$$h \equiv 0 \bmod T^k \Longrightarrow h([\,p\,]) = 0 \bmod T^{pk},$$

we must have $h = 0$, then $\log f = a_1\lambda$ i.e. $f = (1+T)^{a_1} = \alpha_K(\zeta^{a_1})$. □

Lemma 6.5.7 *$\mathcal{O}_K[[T]] = \mathcal{O}_K[[G_\infty]] \cdot (1+T) + \mathcal{O}_K[[T]]^{\Omega_0}$ as $\mathcal{O}_K[[G_\infty]]$-modules.*

Proof. First, note that by Theorem 6.4.1 we have that

$$\mathcal{O}_K[[T]]^{\Omega_0} = [\,p\,]^*(\mathcal{O}_K[[T]]) = \{g([\,p\,]) \mid g \in \mathcal{O}_K[[T]]\}.$$

Now, let $a \in \mathbb{N}$. If a is prime to p, take $\sigma_a \in G_\infty$ such that $\kappa(\tau_a) = a$, then

$$\sigma_a \cdot (1+T) = (1+T)^a \in \mathcal{O}_K[[G_\infty]] \cdot (1+T),$$

is a monic polynomial of degree a. If $a = pb$ we have that

$$[\,p\,]^a = \big((1+T)^p - 1\big)^a \in \mathcal{O}_K[[T]]^{\Omega_0}$$

is a monic polynomial of degree pa. Therefore the $\mathcal{O}_K[[G_\infty]]$-submodule $\mathcal{O}_K[[G_\infty]] \cdot (1+T) + \mathcal{O}_K[[T]]^{\Omega_0}$ contains monic polynomials of any degree, so must be dense in $\mathcal{O}_K[[T]]$, but since it is compact they coincide. □

Definition 6.5.2 *We define $\mathscr{V} = \ker \mathrm{Tr}_K = \{f \in \mathcal{O}_K[[T]] \mid \mathrm{Tr}_K f = 0\}$.*

Theorem 6.5.3 *$\mathscr{V}$ is a principal $\mathcal{O}_K[[G_\infty]]$-module generated by $1+T$.*

Proof. Let $h = \mathrm{Tr}_K(1+T)$. Since $h([\,p\,]) = \sum_{\zeta^p=1} \zeta(1+T) = 0$ we have $h = 0$, then $(1+T) \in \ker \mathrm{Tr}_K$ and since it is a $\mathcal{O}_K[[G_\infty]]$-module, $\mathcal{O}_K[[G_\infty]] \cdot (1+T) \subseteq \ker \mathrm{Tr}_K$. Now by part 3 of Remark 6.4.3 if $h = g([\,p\,]) \in \mathcal{O}[[T]]^{\Omega}$ we have $\mathrm{Tr}_K(h) = p\,g$, but it implies that

$$\mathcal{O}_K[[T]]^{\Omega_0} \cap \mathscr{V} = 0,$$

therefore $\mathcal{O}_K[[G_\infty]] \cdot (1+T) \cap \mathcal{O}_K[[T]]^{\Omega_0} = 0$. By last Lemma we get

$$\mathcal{O}_K[[T]] = \mathcal{O}_K[[G_\infty]] \cdot (1+T) \oplus \mathcal{O}_K[[T]]^{\Omega_0},$$

then we must have $\mathcal{O}_K[[G_\infty]] \cdot (1+T) = \mathscr{V}$. □

Theorem 6.5.4 *We have that* $\Theta_\Omega(\mathfrak{M}_K^\varphi) \subseteq \mathscr{V}$. *Further the sequence of Theorem 6.5.2 induces the following exact sequence of* $\mathcal{O}_K[[G_\infty]]$*-modules:*

$$1 \longrightarrow \mathbb{Z}_p(1) \xrightarrow{\alpha_K} \mathfrak{M}_K^\varphi \xrightarrow{\Theta_\Omega} \mathscr{V} \xrightarrow{\beta_K} \mathbb{Z}_p(1) \longrightarrow 1 \ .$$

Proof. Let $f \in \mathfrak{M}_K$. Taking trace of Θ_{Ω_0} we get

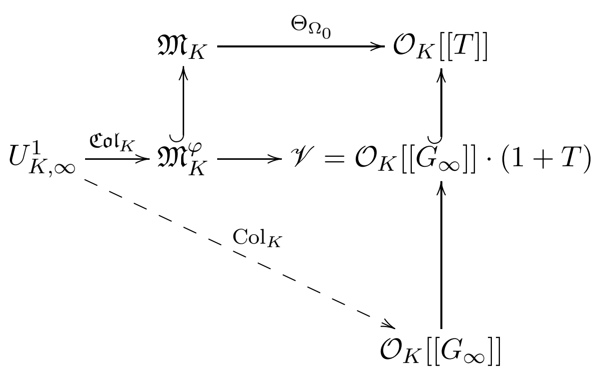
$$\operatorname{Tr}_K \Theta_{\Omega_0}(f) = \operatorname{Tr}_K(\log f) - \frac{1}{p}\varphi \operatorname{Tr}_K\big([\,p\,]^* \log f\big).$$

