Universiteit Leiden

Institut de Mathématiques de Bordeaux

Thuong Tuan Dang

Master Thesis

p-adic Galois Representations and (φ,Γ)-modules

Algebra, Geometry and Number Theory

ALGANT Master Program

Supervisor

Prof. Dr. Denis Benois

Contents

Acknowledgement

I would like to express my deepest gratitude to Professor Denis Benois, my advisor, for his patient guidance and wonderful lectures in Number Theory. Special thanks should be given to the ALGANT committee, and all of my teachers in Leiden and Bordeaux. I would also like to thank Mr. Abhinandan, Mr. Yulin Cai, and Mr. Luming Zhao for their helpful discussions during the time I am in Bordeaux. My grateful thanks are extended to Mr. Pablo Manchon for his useful LaTeX techniques. I would also like to extend my thanks to Mr. Thanh Nguyen and Mr. Tan Tran for sharing with me my difficulties. Finally, I wish to thank my parents and my girlfriend Luulie for their constant support and encouragement throughout my study.

Introduction

Let L be a field, and L^{sep} its separable closure, one of the central goals of modern number theory is to understand about the absolute Galois group $G_L := \text{Gal}(L^{\text{sep}}/L)$. From the group theory point of view, G_L is a profinite group, which is the inverse limit of all Galois groups of finite Galois extensions over L. For some cases, G_L is easy to describe, for example, $L := \mathbb{R}$ or $L := \mathbb{F}_q$. For the case of local fields, the problem is much more complicated, and although we can describe G_L in terms of generators and relations, the arithmetical information is not provided [FV02] (page 169).

Another approach is to understanding G_L via its representations. In the case $L = \mathbb{Q}_p$, we denote $\text{Rep}_{\mathbb{Z}_p}(G_{\mathbb{Q}_p})$ the category of all finitely generated $\mathbb{Z}_p$-modules with continuous actions from $G_{\mathbb{Q}_p}$. Jean-Marc Fontaine [Fon90] developed a theory of (φ, Γ)-modules that allows us to pass from $\text{Rep}_{\mathbb{Z}_p}(G_{\mathbb{Q}_p})$ to another equivalent category, which is easier to understand.

More precisely, if we denote $\mathbb{Q}_p^\infty$ the field extension of $\mathbb{Q}_p$ obtained by adjoining all p^n-th roots of unity, and $\Gamma := \text{Gal}(\mathbb{Q}_p^\infty/\mathbb{Q}_p)$. Let

$$\mathscr{A}_{\mathbb{Q}_p} := \Big\{ \sum_{i\in\mathbb{Z}} a_i X^i | a_i \in \mathbb{Z}_p, \lim_{i\to-\infty} a_i = 0 \Big\}$$

the ring of infinite Laurent series, then the theorem of Fontaine yields $\text{Rep}_{\mathbb{Z}_p}(G_{\mathbb{Q}_p})$ is equivalent to $\text{Mod}^{\text{et}}(\mathscr{A}_{\mathbb{Q}_p})$, where $\text{Mod}^{\text{et}}(\mathscr{A}_{\mathbb{Q}_p})$ is the category of all finitely generated $\mathscr{A}_{\mathbb{Q}_p}$-modules with some other axioms related to the action of Γ. As a corollary of Lubin-Tate theory, we have $\Gamma \cong \mathbb{Z}_p^\times$, which is a procyclic group. Hence, the action of Γ is easier to understand than the action of $G_{\mathbb{Q}_p}$.

The theory of (φ, Γ)-modules was later generalized by M. Kisin and W. Ren [KR09] for arbitrarily local field of characteristic 0 and in this case, cyclotomic extensions are replaced by Lubin-Tate extensions, under the assumption that the Frobenius series is a polynomial. P. Schneider [Sch17] then dealt with the general Frobenius series under the new point of view, so called tilting correspondences, developed by P. Scholze [Sch12], and simplified by K.Kedlaya [Ked15]. And the goal of this thesis is to present the proof of the equivalence of categories in the later settings in details, and discuss about some of its applications.

This text is organized as follows. In the first chapter, we will introduce the theory of formal group law, and Lubin-Tate extensions, and the main goal of this chapter is to prove the isomorphism between $\Gamma_L := \text{Gal}(L_\infty/L)$ and $\mathcal{O}^\times$, for any local field L, where L_∞ is the Lubin-Tate extension of L with a fixed Frobenius series, and $\mathcal{O} := \mathcal{O}_L$ is its ring of integers. In the second chapter, we will treat the theory of ramified Witt vectors in details. The third chapter is devoted for the tilting correspondences with the setting $L/\mathbb{Q}_p$ is a finite extension, and that is a fundamental step to the theory of (φ, Γ)-modules. The main result of this chapter is the (topological) isomorphism between the absolute Galois group of L_∞ and the absolute Galois group of $\mathbb{F}_q((X))$, where $\mathbb{F}_q$ is the residue field of L. Together with it, the close relations between characteristic 0 and characteristic p are reflected via other tilting correspondences. In the fourth chapter, we will introduce the category of etale (φ, Γ)-modules. And in the last chapter, we will introduce the pair of functors $\mathscr{D}$ and $\mathscr{V}$ between $\text{Rep}_{\mathcal{O}}(G_L)$ and $\text{Mod}^{\text{et}}(\mathscr{A}_L)$, and then prove that they are quasi-inverse of each other. We should note that $\mathscr{D}$ and $\mathscr{V}$ have some nice properties, including they are exact and preserve elementary divisors. The main reference for the whole thesis would be [Sch17].

The contribution of the thesis is minor among such big theories and results. The theory of ramified Witt vectors treated in [Sch17] are defined under the assumptions of local fields of characteristic 0, but we realized that it also works for local fields of characteristic p. In the end of Chapter III, as an application of the tilting correspondences, we proved that the p-cohomological dimension of $G_{\mathbb{Q}_p}$ is not larger than 2. It is a result proved by Herr [Her98] by using the theory of (φ, Γ)-modules. We also used the machinery of (φ, Γ)-modules to deduce that in the setting of cyclotomic extension over $\mathbb{Q}_p$, for the rank one case, Galois representations and (φ, Γ)-modules come from twists by characters. And with the use of Galois cohomology, we replaced and simplified some parts of the proof in [Sch17] about the equivalence of categories.

Chapter 1

Lubin-Tate extension

Class field theory studies abelian extensions of a local or global field. One can obtain the description of the maximal abelian extension of a local field by Lubin-Tate theory [LT65]. And in this chapter, we will introduce the theory of Lubin-Tate extension. The main references for this chapter are [Sch17], and [Mil13].

1.1 Formal group law and homomorphisms

We always fix A a commutative ring, let us warm up with the useful statement for the ring of power series of one variable $A[[X]]$.

Lemma 1.1.1. *Let $f = a_1X + a_2X^2 + ... \in A[[X]]$, then there exists $g(X) \in XA[[X]]$ such that $f \circ g(X) = X$ iff $a_1 \in A^\times$. Also, if such g exists, then it is unique, and $f \circ g(X) = g \circ f(X) = X$.*

Proof. Let $g(X) = b_1X + b_2X^2 + ... \in A[[X]]$. We then have

$$f(g(X)) = a_1(b_1X + b_2X^2 + ...) + a_2(b_1X + b_2X^2 + ...)^2 + ... =$$
$$= (a_1b_1)X + (a_1b_2 + a_2b_1)X^2 + ...$$

Then $f(g(X)) = X$ iff $a_1b_1 = 1, a_1b_2 + a_2b_1 = 0, ...$ Hence, $f \circ g(X) = X$ iff $a_1 \in A^\times$. The uniqueness of $g(X)$ directly follows from this.

Assume that $a_1 \in A^\times$, and $g(X)$ is constructed as above. Because $b_1 = (a_1)^{-1} \in A^\times$, we can construct $h(X) \in XA[[X]]$ such that $g \circ h(X) = X$, and hence

$$h(X) = (f \circ g) \circ h(X) = f \circ (g \circ h)(X) = f(X)$$

Hence, $f \circ g(X) = g \circ f(X) = X$. □

Remark 1.1.2. From the lemma above, the set $\{a_1X + a_2X^2 + ... \in A[[X]] | a_1 \in A^\times\}$ is a group.

We are now ready for the definition of formal group.

Definition. Let $A[[X, Y]]$ be the ring of formal power series ring of two variables, $F(X, Y) \in A[[X, Y]]$, then F is said to be a commutative formal group law if:
(i) $F(X, Y) = X + Y +$(terms of degree ≥ 2).
(ii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.
(iii) $F(X, Y) = F(Y, X)$.

For convenience, we will often denote "terms of degree $\geq n$" as $\mod \deg n$.

Proposition 1.1.3. *Let F be a commutative formal group law, then*

(i) $F(X, Y) = X + Y + \sum_{i,j \geq 1} a_i b_j X^i Y^j$

(ii) There exists a unique $i_F(X) \in XA[[X]]$ such that $F(X, i_F(X)) = 0$.

Proof.

(i) Denote $f(X) := F(X, 0) = X \mod \deg 2$, then by the definition, we have

$$F(0, F(X, 0)) = F(F(X, 0), 0) = f \circ f(X)$$

And $F(F(X, 0), 0) = F(X, F(0, 0)) = F(X, 0) = f(X)$, we obtain $f \circ f = f$. This follows from Lemma 1.1.1 that there exists a unique $g \in XA[[X]]$ such that $f \circ g = g \circ f = X$. Hence,

$$f(X) = f \circ (f \circ g(X)) = (f \circ f) \circ g(X) = (f \circ g)(X) = X$$

And this yields $F(X, 0) = X$. By symmetry, we also have $F(0, Y) = Y$. And this yields any commutative formal group law is of the form

$$F(X, Y) = X + Y + \sum_{1 \leq i,j} a_i b_j X^i Y^j$$

(ii) Take Let $i_F(X) = b_1 X + b_2 X^2 + ... \in XA[[X]]$, we have

$$F(X, i_F(X)) = X + i_F(X) + a_{11} X i_F(X) + (a_{12} X i_F(X)^2 + a_{21} X^2 i_F(X)) + ...$$

then $F(X, i_F(X)) = 0$ iff

$$X + (b_1 X + b_2 X^2 + ...) + a_{11} X)(b_1 X + b_2 X^2 + ...) = (b_1 + 1)X + (b_2 + a_{11} b_1) X^2 + ...$$

Solving the system of equations for each coefficients in $i_F(X)$, we can see that $i_F(X)$ is uniquely determined.

□

So, we can add the condition (iv) in the definition of commutative formal group law about the existence of inverse as the remark above. But it turns out to be deduced from (i), (ii) and (iii).

Corollary 1.1.4. *Let K be a non-archimedean complete field, with its ring of integer $A := \mathcal{O}_K$ and its maximal ideal $\mathfrak{m}_K$, and F is a formal group law in $A[[X, Y]]$, if we define $x +_F y := F(x, y)$ for any $x, y \in \mathfrak{m}_K$, then $(\mathfrak{m}_K, +_F)$ forms an abelian group.*

Proof. Due to the definition and Proposition 1.1.3, it is sufficient to check that $x +_F y$ is in $\mathfrak{m}_K$. But because $F(x, y) = x + y + \sum_{i,j \geq 1} a_i b_j x^i y^j$, for $a_i, b_j \in A$, we can see that $F(x, y)$ is in fact in $\mathfrak{m}_K$, due to the convergent criterion of series in non-archimedean complete field. □

Example 1.1.5. Let $G_a(X, Y) := X + Y$, then it can be easily checked that F defines a commutative formal group law, which is called the **additive formal group law**. Similarly, $G_m(X, Y) := X + Y + XY = (1 + X)(1 + Y) - 1)$ also defines a commutative formal group law, which is called the **multiplicative formal group law** . Let K be a complete non-archimedean field, with $\mathcal{O}_K, \mathfrak{m}_K$ is defined as above, then it is easy to check that the group $(\mathfrak{m}_K, +_{G_m})$ is isomorphic to the multiplictive group $1 + \mathfrak{m}_K$ via the map $x \mapsto 1 + x$.