By part 3 of Remark 6.4.3 we have $\operatorname{Tr}_K\big([\,p\,]^* \log f\big) = p\,f$ and by Proposition 6.4.2 $\operatorname{Tr}_K(\log f) = \log(\operatorname{Nr}_K f)$ therefore

$$\operatorname{Tr}_K \Theta_{\Omega_0}(f) = \log(\operatorname{Nr}_K f) - \log(\varphi f) = \log\left(\frac{\operatorname{Nr}_K f}{\varphi f}\right). \tag{6.11}$$

Then $f \in \mathfrak{M}_K^\varphi$ if and only if $\operatorname{Tr}_K \Theta_{\Omega_0}(f) = 0$ i.e. $\Theta_{\Omega_0}(f) \in \mathscr{V}$. About the exactness, since $\alpha_K(\mathbb{Z}_p((1)) \subseteq \mathfrak{M}_K^\varphi$ the sequence is exact in $\mathfrak{M}_K^\varphi$. For $g \in \ker \beta_K$, there is a $f \in m_K$ such that $g = \Theta_{\Omega_0}(f)$ then by (6.11) $g \in \ker \beta_K \cap \mathscr{V}$ if and only if $f \in \mathfrak{M}_K^\varphi$, so the sequence is exact at $\mathscr{V}$, therefore it is exact. □

The following diagram summarizes much of the maps we have defined:



(6.12)

Since $\mathcal{O}_K[[G_\infty]]$ is compact, and the action on $1+T$ is injective and continuous, there exists a well defined continuous map $\operatorname{Col} : U^1_{K,\infty} \longrightarrow \mathcal{O}_K[[G_\infty]]$ characterized by the relation

$$\Theta_\Omega \mathfrak{Col}_K(u) = (1+T)^{\operatorname{Col}(u)}.$$

It will be useful in the next chapter.

Chapter 7

Coleman-Iwasawa-Tsuji Characterization of the p-adic L-functions

7.1 Coleman semi-local Theory for Abelian number fields

Proposition 7.1.1 *Let $K/\mathbb{Q}$ a finite extension and for $\mathfrak{p}|p$ let $(\mathcal{O}_K)_\mathfrak{p}$ be the completions of $\mathcal{O}_K$ at $\mathfrak{p}$. The projections $\mathcal{O}_K \longrightarrow (\mathcal{O}_K)_\mathfrak{p}$ induce a canonical isomorphism*

$$\mathcal{O}_K \otimes_\mathbb{Z} \mathbb{Z}_p \cong \prod_{\mathfrak{p}|p} (\mathcal{O}_K)_\mathfrak{p}.$$

Proof. Both $\mathbb{Z}_p$-modules are free and have the same $\mathbb{Z}_p$-rank since $(\mathcal{O}_K)_\mathfrak{p}$ has $\mathbb{Z}_p$-rank $e_\mathfrak{p} f_\mathfrak{p}$ and $n = \sum_{\mathfrak{p}|p} e_\mathfrak{p} f_\mathfrak{p}$. So it is enough to check that the canonical map is surjective, but this follows by the Chinese reminder theorem.
Let F be an abelian number field unramified at p and $\Delta = \mathrm{Gal}\big(F/\mathbb{Q}\big)$.

Remark 7.1.1

1. *Since Δ is abelian decomposition groups of each $\mathfrak{p}|p$ coincide, so we can set Δ_p as the common decomposition group.*

2. *Since $F/\mathbb{Q}$ is unramified at p we have a Frobenius element element $\varphi \in \Delta_p$, characterized as the automorphism of F which satisfies $\varphi(a) \equiv a^p \bmod \mathfrak{p}$, for all $\mathfrak{p}|p$ i.e.*

   $$\varphi(a) \equiv a^p \bmod p\mathcal{O}_F.$$

   Further φ is a generator of Δ_p.

If $\mathfrak{p}|p$ let us denote $F_\mathfrak{p}$ the completion of F at $\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_F)_\mathfrak{p}$ the ring of $\mathbb{Z}_p$ integral elements of $F_\mathfrak{p}$.

Definition 7.1.1 *We define the topological ring*

$$\widehat{\mathcal{O}}_F := \prod_{\mathfrak{p}|p} \mathcal{O}_\mathfrak{p} \cong \mathcal{O}_F \otimes_\mathbb{Z} \mathbb{Z}_p$$

endowed with the product topology.

From now on fix $\mathfrak{p}'|p$. For each $\mathfrak{p}|p$ the rings $\mathcal{O}_\mathfrak{p}$ and $\mathbb{Z}_p[\Delta]$ has natural structure of $\mathcal{O}_\mathfrak{p}[\Delta_p]$ modules, further since Δ/Δ_p permutes transitively all the primes above p we have that

$$\widehat{\mathcal{O}}_F \cong \prod_{\mathfrak{p}|p} \mathcal{O}_\mathfrak{p} \cong \mathcal{O}_{\mathfrak{p}'} \otimes_{\mathbb{Z}_p[\Delta_p]} \mathbb{Z}_p[\Delta]. \tag{7.1}$$

Last isomorphism describes the $\mathbb{Z}_p[\Delta_p]$-action on $\widehat{\mathcal{O}}_F$. Indeed this Δ-action explicitly can be describe in following way: Let $\mathscr{T}$ a set of representatives of Δ/Δ_p then for $\delta \in \Delta$ there is a unique decomposition $\delta = \tau\sigma$ where $\tau \in \mathscr{T}$ and $\sigma \in \Delta_p$. Therefore there is a well define action

$$\delta \cdot (a_\mathfrak{p})_{\mathfrak{p}|p} = \big(\tau(a_\mathfrak{q})\big)_{\mathfrak{p}|p} \in \widehat{\mathcal{O}}_F, \tag{7.2}$$

where $\mathfrak{q} = \sigma^{-1}(\mathfrak{p})$.

Lemma 7.1.1 *1. Let M a $\mathbb{Z}_p[\Delta_p]$-module. Canonically we have:*

$$\widehat{M} = \prod_{\mathfrak{p}|p} M_\mathfrak{p} \cong M_{\mathfrak{p}'} \otimes_{\mathbb{Z}_p[\Delta_p]} \mathbb{Z}_p[\Delta].$$

2. The $\mathbb{Z}_p[\Delta_p]$-module $\mathbb{Z}_p[\Delta]$ is flat.

Proof. (1) Since canonically $\widehat{M} \cong \prod_{\mathfrak{p}|p} M \otimes_{\mathbb{Z}[\Delta_p]} \mathcal{O}_\mathfrak{p}$, by the isomorphism (7.1) we get

$$\widehat{M} \cong M \otimes_{\mathbb{Z}[\Delta_p]} \prod_{\mathfrak{p}|p} \mathcal{O}_\mathfrak{p} \cong M_{\mathfrak{p}'} \otimes_{\mathbb{Z}_p[\Delta_p]} \mathbb{Z}_p[\Delta].$$

(2) Follows directly from (1) since the localizations and finite products are exact. □

7.2 Kummer theory for abelian unramified extensions

For $n \geq 0$ let $F_n = F(\zeta_{p^{n+1}})$, $G_n = \mathrm{Gal}\big(F_n/F\big)$ and as before put $F_\infty = \bigcup_{n\in\mathbb{N}} F_n$ and $G_\infty = \mathrm{Gal}\big(F_\infty/F\big)$. Lemma 7.1.1 allow us to generalize almost everything we have done in last chapter to the semi-local case for example:

Theorem 7.2.1 *The additive group $\widehat{\mathcal{O}}_F[[X]]$ admits a continues $\widehat{\mathcal{O}}_F[\Delta][[G_\infty]]$-action such that for all $\sigma \in G_\infty$ and $f \in \widehat{\mathcal{O}}_F[[X]]$,*

$$\sigma \cdot f = f\big((1+X)^{\kappa([\sigma])} - 1\big) \tag{7.3}$$

Proof. First, since F is unramified at p we have canonically that $G_\infty \cong \mathrm{Gal}\big(F_{\mathfrak{p}',\infty}/F_{\mathfrak{p}'}\big)$. Now by Lemma 7.1.1 we get $\widehat{\mathcal{O}}_F[[X]] \cong \mathcal{O}_{F_{\mathfrak{p}'}}[[X]] \otimes_{\mathbb{Z}_p[\Delta_p]} \mathbb{Z}_p[\Delta]$, hence it has a natural structure of $\mathcal{O}_{F_{\mathfrak{p}'}}[[G_\infty]]$ module satisfying (7.3), and clearly we may extend this action to an $\mathcal{O}_{F_{\mathfrak{p}'}}[[G_\infty]] \otimes_{\mathbb{Z}_p[\Delta_p]} \mathbb{Z}_p[\Delta]$-action and therefore to an $\widehat{\mathcal{O}}_F[\Delta][[G_\infty]]$-action. □

Now, set

$$\mathfrak{M}_F := \{f \in \widehat{\mathcal{O}}_F[[X]] \mid f(0) = 1 \bmod p\}.$$

Canonically $\mathfrak{M}_F \cong \prod_{\mathfrak{p}|p} \mathfrak{M}_{F_\mathfrak{p}} \cong \mathfrak{M}_{F_{\mathfrak{p}'}} \otimes_{\mathbb{Z}_p[\Delta_p]} \mathbb{Z}_p[\Delta]$, hence it has natural structure of topological $\mathbb{Z}_p[\Delta][[G_\infty]]$ induced by the $\mathbb{Z}_p[[G_\infty]]$-action on $\mathfrak{M}_{F_{\mathfrak{p}'}}$, therefore it satisfies (7.3). Let $\mathcal{N}_F : \mathfrak{M}_F \longrightarrow \mathfrak{M}_F$ the map induced by $\mathrm{Nr}_{F_{\mathfrak{p}'}}$ i.e. $\mathcal{N}_F = \mathrm{Nr}_{F_{\mathfrak{p}'}} \otimes_{\mathbb{Z}_p[\Delta_p]} Id_{\mathbb{Z}_p[\Delta]}$ and $\mathfrak{M}_F^\varphi = \{f \in \mathfrak{M}_F \mid \mathcal{N}_F(f) = \varphi f\}$, where φ is the induced by the Frobenius acting on coefficients. Note that canonically $\mathfrak{M}_F^\varphi \cong \prod_{\mathfrak{p}|p} \mathfrak{M}_{F_\mathfrak{p}}^\varphi \cong \mathfrak{M}_{F_{\mathfrak{p}'}}^\varphi \otimes_{\mathbb{Z}_p[\Delta_p]} \mathbb{Z}_p[\Delta]$