We are now ready to define homomorphisms between formal group laws.

Definition. Let $F, G \in A[[X, Y]]$ be two formal group laws, then a power series $h(X) \in A[[X]]$ is said to be a homomorphism from F to G (say, a homomorphism $h : F \to G$) if

$$f(F(X, Y)) = G(f(X), f(Y))$$

h is said to be an isomorphism if there exists a homomorphism $h' : G \to F$ and $h \circ h'(X) = h' \circ h(X) = X$.

Based on Lemma 1.1.1, there is a useful characterization of isomorphisms between formal group laws.

Lemma 1.1.6. *Let $h : F \to G$ be a homomorphism between formal group laws, then h is an isomorphism iff $h(X) = a_1 X \mod \deg 2$, with $a_1 \in A^\times$.*

Proof. One can see by Lemma 1.1.1 that there exists $h' \in A[[X]]$ such that $h \circ h' = h' \circ h = X$ iff $a_1 \in A^\times$. And in this case, we have

$$h'(G(X,Y)) = h'(G(h \circ h'(X), h \circ h'(Y))) = (h' \circ h) \circ F(h'(X), h'(Y)) = F(h'(X), h'(Y))$$

This proves that $h' : G \to F$ is also a homomorphism. And this finishes our proof. □

Example 1.1.7. Let $G_m(X,Y)$ be the multiplicative formal group law, then for a prime number p, we can define $h(X) = (1+X)^p - 1$, then

$$h(G_m(X,Y)) = (1 + G_m(X,Y))^p - 1 = (1+X)^p(1+Y)^p - 1$$

And

$$G_m(h(X), h(Y)) = G_m((1+X)^p - 1, (1+Y)^p - 1) = (1+X)^p(1+Y)^p - 1$$

This yields $h : G_m \to G_m$ is a homomorphism.

We will conclude this section by the following about the endomorphism ring of formal group law

Proposition 1.1.8. *Let F be a commutative formal group law, then*

$$End(F) = \{f : F \to F | f \text{ is a homomorphism}\}$$

forms a ring, with addition $+_F$, and addition $\circ_F$ defined as $f +_F g := F(f,g)$, and $f \circ_F g := f \circ g$.

Proof. The proof of the proposition above is not difficult, but slightly long, with repetition steps.

Step 0. We easily see that $id : F \to F$ defined as $id \circ F = F$, and $0 : F \to F$ defined as $0 \circ F = 0$ are certainly in $End(F)$.

Step 1. Let $f, g \in End(F)$, we have

$$f \circ g \circ F(X,Y) = F(f \circ g(X), f \circ g(Y))$$

This yields $f \circ g \in End(F)$, with $f \circ id = id \circ f = f$.

Step 2. Let $f, g, h \in End(E)$, or more generally, with $f, g, h \in XA[[X]]$, we can easily see that $(f \circ g) \circ h = f \circ (g \circ h)$.

Step 3. We first let $Z := F(i_F(X), i_F(Y))$, we have

$$F(Y,Z) = F(Y, F(i_F(X), i_F(Y))) = F(F(Y, i_F(Y)), i_F(X)) = F(i_F(X), 0) = i_F(X)$$

And from this,

$$F(F(X,Y), Z) = F(X, F(Y,Z)) = F(X, i_F(X)) = 0$$

Also, we have $F(F(X,Y), i_F(F(X,Y))) = 0$. Because of the uniqueness of i_F, we get

$$i_F(F(X,Y)) = F(i_F(X), i_F(Y))$$

This follows that $i_F \in End(F)$.

Step 4. Let $f, g \in End(F)$, we can define $h(X) := F(f(X), g(X)) = f +_F g$. Then,

$$h(F(X,Y)) = F(f(F(X,Y)), g(F(X,Y))) = F(F(f(X), f(Y)), F(g(X), g(Y)))$$

Similar to Step 3, we can interchange terms and get

$$h(F(X,Y)) = F(F(f(X),g(X)),F(f(Y),g(Y))) = F(h(X),h(Y))$$

And this yields $h \in End(F)$, and it is easy to check that $f +_F 0 = 0 +_F f = f$ and $f +_F g = g +_F f$.

Step 5. One can see, by Step 1 and Step 3, $-f := i_F \circ f \in End(F)$. Also, similar to Step 4, we can see $f +_F (-f) = (-f) +_F f = 0$.

Step 6. We have, for all $f, g, h \in End(F)$

$$e(X) := f \circ (g +_F h) = f(F(g(X),h(X))) = F(f \circ g, f \circ h) = (f \circ g) +_F (f \circ h)$$

And similarly, $(g +_F h) \circ f = (g \circ f) +_F (h \circ f)$.

We can now conclude that $End(F)$ is a ring with addition and multiplication laws defined as above. □

1.2 Lubin-Tate formal group law

Let us first fix some notations: a local field K, with its residue field k_K, and $q := \#k_K$, and p is the characteristic of k_K. Its ring of integers $A := \mathscr{O}_K$ is a D.V.R with its unique maximal ideal $\mathfrak{m}_K$ generated by $\pi := \pi_K$.

Definition. Let $f \in A[[X]]$ be a formal power series, then f is said to be a Frobenius series if

(i) $f(X) = \pi X \mod \deg 2$.

(ii) $f(X) \equiv X^q \mod \pi$.

Example 1.2.1. $f(X) := \pi X + X^q$ is a Frobenius series. Also, when $K = \mathbb{Q}_p$, and $\pi = p$, then $f(x) := (1 + X)^p - 1$ is a Frobenius series.

Let us begin this section with the following

Lemma 1.2.2. *Let f, g be two Frobenius series, and $F(X) \in F[[X_1, ..., X_n]]$ be a formal power series in n-variables, then $f \circ F \equiv F(g, ..., g) \mod \pi$.*

Proof. We have $f \circ F(X_1, ..., X_n) \equiv F(X_1, ..., X_n)^q \mod \pi$, and $F(g(X_1), ..., g(X_n)) \equiv F(X_1^q, ..., X_n^q) \mod \pi$. And we can easily see that $F(X_1, ..., X_n)^q \equiv F(X_1^q, ..., X_n^q) \mod \pi$. □

Using this, we can prove the key lemma for this section

Lemma 1.2.3. *Let f, g be two Frobenius series, and $\psi(X_1, ..., X_n) := a_1X_1 + ... + a_nX_n$ a linear form in $A[X_1, ..., X_n]$. Then there exists a unique $F \in A[X_1, ..., X_n]$ such that*

(i) $F = \psi \mod \deg 2$

(ii) $f \circ F = F(g, ..., g)$

Proof. We will construct F from polynomials in $A[X_1, ..., X_n]$ by reduction with these conditions for all $r \geq 0$

(1)$F_r \in A[X_1, ..., X_n]$ is a polynomial of degree r.

(2) $f \circ F_r = F_r(g, ..., g) \mod \deg r + 1$.

(3) $F_{r+1} = F_r + E_{r+1}$, where E_{r+1} is a homogeneous polynomial of degree $r + 1$ in $A[X_1, ..., X_n]$.

Assume that such F_r are constructed, we let $F := F_r + E_{r+1} + E_{r+2} + ...$ Then it can be seen for all r

$$f(F(X_1, ..., X_n)) = f(F_r + \text{terms of degree} \geq r + 1) = f(F_r) \mod \deg(r + 1)$$

And because of condition (2) and (1), we have

$$f \circ F = F_r(g, ..., g) \mod \deg(r + 1) = F(g, ..., g) \mod \deg(r + 1)$$

So, we get $f \circ F = F(g, ..., g)$. Hence, it is sufficient for us to construct F_r. First, one can see that F_1 is exactly ψ, due to the condition (i), and the condition (ii) is also satisfied since

$$f(\psi(X_1, ..., X_n)) = \pi(a_1X_1 + ... + a_nX_n) \mod \deg 2$$

And also

$$\psi(g(X_1), ..., g(X_n)) = a_1g(X_1) + ... + a_ng(X_n) \equiv \pi(a_1X_1 + ... + a_nX_n) \mod \deg 2$$

And this follows that $F_1 = \psi$. Now, assume that we already constructed F_r, and we want to construct F_{r+1}. Let $F_{r+1} = F_r + E_{r+1}$. We have

$$f(F_r + E_{r+1}) = f(F_r) + \pi E_{r+1} \mod \deg(r + 2)$$

And

$$\begin{aligned} F_{r+1}(g, ..., g) &= F_r(g, ..., g) + E_{r+1}(g, ..., g) = \\ &= F_r(g, ..., g) + E_{r+1}(\pi X_1, ..., \pi X_n) \mod \deg(r + 2) \\ &= F_r(g, ..., g) + \pi^{r+1}E_{r+1}(X_1, ..., X_n) \mod \deg(r + 2) \end{aligned}$$

The last equality follows since E_{r+1} is homogeneous of degree $r + 1$. The condition (2) for F_r implies that $f \circ F_r = F_r(g, ..., g)$. And we want

$$f \circ F_{r+1} = F_{r+1}(g, ..., g)$$

And this is equivalent to say

$$E_{r+1} = \frac{F_r(g, ..., g) - f \circ F_r}{\pi(1 - \pi^r)}$$

But in Lemma 1.2.2, we have prove that $\pi|(F_r(g, ..., g) - f \circ F_r)$, and $(1 - \pi^r) \in A^\times$. So, we can construct E_{r+1} by this formula, and hence F_{r+1}. Now, the uniqueness of F follows easily from this construction. □

The latter development will be applications of Lemma 1.2.3. The first one is

Theorem 1.2.4. *Let f be a Frobenius series, the there exists a unique commutative formal group law F_f such that $f \in End(F_f)$.*

Proof. Based on Lemma 1.2.3, there exists a unique formal power series $F \in A[[X, Y]]$ such that
(i)$F(X, Y) = X + Y \mod \deg 2$.
(ii)$f \circ F = F(f, f)$

And we need to check that in fact F is a commutative formal group law. So we just need to check two things.

(1) $F(X, Y) = F(Y, X)$. Let $G_1 = F(X, Y), G_2 = F(Y, X)$, then $G_i = X + Y \mod \deg 2$, and also $f \circ G_i = G_i(f, f)$. So by the uniqueness in Lemma 1.2.3, we get $G_1 = G_2$.

(2) (Associativity) Let $G_1(X, Y, Z) = F(X, F(Y, Z)), G_2(X, Y, Z) = F(F(X, Y), Z)$, then $G_i = X + Y + Z \mod \deg 2$, and $f \circ G_i = G_i(f, f, f)$. So, by the uniqueness of Lemma 1.2.3 again, we get $G_1 = G_2$.

This follows directly that F is commutative formal group law. □

Definition. Let f be a Frobenius series, then such a commutative formal group law F_f in Theorem 1.2.4 is called a Lubin-Tate's formal group law .

Example 1.2.5. Let $K = \mathbb{Q}_p, \pi = p, f(X) = (1 + X)^p - 1$ is a Frobenius series, then $G_m(X, Y) = (1 + X)(1 + Y) - 1$ is a Lubin-Tate formal group law of f, as in Example 1.1.7 presented.

With the help of Lemma 1.2.3, we can now easily construct homomorphisms between two Lubin-Tate's formal group laws. Let f, g be two Frobenius series, then by Lemma 1.2.3, there exists a unique $[a]_{g,f} \in A[[X]]$ such that $[a]_{g,f} = aX \mod \deg 2$ and $g \circ [a]_{g,f} = [a]_{g,f} \circ f$.