Definition 7.2.1 *We define the* **semi-local units** *of F as*

$$\mathscr{U}_F = \prod_{\mathfrak{p}|p} U^1_{F_\mathfrak{p},\infty}$$

The $\mathbb{Z}_p[[G_\infty]]$-structure of $U^1_{F,\infty}$ induces canonically a $\mathbb{Z}_p[\Delta][[G_\infty]]$ structure n $\mathscr{U}_F$, so in such context we get:

Theorem 7.2.2 *Let $\eta_n = \zeta_{p^{n+1}} - 1$. There is a topological $\mathbb{Z}_p[\Delta][[G_\infty]]$-isomorphism $\mathfrak{Col}_F : \mathscr{U}_F \longrightarrow \mathfrak{M}_F^\varphi$ such that for $u = (u_n)_{n\in\mathbb{N}} \in \mathscr{U}_F$ and $f_\eta = \mathfrak{Col}_F(u) \in \mathfrak{M}_F^\varphi$ we have*

$$f_\eta(\eta_n) = \varphi^n(u_n).$$

Proof. Take $\mathfrak{Col}_F = \mathfrak{Col}_{F_{\mathfrak{p}'}} \otimes_{\mathbb{Z}_p[\Delta_p]} Id_{\mathbb{Z}_p[\Delta]}$. By Theorem 6.5.1 and the flatness of $Id_{\mathbb{Z}_p[\Delta]}$, $\mathfrak{Col}_F$ has the desire properties. □

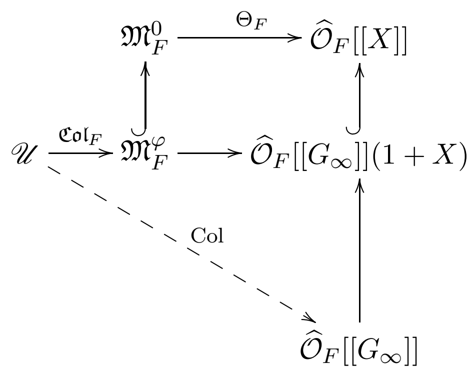
Let Φ be the continuous endomorphism of $\widehat{\mathcal{O}}_F[[X]]$ defined as

$$\Phi(f) = \varphi(f)\big((1+X)^p + 1\big)$$

By Lemma 6.5.3 we have a $\mathbb{Z}_p[\Delta][[G_\infty]]$-homomorphism $\Theta_F : \mathfrak{M}_F^0 \longrightarrow \widehat{\mathcal{O}}_F[[X]]$ defined by

$$\Theta_F(f) = \left(1 - \frac{\Phi}{p}\right)\log(f).$$

From the diagram (6.12) we get



Therefore, for $u \in \mathscr{U}$, there exists a unique element $\mathrm{Col}(u) \in \widehat{\mathcal{O}}_F[[G_\infty]]$ satisfying

$$\Theta_F(\mathfrak{Col}_F(u)) = \mathrm{Col}(u) \cdot (1+X),$$

which defines a $\mathbb{Z}_p[\Delta][[G_\infty]]$-homomorphism $\mathrm{Col} : \mathscr{U} \longrightarrow \widehat{\mathcal{O}}_F[[G_\infty]]$. As every homomorphism, Col admits a unique extension to the total quotient rings

$$\mathrm{Col} : Q(\mathscr{U}_F) \longrightarrow Q(\widehat{\mathcal{O}}_F[[G_\infty]]).$$

Since $Q(\mathscr{U}_F) = \varprojlim (F_n \otimes \mathbb{Q}_p)^\times \cong p^{\mathbb{Z}} \times \mathscr{U}_F$ we have that for $x = p^n\, u \in \varprojlim (F_n \otimes \mathbb{Q}_p)^\times$ with $u \in \mathscr{U}_F$ and every $\sigma \in G_\infty$,

$$(1-\sigma) \cdot x = p^n\, u\, \sigma(p^n\, u)^{-1} = u\, \sigma(u)^{-1} \in \mathscr{U}_F.$$

Hence, the image of Col really lies in

$$\widehat{\mathcal{O}}_F[[G_\infty]]^{\sim} = \left\{ x \in \mathcal{Q}(\mathcal{O}_F[[G_\infty]]) \mid \forall\, \sigma \in G_\infty,\, (1-\sigma)x \in \widehat{\mathcal{O}}_F[[G_\infty]] \right\}$$

so we get the following an extension of $\mathfrak{Col}$ as $\mathbb{Z}_p[\Delta][[G_\infty]]$-homomorphism:

$$\mathrm{Col} : \varprojlim (F_n \otimes \mathbb{Q}_p)^\times \longrightarrow \widehat{\mathcal{O}}_F[[G_\infty]]^{\sim}$$

Let $\Gamma_{\mathfrak{p}} = \mathrm{Gal}\big(F_{\mathfrak{p},\infty}/F_{\mathfrak{p}}\big) \cong \mathbb{Z}_p^\times$. Since they are canonically isomorphic we may write Γ instead of $\Gamma_{\mathfrak{p}}$ doing the corresponding identification in each case.

For a $\mathbb{Z}_p$-module Note that the cyclotomic character $\kappa : \Gamma \longrightarrow \mathbb{Z}_p^\times$ induces a natural topological generator $\gamma_0 \in \Gamma$ such $\kappa(\gamma_0) = 1 + pd$ where $d = [F : \mathbb{Q}]$. By Theorem 4.3.1 for each $\mathfrak{p}|p$, we have an isomorphism of compact $\mathcal{O}_{\mathfrak{p}}$-algebras $\mathcal{O}_{\mathfrak{p}}[[\Gamma]] \cong \mathcal{O}_{\mathfrak{p}}[[T]]$ which identifies the topological generator $\gamma_0 \in \Gamma$ with $1+T$. Further, since we have a canonical isomorphisms $\widehat{\mathcal{O}}_F[[\Gamma]] \cong \prod_{\mathfrak{p}|p} \widehat{\mathcal{O}}_{\mathfrak{p}}[[[\Gamma]]$ and $\widehat{\mathcal{O}}_F[[T]] \cong \prod_{\mathfrak{p}|p} \widehat{\mathcal{O}}_{\mathfrak{p}}[[[T]]$, therefore we get an isomorphism of compact $\widehat{\mathcal{O}}_F$ algebras which sends γ_0 in $1+T$,

$$\widehat{\mathcal{O}}_F[[\Gamma]] \cong \widehat{\mathcal{O}}_F[[T]],$$

Since $G_0 = \mathrm{Gal}\big(F_0/F\big) \cong \mathrm{Gal}\big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\big)$, we may consider the Teichmüller character $\omega : G_0 \longrightarrow \mathbb{Z}_p$. For $0 \le j \le p-2$, let

$$e_j = \frac{1}{p-1} \sum_{\tau \in G_0} \omega^j(\tau)\tau^{-1},$$

denote the idempotents of $\mathbb{Z}_p[G_0]$. Since $G_\infty \cong \Gamma \times G_0$, the idempotents induce the following decomposition of $\widehat{\mathcal{O}}_F$-algebras as $\mathbb{Z}_p[G_0]$-module $\widehat{\mathcal{O}}_F$-algebras

$$\widehat{\mathcal{O}}_F[[G_\infty]] \cong \bigoplus_{j=0}^{p-2} e_j \widehat{\mathcal{O}}_F[[\Gamma]][G_0] \cong \bigoplus_{j=0}^{p-2} \widehat{\mathcal{O}}_F[[\Gamma]] e_j \cong \bigoplus_{j=0}^{p-2} \widehat{\mathcal{O}}_F[[T]] e_j. \tag{7.4}$$

The last isomorphism is induced by $\gamma_0 \longmapsto 1+T$.

Lemma 7.2.1 *The isomorphism given in (7.4) extends uniquely to an isomorphism of $\mathcal{O}_F$-algebras*

$$\widehat{\mathcal{O}}_F[[G_\infty]]^\sim \cong \frac{1}{T}\widehat{\mathcal{O}}_F[[T]]e_0 \oplus \bigoplus_{j=1}^{p-2} \widehat{\mathcal{O}}_F[[T]] e_j. \tag{7.5}$$

Proof. As a morphism of $\mathcal{O}_F$-algebras it extends uniquely on the total quotient field and therefore on $\widehat{\mathcal{O}}_F[[G]]^\sim$. Since $\widehat{\mathcal{O}}_F[[G_\infty]]^\sim$ is a $\mathbb{Z}_p[\Delta]$-module we have

$$\widehat{\mathcal{O}}_F[[G_\infty]]^\sim \cong \bigoplus_{j=1}^{p-2} e_j \widehat{\mathcal{O}}_F[[G_\infty]]^\sim.$$

Then, each $x \in \widehat{\mathcal{O}}_F[[G_\infty]]^\sim$ have a unique decomposition $x = \sum_{i=1}^{p-2} e_j x = \sum_{i=1}^{p-2} x^{(j)} e_j$. By definition $(1-\gamma_0)x \in \widehat{\mathcal{O}}_F[[G_\infty]]$ then $e_0(1-\gamma_0)x \in e_0 \widehat{\mathcal{O}}_F[[G_\infty]] = \widehat{\mathcal{O}}_F[[\Gamma]]e_0$ therefore there exits $\gamma^{(0)} \in \mathcal{O}_F[[\Gamma]]$ such that $e_0 x = (\gamma_0 - 1)^{-1}\gamma^{(0)} e_0$. It is enough to show:

Claim: For $1 \le j \le p-2$ there exits $\gamma^{(j)} \in \widehat{\mathcal{O}}_F[[\Gamma]]$ such $e_j x = \gamma^{(j)} e_j$.