Proposition 1.2.6. *Such an $[a]_{g,f}$ defined above is a homomorphism from F_f to F_g.*

Proof. Let $h := [a]_{g,f} = aX \mod \deg 2$, then we want to show $h \circ F_f = F_g(h, h)$. Let $H_1 := h \circ F_f$, and $H_2 := F_g(h, h)$. Then one can see both H_1, H_2 have linear term as $aX + aY$. Also,

$$g \circ H_1 = g \circ h \circ F_f = h \circ f \circ F_f = h \circ F(f, f) = H_1(f, f)$$

And

$$g \circ H_2 = g \circ F_g(h, h) = F_g(g \circ h, g \circ h) = F_g(h \circ f, h \circ f) = H_2(f, f)$$

So, by the uniqueness of Lemma 1.2.3, we get $H_1 = H_2$. This yields $[a]_{g,f}$ is a homomorphism from F_f to F_g. $\square$

Here is a nice corollary of the proposition above.

Corollary 1.2.7. *Let f, g be two Frobenius series, then $F_f \cong F_g$.*

Proof. One can see for $a \in A^\times$, then $[a]_{g,f} = aX \mod \deg 2$ defines an isomorphism between F_f and F_g, as presented in Lemma 1.1.6 $\square$

Proposition 1.2.8. *Let f be a Frobenius series, $a, b \in A$, then*

$$[ab]_{f,f} = [a]_{f,f}[b]_{f,f} = [ba]_{f,f} = [b]_{f,f}[a]_{f,f}$$

and

$$[a + b]_{f,f} = [a]_{f,f} + [b]_{f,f}$$

And hence, the map

$$\begin{aligned} A &\longrightarrow End(F_f) \\ a &\longmapsto [a]_{f,f} \end{aligned}$$

is an embedding of rings.

Proof. We can see that the four element above (in the ring $End(F_f)$) have the same linear term abX. We have $f \circ [ab]_{f,f} = [ab]_{f,f} \circ f$, and

$$f \circ [a]_{f,f} \circ [b]_{f,f} = [a]_{f,f} \circ f \circ [b]_{f,f} = [a]_{f,f} \circ [b]_{f,f} \circ f$$

Also, $f \circ [ba]_{f,f} = [ba]_{f,f} \circ f$. So, by the uniqueness of Lemma 2.3, we have $[ab]_{f,f} = [a]_{f,f}[b]_{f,f} = [ba]_{f,f} = [b]_{f,f}[a]_{f,f}$. The last equality follows by interchanging a, b in the first equality.

Similarly, we obtain $[a + b]_{f,f} = [a]_{f,f} + [b]_{f,f}$, since both have the same linear term $(a + b)X$. Hence, the map from A to $\mathrm{End}(F_f)$ is a ring homomorphism, and it is obviously injective. $\square$

We are now ready for the Lubin-Tate theory. For convenience, from now on, we can denote $[a]_{f,f} = [a]_f$.

1.3 Lubin-Tate extension

We assume the notations in Section 2, with $\overline{K}$ the algebraic closure of K. Let $M := \{z \in \overline{K} | v_K(z) > 0\}$ the maximal ideal of $\overline{K}$. Recall that for any $z_1, ..., z_n \in M$, and any power series $F(X_1, ..., X_n) \in A[[X_1, ..., X_n]]$, $F(z_1, ..., z_n)$ converges in $\overline{K}$, since norms of terms go to 0, when the indexes go to infinity.

Recall that if f is a Frobenius series, and F_f its corresponding Lubin-Tate's formal group law, we can equip M with the addition defined as $a +_{F_f} b = F_f(a, b)(\forall a, b \in M)$. This turns out $(M, +_{F_f})$ is an abelian group. We can further equip M with an A-module structure as $(a, z) := [a]_f(z)$ for all $z \in M$. This is well-defined, since

(i) $[1]_f(z) = z$.

(ii) $[a]_f(z_1 + z_2) = [a]_f F_f(z_1, z_2) = F_f([a]_f(z_1), [a]_f(z_2)) = [a]_f(z_1) +_{F_f} [a]_f(z_2)$.

(iii) $[ab]_f(z) = [a]_f \circ [b]_f(z)$. This follows from Proposition 1.2.8.

Let g be another Frobenius series, recall that for all $a \in A$, we can construct the map $[a]_{g,f} : F_f \to F_g$. This induces a homomorphism of abelian group

$$[a]_{g,f} : (M, +_{F_f}) \to (M, +_{F_g})$$

Remark 1.3.1. The homomorphism $[a]_{g,f}$ defined above is also an A-module homomorphism.

Proof. It is sufficient to prove that $[a]_{g,f} \circ [b]_f(z) = [b]_g \circ [a]_{g,f}$. The both power series have the same linear term abX. Also,

$$g \circ [a]_{g,f} \circ [b]_f = [a]_{g,f} \circ f \circ [b]_f = [a]_{g,f} \circ [b]_f \circ f$$

And furthermore,

$$g \circ [b]_g \circ [a]_{g,f} = [b]_g \circ g \circ [a]_{g,f} = [b]_g \circ [a]_{g,f} \circ f$$

So, the statement now follows by the uniqueness of Lemma 1.2.3. □

Via this remark, one can see for any $a \in A, [a]_f : (M, +_{F_f}) \to (M, +_{F_f})$ is an A-module homomorphism. And hence $\ker[a]_f$ is an A-submodule of $(M, +_{F_f})$. Let $a := \pi^n$, we obtain $\mathscr{F}_n := \ker[\pi^n]_f = \{z \in M | [\pi^n]_f(z) = 0\}$. Using the uniqueness of Lemma 1.2.3 again, we can see that $[\pi]_f = f, [\pi^2]_f = f \circ f, ..., [\pi^n]_f = f \circ f \circ ... \circ f$ (n terms).

Remark 1.3.2. $\mathscr{F}_n$ has a structure of $\mathscr{O}_K/\pi^n\mathscr{O}_K$-module, and we have a increasing sequence of A-modules

$$\mathscr{F}_1 \subset \mathscr{F}_2 \subset ... \subset \mathscr{F}_n$$

And hence, the increasing of field extensions

$$K \subset K_1 := K(\mathscr{F}_1) \subset ... \subset K_n := K(\mathscr{F}_n) \subset ... \subset K_\infty := \cup_{n\geq 1} K_n$$

Such sequence of field extensions is called Lubin-Tate's tower .

Proof. Assume that $a = b + c\pi^n$, for $a, b, c \in A$, we have for all $z \in \mathscr{F}_n$,

$$[a]_f(z) = [b + c\pi^n]_f(z) = [b]_f(z) +_{F_f} [c\pi^n]_f(z) = [b]_f(z) +_{F_f} [c]_f \circ [\pi^n]_f(z) = [b]_f(z)$$

And this yields $\mathscr{F}_n$ has a $\mathscr{O}_K/\pi^n\mathscr{O}_K$-module structure. The increasing sequences are easily obtain by the fact $f \in XA[[X]]$ and

$$[\pi^n]_f = f \circ f ... \circ f \text{ (n terms)}$$

□

From now on, we will deduce properties of Lubin-Tate tower. One can see that $\mathscr{F}_n$ is obviously dependent on the choice of f, but we will prove that it is not the case for K_n.

Lemma 1.3.3. *Let g be another Frobenius series with $\mathscr{F}'_n = \ker[\pi^n]_g$, then $K(\mathscr{F}_n) = K(\mathscr{F}'_n)$.*

Proof. Choose any $u \in A^\times$ with $[u]_{g,f} : F_f \xrightarrow{\sim} F_g$ is an isomorphism. This induces an isomorphism of A-module $(M, +_{F_f}) \xrightarrow{\sim} (M, +_{F_g})$. And also, it induces an $A/\pi^n A$-isomorphism $\mathscr{F}_n \xrightarrow{\sim} \mathscr{F}'_n$. Hence, in particular, we get $z \in \mathscr{F}_n$ iff $[u]_{g,f}(z) \in \mathscr{F}'_n$. But then, since $z \in M$, $[u]_{g,f}(z)$ converges in $K(z)$, we obtain $K(\mathscr{F}'_n) \subseteq K(\mathscr{F}_n)$. By symmetry, we obtain $K(\mathscr{F}_n) = K(\mathscr{F}'_n)$. $\square$

Via this proof, we can see the explore the algebraic properties of the $A/\pi^n A$-module $\mathscr{F}_n$, it is sufficient for us to choose a simple Frobenis series, $f(X) := \pi X + X^q$.

Lemma 1.3.4. *With f is chosen as above, the map $[\pi]_f : \mathscr{F}_n \to \mathscr{F}_{n-1}$ sending $z \mapsto [\pi]_f(z)$ is a surjective homomorphism of A-module, and its kernel is $\mathscr{F}_1$.*

Proof. One can see easily that $[\pi]_f$ is a well-defined homomorphism. Take any $z_{n-1} \in \mathscr{F}_{n-1}$, we want to find $z_n \in \mathscr{F}_n$, such that $[\pi]_f(z_n) = z_{n-1}$. One can see the equation $\pi X + X^q = z_{n-1}$ always has solutions in $\overline{K}$, and since $v_K(z_{n-1}) > 0$, such a solution z_n also lie in M. And we have $[\pi]_f(z_n) = z_{n-1}$. This yields $[\pi^n]_f(z_n) = 0$, i.e. $z_n \in \mathscr{F}_n$. And hence, $[\pi]_f$ is a surjective homomorphism. The kernel of $[\pi]_f$ now directly follows. $\square$

For the main results of this section, we need the following

Lemma 1.3.5. *Let $z \in M$, then the polynomial $g(X) = z + \pi X + X^q$ has distinct roots in $\overline{K}$.*

Proof. We have $g'(X) = \pi + qX^{q-1}$, which is π when $char(K) = p$. Hence, the statement is obviously true when $char(K) > 0$. Assume for now $char(K) = 0$, and that there exists some $x \in \overline{K}$, with $g(x) = g'(x) = 0$, then $x^{q-1} = -\pi/q$. This yields $|x| \geq 1$, because $|\pi/q| \geq 1$. From this, $|\pi x| < |x| \leq |x|^q$, which follows that $|z| = |\pi x + x^q| \geq 1$. It is a contradiction, since $v_p(z) > 0$. $\square$

We are now ready the for the an important result

Proposition 1.3.6. *$\mathscr{F}_n$ is a free $A/\pi^n A$-module of rank 1. This implies $Aut_{A/\pi^n A}(\mathscr{F}_n) \cong (A/\pi^n A)^\times$.*

Proof. We will prove this fact the induction. When $n = 1$, the equation $f(X) = \pi X + X^q = X(\pi + X^{q-1})$ has q-distinct roots in $\overline{K}$ (Lemma 1.3.5), and $\mathscr{F}_1$ has a structure of $A/\pi A$-vector space structure. This yields $\mathscr{F}_1$ is a 1-dimensional $A/\pi A$-vector space.