Since $\omega^j \neq 1$ there exists a $\tau_j \in G_0$ such that $\omega^j(\tau_j) \neq 1$, hence

$$(1-\tau_j)x \in \widehat{\mathcal{O}}_F[[G_\infty]] = \bigoplus_{j=0}^{p-2} \widehat{\mathcal{O}}_F[[\Gamma]] e_j \cong \bigoplus_{j=0}^{p-2} \widehat{\mathcal{O}}_F[[T]] e_j.$$

Now the j-th component of $(1-\tau_j)x$ is given by

$$e_j(1-\tau_j)x = \frac{1}{p-1} \sum_{\tau \in G_0} \omega^j(\tau)\tau^{-1}(1-\tau_j)x = \frac{1-\omega^j(\tau_j)}{p-1} x^{(j)} e_j \in \widehat{\mathcal{O}}_F[[\Gamma]] e_j.$$

Since $1-\omega^j(\tau_j)$ is a unit we have that $e_j x = \gamma^{(j)} e_j$ with $\gamma^{(j)} \in \mathcal{O}_F[[\Gamma]]$.

We have proved that $x \in \widehat{\mathcal{O}}_F[[G]]^{\sim}$ it have a unique decomposition

$$x = (\gamma_0 - 1)^{-1}\gamma^{(0)} + \sum_{j=1}^{p-2} \gamma^{(j)} e_j$$

with $\gamma^{(k)} \in \widehat{\mathcal{O}}_F[[\Gamma]]$ and clearly all such x lie in $x \in \widehat{\mathcal{O}}_F[[G]]^{\sim}$ therefore we get (7.5). □

Definition 7.2.2 *For $u \in \varprojlim(F_n \otimes \mathbb{Q}_p)$ and $0 \le i \le p-2$, we define $\mathrm{Col}^{(i)}(u)$ as the power series such that under isomorphism 7.5,*

$$\mathrm{Col}(u) \longmapsto \sum_{j=0}^{p-2} \mathrm{Col}^{(j)}(u) e_j.$$

7.3 p-adic L-Function: Coleman-Iwasawa Approach

Let ψ a Dirichlet character of first kind i.e $p^2 \nmid f_\psi$, d the prime-to-p part of f_ψ, $F = \mathbb{Q}(\zeta_d)$ and $\Delta = \mathrm{Gal}\big(F/\mathbb{Q}\big)$. We regard ψ as a character of $G = \mathrm{Gal}\big(\mathbb{Q}(\zeta_{fp})/\mathbb{Q}\big)$ and put $\chi = \psi|_\Delta$. Then uniquely we can write

$$\psi = \chi\omega^i$$

with some $0 \le i \le p-2$. Using the notation of last section $F_n = F(\zeta_{p^{n+1}})$ we have:

Lemma 7.3.1 $\eta_{d,n} = 1 - \zeta_{p^{n+1}}\varphi^{-n}(\zeta_f) \in F_n$. *The sequence*

$$\eta_d = (\eta_{d,n})_{n\in\mathbb{N}}$$

is coherent with respect to norms.

Proof. Since $\mathrm{Gal}\big(F_n/F_{n-1}\big) = \{\sigma_a \mid \sigma_a(\zeta_{p^{n+1}}) = \zeta_p^a \zeta_{p^{n+1}}\}$, we have

$$\begin{aligned} N_{F_n|F_{n-1}}\big(1 - \zeta_{p^{n+1}}\varphi^{-n}(\zeta_d)\big) &= \prod_{a\in F_p} \big(1 - \zeta_p^a \zeta_{p^{n+1}}\varphi^{-n}(\zeta_d)\big) \\ &= 1 - \big(\zeta_{p^{n+1}}\varphi^{-n}(\zeta_d)\big)^p \end{aligned}$$

since $\varphi(\zeta_d) = \zeta_d^p$ we get $N_{F_n|F_{n-1}}\big(1 - \zeta_{p^{n+1}}\varphi^{-n}(\zeta_d)\big) = 1 - \zeta_{p^n}\varphi^{-n}(\zeta_d)$. □

Remark 7.3.1

1. *If $d \ne 1$ then $\eta_{n,d} \in U^1_{F_n}$. Therefore $\eta_d \in \mathscr{U}_F$.*

2. *The sequence η_d has Coleman power series $f_{\eta_d} = \mathfrak{Col}(\eta_d)$ is $1 - \zeta_d(1+X)$, since*

$$\varphi^n(f_{\eta_d}) = 1 - \zeta_{p^{n+1}}\zeta_d = f_{\eta_d}(\zeta_{p^{n+1}} - 1).$$