Assume that the statement holds to $n-1 (n \geq 2)$, then there exists z_{n-1}, the generator of $\mathscr{F}_{n-1}$, and an isomorphism $\phi_{n-1} : A/\pi^{n-1}A \xrightarrow{\sim} \mathscr{F}_{n-1}$ defined as $a \mapsto [a]_f(z_{n-1})$. By using Lemma 1.3.4, there exists $z_n \in \mathscr{F}_n$, with $[\pi]_f(z_n) = z_{n-1}$. Also, the map $\phi_n : A/\pi^n A \xrightarrow{F}{}_n$ defined as $a \mapsto [a]_f(z_n)$ making the following diagram commute:

$$\begin{tikzcd}
0 \arrow[r] & k \cong \pi^{n-1}A/\pi^n A \arrow[r] \arrow[d] & A/\pi^n A \arrow[r] \arrow[d, "\phi_n"] & A/\pi^{n-1}A \arrow[r] \arrow[d, "\phi_{n-1}"] & 0 \\
0 \arrow[r] & \mathscr{F}_1 \arrow[r] & \mathscr{F}_n \arrow[r, "{[\pi]_f}"] & \mathscr{F}_{n-1} \arrow[r] & 0
\end{tikzcd}$$

where rows are exact, with the first and the last vertical arrows are isomorphisms. This yields the arrow in the middle is an isomorphism, too. Hence, $\mathscr{F}_n$ is a free $A/\pi^n A$-module of rank 1. The later statement is now clear. $\square$

Because $\#A/\pi^n A = q^n$, we have $\#\mathscr{F}_n = q^n$. And hence $[K_n : K] < +\infty$. And we conclude this section by the following

Theorem 1.3.7. *The Lubin-Tate's tower*

$$K \subset K_1 \subset ... \subset K_n$$

is a tower of totally ramified Galois extension, with $[K_n : K] = q^{n-1}(q-1)$. *Moreover, if* z_n *is a generator for* $\mathscr{F}_n$ *as* $A/\pi^n A$*-module, then* z_n *is a uniformizer for* K_n. *And that* $Gal(K_\infty/K) \cong A^\times$.

Proof. For any $\sigma \in Gal(\overline{K}/K)$, because σ acts as identity map in K, σ acts on $(M, +_{F_f})$ as an A-module isomorphism, since for all $z, z_1, z_2 \in M$, $\sigma([a]_f(z)) = [a]_f(\sigma(z))$, and also $\sigma F_f(z_1, z_2) = F_f(\sigma(z_1), \sigma(z_2))$. From this, σ induces an $A/\pi^n A$-module automorphism on $\mathscr{F}_n$. This yields by Proposition 1.3.6, for each σ, there exists only one $\phi_\sigma \in Aut_{A/\pi^n A}(\mathscr{F}_n)$, such that $\sigma(z) = \phi_\sigma(z)$, for all $z \in \mathscr{F}_n$. And hence, one obtain an embedding from $Gal(K_n/K)$ to $Aut_{A/\pi^n A}(\mathscr{F}_n)$.

One can see that $K_1 = K(\mathscr{F}_1)$, i.e. K_1 is obtained by adjoining roots of the polynomial $f(X) = \pi X + X^q$, which is separable. Hence, K_1/K is Galois. If $z_1 \neq 0$ is a root of $f(X)$, we can see that z_1 is a root of $g(X) := \pi + X^{q-1}$, which is an Eisentein polynomial. Hence, $[K_1 : K] \geq q-1$ and z_1 is a uniformizer for K_1. Due to our previous argument, we have $[K_1 : K] = q-1$.

For $n \geq 2$, assume that the statements hold for $n-1$, we can see $K(\mathscr{F}_n)$ is an extension of $K(\mathscr{F}_{n-1})$ by adjoining roots of the polynomial $\pi X + X^q = z_{n-1}$, for all z_{n-1}: generator of $\mathscr{F}_{n-1}$ as $A/\pi^{n-1}A$-module. For such z_{n-1}, the polynomial $g(X) := -z_{n-1} + \pi X + X^q$ is Eisentein of degree q over K_{n-1} (since z_{n-1} is a uniformizer for K_{n-1}), and by Lemma 1.3.5, $g(X)$ is separable. This implies K_n/K_{n-1} is totally ramified Galois extension of degree at least q. Hence, one obtains $[K_n : K] \geq q^{n-1}(q-1)$. But then, due to our previous argument, $\#\mathrm{Gal}(K_n/K) \leq q^{n-1}(q-1)$. It follows directly that $\mathrm{Gal}(K_n/K) \cong (A/\pi^n A)^\times$, and that $[K_n : K] = q^{n-1}(q-1)$, and that K_n/K_{n-1} is totally ramified, and z_n is a uniformizer of K_n since the polynomial $g(X)$ defined above is Eisentein. With this result at hand, we obtain

$$\mathrm{Gal}(K_\infty/K) = \varprojlim \mathrm{Gal}(K_n/K) \cong \varprojlim (A/\pi^n A)^\times \cong A^\times$$

□

Remark 1.3.8. One can see that the Lubin-Tate construction above basically gives us the 1-dimensional representation of the absolute Galois group. It is very similar to the 2-dimensional representation obtained by using Tate modules on elliptic curves.

Example 1.3.9. Let $K = \mathbb{Q}_p, \pi = p$, with Frobenius series $f(X) := (1+X)^p - 1$, then the Lubin-Tate formal group associated to f is G_m. In this case, $[p]_f = f(X) = (1+X)^p - 1$, and $\mathscr{F}_1$ consists of roots of $f(X)$. Hence, $\mathscr{F}_1 = \{z \in \overline{\mathbb{Q}_p} | (1+z)^p = 1\}$, and $\mathbb{Q}_p(\mathscr{F}_1) = \mathbb{Q}_p(\zeta_p)$, where ζ_p is a primitive p-th root of unity. Similarly, $\mathbb{Q}_p(\mathscr{F}_n) = \mathbb{Q}_p(\zeta_{p^n})$, where ζ_{p^n} is a primitive p^n-th root of unity. And hence, we obtain $K_\infty = \mathbb{Q}_p^\infty$, which is the field extension of $\mathbb{Q}_p$ obtained by adjoining all p^n-th root of unity. And it follows from the proposition above that $\mathrm{Gal}(\mathbb{Q}_p^\infty/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$.

Chapter 2

Ramified Witt vectors

The theory of ramified Witt vectors is very important for our later applications about the un-tilting process and the construction the Fontaine's ring A in the next chapters. Our main reference for this section is [Sch17]. We fix L a non-archimedean local field, with $\mathcal{O}$ its ring of integers with a uniformizer π, k its residue field, and $q = \#k$, B an $\mathcal{O}$-algebra. For any set R, we denote $R^{\mathbb{N}_0} := \{(r_0, r_1, ...)|r_i \in R\}$, and for any map $\rho : R_1 \to R_2$ of sets, we denote

$$\begin{aligned} \rho^{\mathbb{N}_0} : R_1^{\mathbb{N}_0} &\longrightarrow R_2^{\mathbb{N}_0} \\ (r_0, r_1, ...) &\longmapsto (\rho(r_0), \rho(r_1), ...) \end{aligned}$$

2.1 The ring of ramified Witt vectors

We can consider the **n-th Witt polynomial** defined by

$$\Phi_n(X_0, ..., X_n) = X_0^{q^n} + \pi X_1^{q^{n-1}} + ... + \pi^{n-1} X_{n-1}^q + \pi^n X_n$$

Inductively, we have

$$\Phi_0(X_0) = X_0, \Phi_n(X_0, ..., X_n) = \Phi_{n-1}(X_0^q, ..., X_{n-1}^q) + \pi^n X_n = X_0^{q^n} + \pi\Phi_{n-1}(X_1, ..., X_n)$$

In this section, we will prove that $B^{\mathbb{N}_0}$ with the multiplication and addition formulas defined related to Witt polynomials is a ring, which is called the ring of ramified Witt's vectors, denoted by $W(B)$. We will begin with a couple of lemmas

Lemma 2.1.1. *Let $b, c \in B$ such that $b \equiv c \mod \pi^n B$, then $b^{q^n} \equiv c^{q^n} \mod \pi^{m+n} B$*

Proof. In the case $\mathrm{char} L = p$, we have $b^{q^n} - c^{q^n} = (b - c)^{q^n} \equiv 0 \mod \pi^{m+n} B$. Otherwise, the statement follows directly from induction. $\square$

Lemma 2.1.2. *Let $b_0, ..., b_n, c_0, ..., c_n$ be elements in B*

1. *Assume that $b_i \equiv c_i \mod \pi^m B$ for all $0 \leq i \leq n$, then $\Phi_n(b_0, ..., b_n) = \Phi_n(c_0, ..., c_n) \mod \pi^{m+n} B$.*
2. *If $\pi 1_B$ is not a zero divisor in B, and $b_i \equiv c_i \mod \pi^m B$ for all $0 \leq i \leq n-1$, then $\Phi_n(b_0, ..., b_n) \equiv \Phi_n(c_0, ..., c_n) \mod \pi^{m+n} B$ iff $b_n \equiv c_n \mod \pi^m B$.*

Proof. 1. We have $\Phi_0(b_0) = b_0 \equiv \Phi_0(c_0) = c_0 \mod \pi^n B$. Using induction, assume that the statement holds for k pairs (b_i, c_i). Because $b_{k+1} \equiv c_{k+1} \mod \pi^n B$, then by Lemma 2.1.1, and induction hypothesis, we get

$$\Phi_{k+1}(b_0, ..., b_{k+1}) = b_0^{q^k} + \pi\Phi_k(b_1, ..., b_k) \equiv c_0^{q^k} + \pi\Phi_k(c_1, ..., c_k) = \Phi_{k+1}(c_0, ..., c_{k+1}) \mod \pi^{k+n} B$$

2. Assume that $\Phi_n(b_0, ..., b_n) \equiv \Phi_n(c_0, ..., c_n) \mod \pi^{m+n} B$, one has

$$\begin{cases} \Phi_n(b_0, ..., b_n) = \Phi_{n-1}(b_0^q, ..., b_{n-1}^q) + \pi^n b_n \\ \Phi_n(c_0, ..., c_n) = \Phi_{n-1}(c_0^q, ..., c_{n-1}^q) + \pi^n c_n \end{cases}$$

And $b_i \equiv c_i \mod \pi^n B$ for all $0 \leq i \leq n-1$ yields $b_i^q \equiv c_i^q \mod \pi^{m+1} B$. And it follows from the previous part that $\Phi_{n-1}(b_0^q, ..., b_{n-1}^q) \equiv \Phi_{n-1}(c_0^q, ..., c_{n-1}^q) \mod \pi^{m+n} B$. Because $\pi 1_B$ is not a zero divisor, we then get $b_n \equiv c_n \mod \pi^m B$. □

One can see that $B^{\mathbb{N}_0}$ is a ring with multiplication and addition are induced from B. We can define some maps

$$\begin{aligned} f_B : B^{\mathbb{N}_0} &\longrightarrow B^{\mathbb{N}_0} \\ (b_0, b_1, ...) &\longmapsto (b_1, b_2, ...) \end{aligned}$$

$$\begin{aligned} v_B : B^{\mathbb{N}_0} &\longrightarrow B^{\mathbb{N}_0} \\ (b_0, b_1, ...) &\longmapsto (0, \pi b_0, \pi b_1, ...) \end{aligned}$$

$$\begin{aligned} \Phi_B : B^{\mathbb{N}_0} &\longrightarrow B^{\mathbb{N}_0} \\ (b_0, b_1, ...) &\longmapsto (\Phi_0(b_0), \Phi_1(b_0, b_1), ...) \end{aligned}$$

We have f_B is an $\mathcal{O}$-algebra endomorphism of $B^{\mathbb{N}_0}$, and the map v_B is an $\mathcal{O}$-module endomorphism of B. We will focus no Φ_B.

Lemma 2.1.3.

1. *If $\pi 1_B$ is not a zero divisor, then Φ_B is injective.*
2. *If $\pi 1_B \in B^\times$, then Φ_B is bijective.*

Proof.

1. Assume that $\Phi_B((b_0, b_1, ...)) = \Phi_B((c_0, c_1, ...))$, then we have
$$b_0 = \Phi_0(b_0) = \Phi_0(c_0) = c_0$$
$$\Phi_{n+1}(b_0, b_1, ..., b_{n+1}) = \Phi_n(b_0^q, ..., b_n^q) + \pi^{n+1} b_{n+1} = \Phi_n(c_0^q, ..., c_n^q) + \pi^{n+1} c_{n+1}$$
And because $\pi 1_B$ is not a zero divisor, we get $b_{n+1} = c_{n+1}$ by induction, and this yields $(b_0, b_1, ...) = (c_0, c_1, ...)$.
2. Take any $(c_0, c_1, ...) \in B^{\mathbb{N}_0}$, we have to find $(b_0, b_1, ...) \in B^{\mathbb{N}_0}$ such that $\Phi_B(b_0, b_1, ...) = (c_0, c_1, ...)$. It is equivalent to have
$$b_0 = c_0, \pi b_1 = c_1 - b_0^q, \pi^2 b_2 = c_2 - b_0^{q^2} - \pi b_1^q, ...$$
Because $\pi 1_B$ is invertible, we ca always find such b_i. And by the first part, Φ_B is bijective.

□

We denote $\mathrm{End}_{\mathcal{O}}(B)$ the ring of all $\mathcal{O}$-algebra endomorphism of B. In case $\mathrm{End}_{\mathcal{O}}(B)$ has an element look like Frobenius, we can describe the image of Φ_B via the following

Proposition 2.1.4. *Assume that there exists θ in $End_{\mathcal{O}}(B)$ such that $\theta(b) \equiv b^q \mod \pi B$, then*

1. *Let $b_0, ..., b_{n-1}$ be in B, we denote $u_{n-1} := \Phi_{n-1}(b_0, b_1, ..., b_{n-1})$, and $u_n \in B$, then $u_n = \Phi_n(b_0, ..., b_n)$ for some $b_n \in B$ iff $\theta(u_{n-1}) \equiv u_n \mod \pi^n B$.*

2. Denote $B' = \mathrm{im}\Phi_B$, then

$$B' = \{(b_0, b_1, ...) | \theta(b_i) \equiv b_{i+1} \mod \pi^{i+1}B\}$$

And $f_B(B') \subseteq B', v_B(B') \subseteq B'$.

Proof.

1. Assume that $u_n = \Phi_n(b_0, ..., b_n) = \Phi_{n-1}(b_0^q, ..., b_{n-1}^q) + \pi^n b_n$, we then have

$$\theta(u_{n-1}) = \theta(\Phi_{n-1}(b_0, b_1, ..., b_{n-1})) = \Phi_{n-1}(\theta(b_0), ..., \theta(b_{n-1}))$$

Because $\theta(b_i) \equiv b_i^q \mod \pi B$, by Lemma 2.1.2, we get

$$\Phi_{n-1}(b_0^q, ..., b_{n-1}^q) \equiv \Phi_{n-1}(\theta(b_0), ..., \theta(b_{n-d})) \mod \pi^n B \tag{2.1}$$

So, this yields $\theta(u_{n-1}) \equiv u_n \mod \pi^n B$. Conversely, because 2.1 always holds, the assumption $\theta(u_{n-1}) \equiv u_n \mod \pi^n B$ implies that $u_n \equiv \Phi_{n-1}(b_0^q, ..., b_{n-1}^q)$, i.e. there exists some $b_n \in B$ such that $u_n = \Phi_{n-1}(b_0^q, ..., b_{n-1}^q) + \pi^n b_n = \Phi_n(b_0, ..., b_n)$.

2. Let $(b_0, b_1, ...) \in B^{\mathbb{N}_0}$, we have

$$\Phi_B(b_0, b_1, ...) = (\Phi_0(b_0), \Phi_1(b_0, b_1), ...) = (b_0, b_0^q + \pi b_1, ...)$$

And hence, $(c_0, c_1, ...) \in \mathrm{im}\Phi_B$ iff there exists some $b_0, b_1, ...$ in B such that

$$c_0 = b_0, c_1 = b_0^q + \pi b_1 = \Phi_1(b_0, b_1), ...$$

By the previous part, this occurs iff $\theta(c_i) \equiv c_{i+1} \mod \pi^{i+1}B$. And this yields

$$B' = \{(b_0, b_1, ...) | \theta(b_i) \equiv b_{i+1} \mod \pi^{i+1}B\}$$

□

The proposition above is particularly important in this and later chapter. We will discuss about its applications. First, denote $A = \mathcal{O}[X_0, X_1, ..., Y_0, Y_1, ...]$. We define $\theta \in \mathrm{End}_{\mathcal{O}}(A)$ by $\theta(X_i) = X_i^q, \theta(Y_i) = Y_i^q$.

Lemma 2.1.5. *For any $a \in A$, we have $\theta(a) \equiv a^q \mod \pi A$.*

Proof. Consider $A' := \{a \in A | \theta(a) \equiv a^q \mod \pi A\}$. It is a $\mathcal{O}$-subalgebra of A. Because $q = \#k$, for all $\lambda \in \mathcal{O}$, we have $a^q \equiv a \mod \pi A$, and because θ fixes $\mathcal{O}$, we have $\mathcal{O} \subset A'$. This yields $A' = A$. □

Let $X := (X_0, X_1, ...) \in A^{\mathbb{N}_0}, Y := (Y_0, Y_1, ...) \in A^{\mathbb{N}_0}$, we have

$$\Phi_A(X) + \Phi_A(Y) = (X_0 + Y_0, X_0^q + Y_0^q + \pi X_1 + \pi Y_1, ...)$$

By Proposition 2.1.4 (1), we have

$$\theta(\Phi_n(X_0, ..., X_n)) \equiv \Phi_{n+1}(X_0, ..., X_{n+1}) \mod \pi^{n+1}B$$

And this yields

$$\theta(\Phi_n(X_0, ..., X_n) + \Phi_n(Y_0, ..., Y_n)) = \theta(\Phi_n((_0, ..., (_n)X_0, ..., X_n)) + \theta(\Phi_n((_0, ..., (_n)Y_0, ..., Y_n)) \equiv$$
$$\equiv \Phi_{n+1}(X_0, ..., X_{n+1}) + \Phi_{n+1}(Y_0, Y_1, ..., Y_{n+1}) \mod \pi^{n+1}B$$

Hence, by Proposition 2.1.4 (2), there exists $S = (S_0, S_1, ...) \in A^{\mathbb{N}_0}$ such that

$$\Phi_A(S) = \Phi_A(X) + \Phi_A(Y)$$

And it is obvious that $\pi 1_A$ is not a zero divisor, by Lemma 2.1.3, the existstence of S is unique. Similarly, we obtain that, there exists a unique P, I, F in $A^{\mathbb{N}_0}$, such that

$$\Phi_A(P) = \Phi_A(X) + \Phi_A(Y), \Phi_A(I) = -\Phi_A(X), \Phi_A(F) = f_A(\Phi_A(X))$$

Say another words, we obtain

Proposition 2.1.6. *There exists $S_n, P_n \in \mathcal{O}[X_0, ..., X_n, Y_0, ..., Y_n]$ and $I_n \in \mathcal{O}[X_0, ..., X_n], F_n \in \mathcal{O}[X_0, ..., X_{n+1}]$, such that*

$$\begin{cases} \Phi_n(S_0, ..., S_n) = \Phi_n(X_0, ..., X_n) + \Phi_n(Y_0, ..., Y_n) \\ \Phi_n(P_0, ..., P_n) = \Phi_n(X_0, ..., X_n)\Phi_n(Y_0, ..., Y_n) \\ \Phi_n(I_0, ..., I_n) = -\Phi_n(X_0, ..., X_n) \\ \Phi_n(F_0, ..., F_n) = \Phi_n(X_0, ..., X_{n+1}) \end{cases} \tag{2.2}$$

Lemma 2.1.7. *For all $n \geq 0$, $F_n \equiv X_n^q \mod \pi A$.*

Proof. Using 2.2, when $n = 0$, we have $F_0 = X_0^q + \pi X_1$, and this yields $F_0 \equiv X_0^q \mod \pi A$. Assume that the statement holds for all integer $k \leq n$. We have

$$\Phi_{n+1}(F_0, F_1, ..., F_{n+1}) = \Phi_n(F_0^q, ..., F_n^q) + \pi^{n+1} F_{n+1}$$

And

$$\Phi_{n+2}(X_0, X_1, ..., X_{n+2}) = \Phi_{n+1}(X_0^q, ..., X_{n+1}^q) + \pi^{n+2} X_{n+2} =$$

$$= \Phi_n(X_0^{q^2}, ..., X_n^{q^2}) + \pi^{n+1} X_{n+1}^q + \pi^{n+2} X_{n+1}$$

By induction hypothesis, $F_i \equiv X_i^q \mod \pi A$, and $F_i^q \equiv X_i^{q^2} \mod \pi^2 A$, for all $0 \leq i \leq n$. From Lemma 2.1.2, we get

$$\Phi_n(F_0^q, ..., F_n^q) \equiv \Phi_n(X_0^{q^2}, ..., X_n^{q^2}) \mod \pi^{n+2} A$$

And the identity in 2.2 implies that when we reduce modulo π^{n+2}, we will get

$$F_{n+1} \equiv X_{n+1}^q$$

□

We are now ready for the definition of the ring of(ramified) Witt's vectors $W(B)$. Let B be an $\mathcal{O}$-algebra, as sets, we identify $W(B) := B^{\mathbb{N}_0}$, and the multiplication and addition on $W(B)$ are defined to be

$$\begin{cases} (a_n)_n \boxplus (b_n)_n = (S_n(a_0, ..., a_n, b_0, ..., b_n))_n \\ (a_n)_n \boxdot (b_n)_n = (P_n(a_0, ..., a_n, b_0, ..., b_n))_n \end{cases} \tag{2.3}$$

Proposition 2.1.8. *W(B), with the addition and multiplication in 2.3 is a commutative ring, with $(0, 0, ...)$ is the zero element, and $(1, 0, 0, ...)$ is the identity element, and the inverse of $(a_n)_n \in W(B)$ is $(I_n(a_0, ..., a_n))_n$. Moreover, $\Phi_B : W(B) \to B^{\mathbb{N}_0}$ is a ring homomorphism.*

Proof. Let us denote $B_1 := \mathcal{O}[X_b | b \in B]$, with the map $\rho : B_1 \to B$ defined by $\rho(X_b) = b$ as an $\mathcal{O}$-algebra homomorphism. Let us denote $B_1' := \Phi_{B_1}(B_1^{\mathbb{N}_0})$. Note that by Proposition 2.1.6, for any $b, c \in B_1^{\mathbb{N}_0}$, $\Phi_{B_1}(b) + \Phi_{B_1}(c) \in \operatorname{im}(\Phi_{B_1}) = B_1'$. Because B_1' is in bijection with $B_1^{\mathbb{N}_0}$ by Lemma 2.1.2, we can introduce the new addition and multiplication in B_1 via the bijective map $B_1^{\mathbb{N}_0} \xrightarrow{\Phi_{B_1}} B_1'$. They are defined as follows

$$b \oplus c := \Phi_{B_1}^{-1}(\Phi_{B_1}(b) + \Phi_{B_1}(c)), b \odot c := \Phi_{B_1}^{-1}(\Phi_{B_1}(b) + \Phi_{B_1}(c))$$

Via this definition, we have

$$\Phi_{B_1}(b \oplus c) = \Phi_{B_1}(b) + \Phi_{B_1}(c), \Phi_{B_1}(b \odot c) = \Phi_{B_1}(b)\Phi_{B_1}(c)$$

Via $\oplus, \odot$, $B_1^{\mathbb{N}_0}$ now becomes a ring, and it can be seen from the definition of Φ_{B_1} that

$$\Phi_{B_1}(1, 0, ..., 0, ...) = (1, 1, ...), \Phi_{B_1}(0, 0, ...) = (0, 0, ...)$$

And now, the ring law on $B_1^{\mathbb{N}_0}$ induces the ring law on $B^{\mathbb{N}_0}$ via $\rho^{\mathbb{N}_0}$, by sending each coordinate X_i of $B_1^{\mathbb{N}_0}$ to the corresponding coordinate $\rho(X_i)$ in $B^{\mathbb{N}_0}$. By 2.2 and 2.3, we can see that, on $W(B)$

$$\Phi_B((a_n)_n \boxplus (b_n)_n) = \Phi_B((a_n)_n) + \Phi_B((b_n)_n), \Phi_B((a_n)_n \boxdot (b_n)_n) = \Phi_B((a_n)_n)\Phi_B((b_n)_n)$$

Hence, $\boxplus, \boxdot$ are exactly the addition and multiplication on $W(B)$ induced from $\oplus, \odot$ on $N_0^{\mathbb{N}_0}$. The statements now follows. $\square$

Definition. The ring W(B) above is called the **ring of ramified Witt vectors** with coefficients in L. In some cases, to distinguish, we will write $W(B)_L$ instead of $W(B)$.