Let $\xi_\chi = \sum_{\delta\in\Delta} \chi(\delta^{-1})\delta \in \mathbb{Z}[\zeta_d][\Delta]$. ξ_χ acts naturally (on coefficients) on $F[[X]]$ and since $\xi({\zeta_d}^a) = \chi(a)\xi(\zeta_d)$, for every $y \in \widehat{\mathcal{O}}_F$ there is a unique $\widetilde{y} \in \mathbb{Z}_p[\chi]$ such that

$$\xi_\chi(y) = \widetilde{y}\xi_\chi(\zeta_f).$$

Definition 7.3.1 *For $\psi = \chi\omega^i$ as before, we define g_ψ as*

$$g_\psi(T)\xi_\chi(\zeta_d) = -\xi_\chi\big(\mathrm{Col}^{(i)}(\eta_d)\big).$$

For $f \in \widehat{\mathcal{O}}_F[[X]]$, let

$$Df(X) = (1+X)\frac{d}{dX}f(X).$$

Lemma 7.3.2 *Let $f_{\eta_d} = \mathfrak{Col}(\eta_d)$, then:*

$$\xi_\chi(D\Theta_F f_{\eta_d})|_{X=e^Z-1} = \sum_{n=1}^{\infty}\big(1-\chi(p)p^{n-1}\big)B_{n,\chi}\frac{Z^{n-1}}{n!}\xi_\chi(\zeta_d).$$

Proof. By Remark 7.3.1 $f_{\eta_d} = 1-\zeta_d(1+X)$ therefore

$$\Phi(f_{\eta_d}) = \varphi(f_{\eta_d})\big((1+X)^p-1\big) = 1-\zeta_d^p(1+X)^p.$$

Now, by definition of Θ_F and D we have:

$$\begin{aligned} D\left(1-\tfrac{\Phi}{p}\right)\log f_{\eta_d} &= \frac{f'_{\eta_d}}{f_{\eta_d}} - \frac{1}{p}\frac{(\varphi f_{\eta_d})'}{(\varphi f_{\eta_d})} \\ &= \frac{\zeta_d(1+X)}{\zeta_d(1+X)-1} - \frac{\zeta_d^p(1+X)^p}{\zeta_d^p(1+X)^p-1} \qquad {}^{1} \\ &= \sum_{a=1}^{f}\frac{\zeta_d^a(1+X)^a}{(1+X)^f-1} - \sum_{a=1}^{f}\frac{\zeta_d^{ap}(1+X)^{ap}}{(1+X)^{fp}-1} \end{aligned}$$

Applying ξ_χ to both sides (since $\xi({\zeta_d}^a) = \chi(a)\xi(\zeta_d)$),

$$\xi_\chi\left(D\Theta_F f_{\eta_d}\right) = \left(\sum_{a=1}^{f}\frac{\chi(a)(1+X)^a}{(1+X)^f-1} - \sum_{a=1}^{f}\frac{\chi(ap)(1+X)^{ap}}{(1+X)^{fp}-1}\right)\xi_\chi(\zeta_d).$$

Finally, setting $X = e^Z-1$ we get:

$$\begin{aligned} \xi_\chi(D\Theta_F f_{\eta_d})|_{X=e^Z-1} &= \left(\sum_{a=1}^{f}\frac{\chi(a)e^{Za}}{e^{Zf}-1} - \sum_{a=1}^{f}\frac{\chi(ap)e^{Zap}}{e^{Zfp}-1}\right)\xi_\chi(\zeta_d) \\ &= \left(\sum_{n=1}^{\infty}B_{n,\chi}\frac{Z^{n-1}}{n!} - \chi(p)\sum_{n=1}^{\infty}B_{n,\chi}\frac{(pZ)^{n-1}}{n!}\right)\xi_\chi(\zeta_d). \end{aligned}$$

□

[1] in this step we are using the general fact $\sum_{a=1}^{f}(\zeta_d T)^a = \frac{T^f-1}{\zeta_d T-1}\zeta_d T$, hence $\sum_{a=1}^{f}\frac{(\zeta_d T)^a}{T^f-1} = \frac{\zeta_d T}{\zeta_d T-1}$.

Lemma 7.3.3 *Let $f \in \widehat{\mathcal{O}}_K[[T]](1+X)$. If*

$$f(X) = \left(\sum_{j=0}^{p-2} \beta_j(T) e_j\right) \cdot (1+X)$$

with $\beta_j \in \widehat{\mathcal{O}}_K[[T]]$. Then we have

$$D^k f(0) = \beta_j(\kappa(\gamma_0)^k - 1) \tag{7.6}$$

For all $k \geq 1$ with $k \equiv j \bmod p-1$.

Proof. Let $\beta = (1+T)^n$ and $f = \beta(T)e_j \cdot (1+X)$. Since $\beta(T)e_j$ corresponds in $\mathcal{O}_K[[G_\infty]]$ to $\frac{1}{p-1} \sum_{\tau \in G_0} \omega^j(\tau)\tau^{-1}\gamma_0^n$, hence we have that

$$f = \frac{1}{p-1} \sum_{\tau \in G_0} \omega^j(\tau)(\tau^{-1}\gamma_0^n) \cdot (1+X) = \frac{1}{p-1} \sum_{\tau \in G_0} \omega^j(\tau)(1+X)^{\kappa(\gamma_0^n \tau^{-1})}.$$