We next introduce the notion of Teichmuller lifts.

Definition. Let B be an $\mathcal{O}$-algebra, we denote the map

$$\begin{aligned} \tau : B &\longrightarrow W(B) \\ b_0 &\longmapsto (b_0, 0, ...) \end{aligned}$$

the **Teichmuller lift**.

Lemma 2.1.9. *The map τ above is multiplicative.*

Proof. Due to the definition of the multiplication in $W(B)$ in 2.4, and by 2.2, we get $P_0(X_0, Y_0) = X_0Y_0$, and hence, it is sufficient to prove that $\widetilde{P_n}(X_0, Y_0) := P_n(X_0, 0, ..., 0, Y_0, 0, ..., 0) = 0$, for any $n \geq 1$. In the case $n = 1$, we have

$$P_0^q + \pi\widetilde{P_1} = \Phi_1(P_0, \widetilde{P_1}) = \Phi_n(X_0, 0)\Phi_n(Y_0, 0) = (X_0Y_0)^q$$

And since $\pi 1_A$ is not a zero disivor, we get $\widetilde{P_1} = 1$. For $n > 1$, $\widetilde{P_n} = 1$ follows easily by induction, and the same argument. $\square$

2.2 Functorial properties of Witt vectors

With notations as in the first section, we will study the functorial properties of Witt's vectors. Begin with two $\mathcal{O}$-algebras B_1, B_2, and $\rho : B_1 \to B_2$ an $\mathcal{O}$-algebra homomorphism. One can define

$$\begin{aligned} W(\rho) : W(B_1) &\longrightarrow W(B_2) \\ (b_0, b_1, ...) &\longmapsto (\rho(b_0), \rho(b_1), ...) \end{aligned}$$

Lemma 2.2.1.

1. *The following diagram is commutative*

$$\begin{tikzcd} B_1^{\mathbb{N}_0} \arrow[r, "\rho^{\mathbb{N}_0}"] & B_2^{\mathbb{N}_0} \\ W(B_1) \arrow[u, "\Phi_{B_1}"] \arrow[r, "W(\rho)"'] & W(B_2) \arrow[u, "\Phi_{B_2}"'] \end{tikzcd}$$

2. *The map $W(\rho)$ defined above is a ring homomorphism.*

Proof.

1. We have
$$\rho^{\mathbb{N}_0}(\Phi_{B_1}(b_0, b_1, ...)) = \rho^{\mathbb{N}_0}(\Phi_0(b_0), \Phi_1(b_0, b_1), ...) = (\rho \circ \Phi_n(b_0, ..., b_n))_n$$

   Note that since ρ is an $\mathcal{O}$-algebra homomorphism, ρ and Φ_n commute, and this yields

$$(\rho \circ \Phi_n(b_0, ..., b_n))_n = (\Phi_n(\rho(b_0), ..., \rho(b_n)))_n = \Phi_{B_2}(W(\rho))$$

2. We have

$$W(\rho)((a_n)_n \boxplus (b_n)_n) = W(p)(S_n(a_0, ..., a_n, b_0, ..., b_n)_n) = (\rho(S_n(a_0, ..., a_n, b_0, ..., b_n)))_n$$

Because $S_n \in \mathcal{O}[X_0, ..., X_n, Y_0, ..., Y_n]$, ρ and S_n commute, and hence

$$(\rho(S_n(a_0, ..., a_n, b_0, ..., b_n)))_n = (S_n(\rho(a_0), ..., \rho(a_n), \rho(b_0), ..., \rho(b_n)))_n = W(\rho)((a_n)_n) \boxplus W(\rho)((b_n)_n)$$

The similar arguments can also be applied for $\boxdot$, and this yields $W(\rho)$ is a ring homomorphism.

$\square$

Consider the map

$$\begin{aligned} \sigma : \mathcal{O} &\longrightarrow \mathcal{O}^{\mathbb{N}_0} \\ \lambda &\longmapsto (\lambda, \lambda, ...) \end{aligned}$$

Let us apply the second part of Proposition 2.1.4 to $B := \mathcal{O}, \theta := id$, this ensures the existence of the map

$$\begin{aligned} \Omega : \mathcal{O} &\longrightarrow W(\mathcal{O}) \\ \lambda &\longmapsto (\Omega_0(\lambda), \Omega_1(\lambda), ...) \end{aligned}$$

such that the diagram

$$\begin{tikzcd} \mathcal{O} \arrow[r, "\Omega"] \arrow[dr, "\sigma"'] & W(\mathcal{O}) \arrow[d, "\Phi_{\mathcal{O}}"] \\ & \mathcal{O}^{\mathbb{N}_0} \end{tikzcd}$$

is commutative. Let us denote $\mathcal{O}' := \text{im}(\Phi_{\mathcal{O}})$, then the map $\Phi_{\mathcal{O}}$ is a ring isomorphism between $W(\mathcal{O})$ and $\mathcal{O}'$, since π is not a zero divisor in $\mathcal{O}$. And $\sigma : \mathcal{O} \to \mathcal{O}'$ is also a ring homomorphism. Hence, Ω is also a ring homomorphism. This makes $W(\mathcal{O})$ becomes an $\mathcal{O}$-algebra.

Proposition 2.2.2. *Let B be an $\mathcal{O}$-algebra, then $W(B)$ is an $\mathcal{O}$-algebra. Furthermore, Φ_B, Φ_n are $\mathcal{O}$-algebra homomorphisms, for all n.*

Proof. Let ρ be the canonical map from $\mathcal{O}$ to B. From Lemma 2.2.1, and the diagram above, we obtain the following commutative diagram

$$\begin{tikzcd} \mathcal{O} \arrow[r, "\Omega"] \arrow[dr, "\sigma"'] & W(\mathcal{O}) \arrow[r, "W(\rho)"] \arrow[d, "\Phi_{\mathcal{O}}"] & W(B) \arrow[d, "\Phi_B"] \\ & \mathcal{O}^{\mathbb{N}_0} \arrow[r, "\rho^{\mathbb{N}_0}"'] & B^{\mathbb{N}_0} \end{tikzcd} \tag{2.4}$$

And this makes $W(B)$ an $\mathcal{O}$-algebra, and for any $\lambda \in \mathcal{O}, b \in W(B)$, we have

$$\lambda b = W(\rho)\Omega(\lambda) \boxdot b$$

And by 2.4 again, we obtain the following diagram

$$\begin{tikzcd} W(B) \arrow[r, "\Phi_B"] \arrow[d, ".\lambda"'] & B^{\mathbb{N}_0} \arrow[d, ".\lambda"] \\ W(B) \arrow[r, "\Phi_B"] & B^{\mathbb{N}_0} \end{tikzcd}$$

This diagram is commutative, since Φ_B is a ring homomorphism and

$$\Phi_B(\lambda b) = \Phi_B(W(\rho)\Omega(\lambda) \boxdot b) = \Phi_B(W(\rho)\Omega(\lambda))\Phi_B(b) = \rho^{\mathbb{N}_0}(\sigma(\lambda))\Phi_B(b) = (\lambda, \lambda, ...)\Phi_B(b) = \lambda\Phi_B(b)$$

where the third identity follows from 2.4. Hence, one gets Φ_B is an $\mathcal{O}$-algebra homomorphism.

Finally, let us denote $p_n : B^{\mathbb{N}_0} \to B$ the projection map to the n-th coordinate. It then follows from the commutative diagram

$$\begin{tikzcd} W(B) \arrow[r, "\Phi_B"] \arrow[dr, "\Phi_n"'] & B^{\mathbb{N}_0} \arrow[d, "p_n"] \\ & B \end{tikzcd}$$

that $\Phi_n : W(B) \to B$ is also an $\mathcal{O}$-algebra homomorphism. □

Using the commutative diagram in Lemma 2.2.1, and the method of the proof above, we have

Proposition 2.2.3.

1. *Let $\rho : B_1 \to B_2$ be an $\mathcal{O}$-algebra homomorphism of $\mathcal{O}$-algebras, then $W(\rho) : W(B_1) \to W(B_2)$ is also an $\mathcal{O}$-algebra homomorphism.*

2. *The functor*

$$\begin{aligned} W : \mathcal{O}\text{-}alg &\longrightarrow \mathcal{O}\text{-}alg \\ B &\longmapsto W(B) \end{aligned}$$

is a well-defined exact functor.

Proof.

1. Let $\rho_1 : \mathcal{O} \to B_1$ and $\rho_2 : \mathcal{O} \to B_2$ be the canonical maps. Then $\rho : B_1 \to B_2$ is an $\mathcal{O}$-algebra homomorphism implies that $\rho \circ \rho_1 = \rho_2$. And it follows that $W(\rho_2) = W(\rho) \circ W(\rho_1)$. And for all $\lambda \in \mathcal{O}, b \in B_1$, we have

$$W(\rho)(\lambda b) = W(\rho)(W(\rho_1)(\Omega(\lambda)) \boxdot b) = W(\rho)(W(\rho_1)(\Omega(b))) \boxdot W(b) =$$

$$= W(\rho_2)(\Omega(\lambda)) \boxdot W(\rho)(b) = \lambda W(\rho)(b)$$

where the first and the last identity follows from the explicit description of the action from $\mathcal{O}$ to $W(B_i)(i = 1, 2)$ described in the proof of the proposition above, the second identity follows from the fact that $W(\rho)$ is a ring homomorphism, and the third identity is obtained since $W(\rho_2) = W(\rho) \circ W(\rho_1)$.

2. The fact that $W(-)$ is a well-defined functor follows from Proposition 2.2.2, and the above argument. And the description of $W(\rho)$ for $\rho : B_1 \to B_2$ in $\mathcal{O}$-alg yields $W(-)$ is an exact functor.

□

2.3 Frobenius and Verschiebung

We will now describe the Frobenius and Verschiebung maps on the ring Witt's vectors. They turn out to be very useful in practice when one wants to compute things related to Witt's vectors, especially in the case B is a k-algebra, which will be treated in the next section.

Recall that in the first section, we defined $A := \mathcal{O}[X_0, X_1, ..., Y_0, Y_1, ...]$, and proved the existence and uniqueness of $F = (F_0, F_1, ...)$ such that

- $F_n \in \mathcal{O}[X_0, ..., X_{n+1}]$.
- $\Phi_A(F) = f_A(\Phi_A(X))$, where $X := (X_0, X_1, ...)$.
- $\Phi_{n+1}(X_0, ..., X_{n+1}) = \Phi_n(F_0, ..., F_n)$.
- $F_n \equiv X_n^q \mod \pi A$.

Using this, one can define the **Frobenius on** $W(B)$ as follows

$$\begin{aligned} F_B : W(B) &\longrightarrow W(B) \\ (b_0, b_1, ...) &\longmapsto (F_n(b_0, ..., b_{n+1}))_n \end{aligned}$$

We will prove that

Proposition 2.3.1. *F_B is an $\mathcal{O}$-algebra endomorphism of $W(B)$, and $F_B(b) \equiv b^q \mod \pi W(B)$ for all $b \in W(B)$.*

Proof. To prove the statement, we can use the technique in Proposition 2.1.8. Let us define $B_1 := \mathcal{O}[X_b | b \in B]$ and $\rho : B_1 \to B$ sending X_b to b, and $B_1' := \Phi_{B_1}(B_1^{\mathbb{N}_0})$. In the level of B_1, we have this diagram

$$\begin{tikzcd} W(B_1) \arrow[r, "F_{B_1}"] \arrow[d, "\Phi_{B_1}"'] & W(B_1) \arrow[d, "\Phi_{B_1}"] \\ B_1' \arrow[r, "f_{B_1'}"'] & B_1' \end{tikzcd}$$

is commutative, where $f'_{B_1}(b_0, b_1, ...) = (b_1, b_2, ...)$ because

$$\Phi_{B_1}(F_{B_1}(b_0, b_1, ...)) = \Phi_{B_1}((F_n(b_0, ..., b_{n+1}))_n) = f_{B_1'} \circ \Phi_{B_1}(b_0, ..., b_n, ...)$$

But we know that f'_{B_1} is an $\mathcal{O}$-algebra endomorphism, and so is F_{B_1}, since the two vertical arrows are isomorphisms. We can now use the functorial properties via the $\mathcal{O}$-algebra homomorphism ρ, and this yields F_B is an $\mathcal{O}$-algebra homomorphism.

To prove the second statement, we can also use the diagram above. Take any $(b_0, b_1, ...) \in W(B_1)$, we have the commutative diagram

$$\begin{tikzcd} (b_0, b_1, ...) \arrow[r, "F_{B_1}"] \arrow[d, "\Phi_{B_1}"'] & (F_n(b_0, ..., b_{n+1}))_n \arrow[d, "\Phi_{B_1}"] \\ (b_0, b_0^q + \pi b_1, ...) \arrow[r, "f_{B_1'}"'] & (b_0^q + \pi b_1, b_0^{q^2} + \pi b_1^q + \pi^2 b_2, ...) \end{tikzcd}$$

And via f'_{B_1}, we have $b_0^q + \pi b_1 \equiv b_0^q \mod \pi B_1'$, $b_0^{q^2} + \pi b_1^q + \pi^2 b_2 \equiv (b_0^q + \pi b_1)^q \mod \pi B_1'$,.... And via the ring isomorphism Φ_{B_1}, we have $F_{B_1}(b) \equiv b^q \mod \pi B_1$, for all $b \in B_1$. Again, using ρ, we have $F_B(b) \equiv b^q$, for all $b \in W(B)$. $\square$

We note that the technique using in the proof above is common when we want to prove identities on the ring of Witt's vectors. We next defined the Verschiebung map

$$\begin{aligned} V_B : W(B) &\longrightarrow W(B) \\ (b_0, b_1, ...) &\longmapsto (0, b_0, b_1, ...) \end{aligned}$$

Proposition 2.3.2. *V_B is an $\mathcal{O}$-module endomorphism.*

Proof. By the same technique as above, we can see what happens in $W(B_1)$. Look at the diagram

$$\begin{tikzcd}(b_0, b_1, ...) \arrow[r, "V_{B_1}"] \arrow[d, "\Phi_{B_1}"'] & (0, b_0, b_1, ...) \arrow[d, "\Phi_{B_1}"] \\ (b_0, b_0^q + \pi b_1, ...) \arrow[r, "v_{B_1'}"'] & (0, \pi b_0, \pi b_0^q + \pi^2 b_1, ...)\end{tikzcd}$$

where $v_{B_1'}(b_0, b_1, ...) = (0, \pi b_0, \pi b_1, ...)$. We have

$$\Phi_{B_1}(V_{B_1}(b_0, b_1, ...)) = \Phi_{B_1}(0, b_0, b_1, ...) = (0, \pi b_0, \pi b_0^q + \pi^2 b_1, ...)$$

And

$$v_{B_1'}(\Phi_{B_1}(b_0, b_1, ...)) = v_{B_1'}(b_0, b_0^q + \pi b_1, ...) = (0, \pi b_0, \pi b_0^q + \pi^2 b_1, ...)$$

This yields the diagram above is commutative. And hence V_{B_1} is an $\mathcal{O}$-module endomorphism, since so is $v_{B_1'}$. And by the functorial properties again, one gets V_B is an $\mathcal{O}$-module endomorphism. □

Here are some identities related to Frobenius and Verschiebung maps.

Proposition 2.3.3. *We have*

1. $F_B(V_B(b)) = \pi b$, *for all* $b \in W(B)$.
2. $V_B(a \boxdot F(b)) = V_B(a) \boxdot b$, *for all* $a, b \in W(B)$.

Proof.

1. Again, it is sufficient to see what happends in $W(B_1)$. Look at the diagram

$$\begin{tikzcd}W(B_1) \arrow[r, "V_{B_1}"] \arrow[d, "\Phi_{B_1}"'] & W(B_1) \arrow[r, "F_{B_1}"] \arrow[d, "\Phi_{B_1}"] & W(B_1) \arrow[d, "\Phi_{B_1}"] \\ B_1' \arrow[r, "v_{B_1'}"'] & B_1' \arrow[r, "f_{B_1'}"'] & B_1'\end{tikzcd}$$

   It is commutative, by Proposition 2.3.1 and Proposition 2.3.2. Now

$$f_{B_1'} \circ v_{B_1'}(b_0, b_1, ...) = f_{B_1'}(0, \pi b_0, \pi b_1, ...) = \pi(b_0, b_1, ...)$$

   Hence,

$$f_{B_1'} \circ v_{B_1'} \circ \Phi_{B_1}(b_0, b_1, ...) = \pi \Phi_{B_1}(b_0, b_1, ...)$$

   Because Φ_{B_1} is an $\mathcal{O}$-algebra isomorphism, we must have $F_{B_1} \circ V_{B_1}(b) = \pi b$.

2. For all $a, b \in W(B_1)$, we have

$$V_{B_1}(a \boxdot F_{B_1}(b)) = V_{B_1}(a) \boxdot b \Leftrightarrow \Phi_{B_1}(V_{B_1}(a \boxdot F_{B_1}(b))) = \Phi_{B_1}(V_{B_1}(a) \boxdot b) \Leftrightarrow$$

$$\Leftrightarrow v_{B_1'}(\Phi_{B_1}(a)\Phi_{B_1}(F_{B_1}(b))) = \Phi_{B_1}(V_{B_1}(a))\Phi_{B_1}(b) \Leftrightarrow v_{B_1'}(\Phi_{B_1}(a) f_{B_1'}(\Phi_{B_1}(b))) = v_{B_1'}(\Phi_{B_1}(a))\Phi_{B_1}(b)$$

   And the last identity now follows, since if we let $a = (a_0, a_1, ...)$, $b = (b_0, b_1, ...)$, $\Phi_n^a := \Phi_n(a_0, ..., a_n)$, $\Phi_n^b := \Phi_n(b_0, ..., b_n)$, then the left hand side of the last equality is

$$v_{B_1'}(\Phi_0^a \Phi_1^b, \Phi_1^a \Phi_2^b, ...) = (0, \pi \Phi_0^a \Phi_1^b, \pi \Phi_1^a \Phi_2^b, ...)$$

   while the right hand side is

$$(0, \pi \Phi_0^a, \pi \Phi_1^a, ...)(\Phi_0^b, \Phi_1^b, ...) = (0, \pi \Phi_0^a \Phi_1^b, ...)$$

   We now obtain the statement.

□

For simplicity, when B is given, we denote $V := V_B, F := F(B)$ on $W(B)$. We can now study further the properties of the Verschiebung map. This will lead to some conclusions about the π-adic topology on $W(B)$ for some important cases as the next section will point out. Let us denote

$$V_m(B) := \mathrm{im}(V^m) = \{(b_0, ..., b_{m-1}, b_m, ...) \in W(B) | b_0 = ... = b_{m-1} = 0\}$$

We obviously have $V_0(B) = W(B) \supseteq V_1(B) \supseteq V_2(B) \supseteq ...$, and $\bigcap_{m\geq 0} V_m(B) = 0$.

Lemma 2.3.4. *$V_m(B)$ is an ideal of $W(B)$ for all m.*

Proof. Proposition 2.3.2 implies that $V_m(B)$ is a subgroup of $W(B)$ and Proposition 2.3.3 implies that $b \boxdot c \in V_m(B)$, for all $b \in W(B), c \in V_m(B)$. □

Lemma 2.3.5. *$V_1(B)^m = \pi^{m-1}V_1(B)$ for all $m \geq 1$.*

Proof. The case $m = 1$ is trivial. When $m = 2$, by Proposition 2.3.3 we have for all $a, b \in W(B)$,

$$V(a) \boxdot V(b) = V(a \boxdot F(V(b))) = V(a \boxdot \pi b) = \pi V(a \boxdot b)$$

Hence, $V_1(B)^2 = \pi V_1(B)$. When $m = 3$

$$V_1(B)^3 = (V_1(B))^2 V_1(B) = \pi V_1(B)^2 = \pi^2 V_1(B)$$

Using this inductively, we get the statement for all $m \geq 1$ □

We denote $W_m(B) := W(B)/V_m(B)$, it is called **the ring of Witt's vectors of length** m with coefficients in B. We will now describe elements in $W_m(B)$.

Lemma 2.3.6.

1. *Let $(a_n)_n, (b_n)_n \in W(B)$, such that $a_n b_n = 0$ for all n, then*

$$(a_n)_n \boxplus (b_n)_n = (a_n + b_n)_n$$

2. *Let $(b_n)_n \in W(B)$ and $(0, ..., 0, c_m, c_{m+1}, ...) \in W(B)$, we can find $(0, ..., 0, x_m, x_{m+1}, ...)$ in $W(B)$ such that*

$$(b_0, ..., b_{m-1}, 0, 0, ...) \boxplus (0, ..., 0, x_m, x_{m+1}, ...) = (b_n)_n \boxplus (0, ..., 0, c_m, c_{m+1}, ...)$$

3. *There is a bijection*

$$\begin{aligned} B^m &\longrightarrow W_m(B) \\ (b_0, ..., b_{m-1}) &\longmapsto (b_0, ..., b_{m-1}, 0, ...) \boxplus V_m(B) \end{aligned}$$

Proof.

1. Turn things into $W(B_1)$ again. Let $\rho : B_1 \to B$ be the projection map, it is equivalent to prove that

$$W(\rho)((X_{a_n})_n \boxplus (X_{b_n})_n) = W(\rho)((X_{a_n})_n + (X_{b_n})_n)$$

It is equivalent to say

$$W(\rho)(\Phi_{B_1}((X_{a_n})_n \boxplus (X_{b_n})_n)) = W(\rho)(\Phi_{B_1}((X_{a_n})_n + (X_{b_n})_n)) \Leftrightarrow \Phi_B((a_n)_n) + \Phi_B((b_n)_n) = \Phi_B((a_n + b_n)_n)$$

But the last identity follows directly from the condition $a_n b_n = 0$ for all n, since

$$\Phi_n(a_0, ..., a_n) + \Phi_n(b_0, ..., b_n) = \Phi_n(a_0 + b_0, ..., a_n + b_n)$$

2. We have $(b_0, ..., b_{m-1}, 0, 0, ...) \boxplus (0, ..., 0, x_m, x_{m+1}, ...) = (b_0, ..., b_{m-1}, x_m, x_{m+1})$ by the previous result. Also,

$$(b_0, b_1, ...) \boxplus (0, ..., 0, c_m, c_{m+1}, ...) = (b_0, ..., b_{m-1}, S_m(b_0, ..., b_m, 0, ..., 0, c_m), ...)$$

And we just need to choose $x_m = S_m(b_0, ..., b_m, 0, ..., 0, c_m)$, and so on. From this, one can also see that the existence of x_m is unique.