Now, since $D^k (1+X)^\alpha = \alpha^k (1+X)^\alpha$ and $\kappa(\tau^{-1})^k = \omega^{-k}(\tau)$, we have

$$\begin{aligned} D^k f &= \frac{1}{p-1} \sum_{\tau \in G_0} \omega^j(\tau)\kappa(\gamma_0^n \tau^{-1})^k (1+X)^{\kappa(\gamma_0^n \tau^{-1})} \\ &= \frac{1}{p-1} \sum_{\tau \in G_0} \omega^j(\tau)\omega^{-k}(\tau)\kappa(\gamma_0^k)^n (1+X)^{\kappa(\gamma_0^n \tau^{-1})}. \end{aligned}$$

Therefore

$$D^k f(0) = \begin{cases} \beta\big(\kappa(\gamma_0 - 1)\big) & k \equiv j \bmod p-1 \\ 0 & k \not\equiv j \bmod p-1 \end{cases}$$

By linearity (7.6) holds for linear combinations of e_j with polynomial coefficients. By continuity of the derivative and the action it must hold for general power series. $\square$

Theorem 7.3.1 (Iwasawa-Coleman-Tsuji) *Let $\psi = \chi\omega^i$ as above. For $k \geq 1$ with $k \equiv i \bmod p-1$, we have*

$$g_\psi\big(\kappa(\gamma_0)^k - 1\big) = -\big(1 - \chi(p)p^{k-1}\big)\frac{B_{k,\chi}}{k} = L_p(\psi, 1-k),$$

therefore for any $s \in \mathbb{Z}_p$

$$L_p(\psi, s) = g_\psi\big(\kappa(\gamma_0)^{1-s} - 1\big).$$

Proof. Since $\Theta_F\big(f_{\eta_d}(X)\big) = \mathrm{Col}(f_{\eta_d})(1+X) = \sum \mathrm{Col}^{(j)}(T)e_j \cdot (1+X)$, by Lemma 7.3.3 we have:

$$D^k \, \mathrm{Col}(f_{\eta_d})(1+X)|_{X=0} = \mathrm{Col}^{(i)}\big(\kappa(\gamma_0)^k - 1\big). \tag{7.7}$$

Put $X = e^{\mathbb{Z}} - 1$, then $D = (1+X)\frac{d}{dX} = \frac{d}{dZ}$. Applying D^{k-1} to (7.7) we get

$$\begin{aligned} & g_\psi\big(\kappa(\gamma_0)^k - 1\big)\xi_\chi(\zeta_d) = D^{k-1}\xi_\chi(D\Theta_F f_{\eta_d}) \\ = \quad & D^{k-1}\left(\sum_{n=1}^{\infty}\big(1-\chi(p)p^{n-1}\big)B_{n,\chi}\frac{Z^{n-1}}{n!}\right)\Bigg|_{Z=0}\xi_\chi(\zeta_d), \end{aligned}$$

hence

$$\begin{aligned} & g_\psi\big(\kappa(\gamma_0)^k - 1\big)\xi_\chi(\zeta_d) \\ = \quad & D^{k-1}\xi_\chi(D\Theta_F f_{\eta_d}) \\ = \quad & D^{k-1}\sum_{n=1}^{\infty}\big(1-\chi(p)p^{n-1}\big)B_{n,\chi}\frac{Z^{n-1}}{n!}\xi_\chi(\zeta_d)\Bigg|_{Z=0}\xi_\chi(\zeta_d) \\ = \quad & \big(1-\chi(p)p^{k-1}\big)\frac{B_{k,\chi}}{k}\xi_\chi(\zeta_d). \end{aligned}$$

This completes the proof. □

Bibliography

[Col79] Robert F. Coleman. Division values in local fields. *Invent. Math.*, 53(2):91–116, 1979.

[Col83] R. Coleman. Local units modulo circular units. *Proc. Amer. Math. Soc.*, 89(1):1–7, 1983.

[CS06] J. Coates and R. Sujatha. *Cyclotomic fields and zeta values*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[Gre92] Cornelius Greither. Class groups of abelian fields, and the main conjecture. *Ann. Inst. Fourier (Grenoble)*, 42(3):449–499, 1992.

[Iwa72] Kenkichi Iwasawa. *Lectures on p-adic L-functions*. Princeton University Press, Princeton, N.J., 1972. Annals of Mathematics Studies, No. 74.

[Iwa86] Kenkichi Iwasawa. *Local class field theory*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1986. Oxford Mathematical Monographs.

[KL64] Tomio Kubota and Heinrich-Wolfgang Leopoldt. Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen. *J. Reine Angew. Math.*, 214/215:328–339, 1964.

[Lan90] Serge Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990. With an appendix by Karl Rubin.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Mil08] James S. Milne. Fields and galois theory (v4.20), 2008. Available at www.jmilne.org/math/.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Rob00] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Tsu99] Takae Tsuji. Semi-local units modulo cyclotomic units. *J. Number Theory*, 78(1):1–26, 1999.

[Tsu01] Takae Tsuji. The Stickelberger elements and the cyclotomic units in the cyclotomic $\mathbb{Z}_p$-extensions. *J. Math. Sci. Univ. Tokyo*, 8(2):211–222, 2001.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wil98] John S. Wilson. *Profinite groups*, volume 19 of *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press, New York, 1998.