3. By the second part, for any $(b_n)_n \in W(B)$ and $(0, ..., 0, c_m, c_{m+1}, ...) \in W(B)$, there exists a unique element $(0, ..., 0, x_m, x_{m+1})$ in $W(B)$ such that

$$(b_0, ..., b_m, 0, ...) \boxplus (0, ..., 0, x_m, x_{m+1}, ...) = (b_n)_n \boxplus (0, ..., 0, c_m, c_{m+1}, ...)$$

So, in particular, $(b_0, ..., b_{m-1}, 0, ...) \equiv (b_n)_n \mod V_m B$. And hence, the map defined above is surjective. For the injectivity, assume that

$$(a_0, ..., a_{m-1}, 0, ...) \boxplus V_m(B) = (b_0, ..., b_{m-1}, 0, ...) + V_m(B)$$

then there exists $(0, ..., 0, c_m, ...), (0, ..., 0, d_m, ...)$ in $V_m(B)$ such that

$$(a_0, ..., a_{m-1}, 0, ...) \boxplus (0, ..., 0, c_m, ...) = (b_0, ..., b_{m-1}, 0, ...) \boxplus (0, ..., 0, d_m, ...)$$

Due to 1, we have the LHS is $(a_0, ..., a_{m-1}, c_m, c_{m+1}, ...)$ and the RHS is $(b_0, ..., b_{m-1}, d_m, d_{m+1}, ...)$. Hence, $a_i = b_i$ for all $0 \leq i \leq m-1$.

□

As a corollary of the lemma above, we have

Corollary 2.3.7. *$W_m(B) = \{(b_0, ..., b_{m-1}, 0, ...) | b_i \in B\}$. And the map*

$$\begin{aligned} W(B) &\longrightarrow \varprojlim_m W_m(B) \\ b &\longmapsto (b \boxplus V_m(B))_m \end{aligned}$$

is an $\mathcal{O}$-algebra isomorphism.

2.4 The main cases

Most of applications of Witt's vectors focus on the case B is a k-algebra. In this case, due to the commutative diagram

$$\begin{tikzcd} k \cong \mathcal{O}/\pi\mathcal{O} \arrow[r] & B \\ \mathcal{O} \arrow[u] \arrow[ur, "\rho"] & \end{tikzcd}$$

we can consider B as an $\mathcal{O}$-algebra with the scalar product $\lambda b := (\lambda \mod \pi) b$, for $\lambda \in \mathcal{O}, b \in B$. In this case, as $\pi \equiv 0$ in k, we get $\pi B = 0$, and for any $\lambda \in \mathcal{O}$, we have $\lambda^q \equiv \lambda \mod \pi$, and hence $(\lambda b)^q = \lambda b^q$, for all $\lambda \in \mathcal{O}, b \in B$. Let p be the characteristic of k. If $\mathrm{char}(L) = 0$, we have $u\pi^e = p$, for some $u \in \mathcal{O}^\times$, and e is the ramification index, and hence $pB = 0$. In case $\mathrm{char}(L) = p$, the fact that $pB = 0$ is trivial. So, in any case, we obtain the Frobenius map on B

$$\begin{aligned} B &\longrightarrow B \\ x &\longmapsto x^q \end{aligned}$$

is an $\mathcal{O}$-algebra endomorphism. We say that B is perfect if this map is an isomorphism. We begin this section with the following

Proposition 2.4.1. *Let B be a k-algebra, then*

$$F((b_n)_n) = (b_n^q)_n$$

and when B is perfect, F is an automorphism of $\mathcal{O}$-algebra.

Proof. The first statement follows directly from Lemma 2.1.7, and the second statement follows directly from definition that the Frobenius map on B is bijective, and F is an $\mathcal{O}$-algebra endomorphism. □

The Frobenius on $W(B)$ is now in an easy form, and together with it, we also obtain some interesing properties, including the filtration in $W(B)$.

Proposition 2.4.2. *Let B be a k-algebra, for all $b = (b_0, b_1, ...) \in W(B)$, we have*

1. $\pi b = F(V(b)) = V(F(b)) = (0, b_0^q, b_1^q, ...)$.
2. $V_m(B) \boxdot V_n(B) \subseteq V_{m+n}(B)$.
3. $\pi^m W(B) \subseteq V_1(B)^m = \pi^{m-1} V_1(B) \subseteq \pi^{m-1} W(B)$.

Proof.

1. The identity $F(V(b)) = \pi b$ follows from Lemma 2.3.3, and due to Proposition 2.4.1, we have

$$F(V(b_0, b_1, ...)) = F(0, b_0, b_1, ...) = (0, b_0^q, b_1^q, ...) = V(F(b_0, b_1, ...))$$

2. For all $a, b \in W(B)$, using Lemma 2.3.3, we have

$$V^m(a) \boxdot V^n(b) = V(V^{m-1}(a)) \boxdot V^n(a) = V(V^{m-1}(a) \boxdot F(V^n(b))) = ... = V^m(a \boxdot F^m(V^n(b))$$

And by the first part, F and V are commutative, so

$$a \boxdot F^m(V^n(b)) = V^n(F^m(b)) \boxdot a = V(V^{n-1}(F^m(b))) \boxdot a =$$
$$V(V^{n-1}(F^m(B) \boxdot F(a))) = ... = V^n(F^m(b) \boxdot F^n(a))$$

We finally get $V^m(a)V^n(b) = V^{m+n}(F^m(b) \boxdot F^n(a))$. This yields $V_m(B) \boxdot V_n(B) \subseteq V_{m+n}B$.

3. By the first part, we obtain

$$\pi^m W(B) = \pi^{m-1}\pi W(B) \subseteq \pi^{m-1} V_1(B)$$

And by Lemma 2.3.5, we get $\pi^{m-1} V_1(B) = V_1(B)^m$. The last inclusion is trivial.

□

By the filtration in the last part, we get an important

Proposition 2.4.3. *Let B be k-algebra, then the algebra homomorphisms*

$$\begin{array}{ccc} W(B) & \longrightarrow & \varprojlim_m W(B)/\pi^m W(B) \\ b & \longmapsto & (b \boxplus \pi^m W(B))_m \end{array} \tag{2.5}$$

$$\begin{array}{ccc} W(B) & \longrightarrow & \varprojlim_m W(B)/V_1(B)^m \\ b & \longmapsto & (b \boxplus V_1(B)^m)_m \end{array} \tag{2.6}$$

are isomorphism.

Proof. We have $\pi^m W(B) = \{0, ..., 0, b_m^{q^m}, b_{m+1}^{q^m}, ...\}$. Hence, it is clear that the first map is injective, since $\bigcap m \geq 0\pi^m W(B) = 0$. Assume for now $(b^{(m)} \boxplus \pi^m W(B))_m \in \varprojlim_m W(B)/\pi^m W(B)$. Because $\pi^m W(B) \subseteq V_m(B)$, and due to the isomorphism in Corollary 2.3.7, there exists $b \in W(B)$ such that $b \boxplus V_m(B) = b^{(m)} \boxplus V_m(B)$ for any m. This yields for all $j \geq m$,

$$b \boxplus V_j(B) \boxplus \pi^m W(B) = b^{(j)} \boxplus V_j(B) \boxplus \pi^m W(B)$$

And because $b^{(j)} \boxplus \pi^m W(B) = b^{(j)} + \pi^j W(B) \mod \pi^m W(B) = b^{(m)} + \pi^m W(B)$, we get

$$b \boxplus V_j(B) \boxplus \pi^m W(B) = b^{(m)} \boxplus V_j(B) \boxplus \pi^m W(B)$$

And this yields

$$b \boxplus \bigcap_{j \geq m} \Big(V_j(B) \boxplus \pi^m W(B)\Big) = b^{(m)} \boxplus \bigcap_{j \geq m} \Big(V_j(B) \boxplus \pi^m W(B)\Big)$$

We will prove that

$$\bigcap_{j \geq m} (V_j(B) \boxplus \pi^m W(B)) = \pi^m W(B)$$

If this hold, then the map 2.5 is now surjective. To prove this, we note that

$$\bigcap_{j \geq m} (V_j(B) \boxplus \pi^m W(B)) \supseteq \Big(\bigcap_{j \geq m} V_j(B)\Big) \boxplus \pi^m W(B) = \pi^m W(B)$$

For the reverse inclusion, let us choose any $c = (c_0, c_1, ...) \in \bigcap_{j \geq m}(V_j(B) \boxplus \pi^m W(B))$, then for any $j > m$, there exists $(0, ..., 0, a_j, a_{j+1}, ...)$ in $V_j(B)$ and $(0, ..., 0, b_{j,m}^{q^m}, b_{j,m+1}^{q^m}, ...)$ in $\pi^m W(B)$, such that

$$(c_0, c_1, ...) = (0, ..., 0, a_j, a_{j+1}, ...) \boxplus (0, ..., 0, b_{j,m}^{q^m}, b_{j,m+1}^{q^m}, ...)$$

And as a consequence of Lemma 2.3.6, we get $c_0 = ... = c_{m-1} = 0, c_m = b_{j,m}^{q^m}, ..., c_{j-1} = b_{j,j-1}^{q^m}$. Since j is choosen arbitrary, we get $c \in \pi^m W$. And this yields the first map is bijective. For the second map, due to Proposition 2.4.2, we have $\pi^m W(B) \subseteq V_1(B)^m \subseteq \pi^{m-1} W(B)$, so the commutative diagram below

$$\begin{tikzcd}
 & \varprojlim W(B)/\pi^{m-1}W(B) \\
W(B) \arrow[ur, "(1)"] \arrow[r, "(2)"] \arrow[dr, "(3)"'] & \varprojlim W(B)/V_1(B)^m \arrow[u, "(5)"'] \\
 & \varprojlim W(B)/\pi^m W(B) \arrow[u, "(4)"']
\end{tikzcd}$$

has (1), (3), $(5) \circ (4)$ are bijective. And (4) and (5) are injective. This yields all of them are bijective. And the isomorphism in 2.6 is now obtained. $\square$

As a corollary, we get

Corollary 2.4.4. *Let B be a k-algebra, then $W(B)$ is complete, Hausdorff with respect to the π-adic topology. And the topology on B defined by the filtered system $\{V_m(B)\}$ is identical to the π-adic topology on B.*

Let us now move to a special case when B is a perfect k-algebra.

Proposition 2.4.5. *Let B be a perfect k-algebra, then*

1. *$\pi 1_{W(B)}$ is not a zero divisor in $W(B)$.*

2. *Let $\tau : B \to W(B)$ be the Teichmuller lift, then for all $b = (b_0, b_1, ...)$ in $W(B)$*

$$b \boxplus V_m(B) = \tau(b_0) \boxplus \pi\tau(b_1^{q^{-1}}) \boxplus ... \boxplus \pi^{m-1}\tau(b_{m-1}^{q^{-(m-1)}}) \boxplus V_m(B)$$

3. *$V_m(B) = V_1(B)^m = \pi^m W(B)$.*

Proof.

1. For all $0 \neq c = (c_0, c_1, ...) \in W(B)$, we have

$$\pi c = (0, c_0^q, c_1^q, ...)$$

   Since B is perfect, the Frobenius on B is an automorphism. Hence $\pi c \neq 0$.

2. We have

$$\begin{aligned}\tau(b_0) \boxplus \pi\tau(b_1^{q^{-1}}) \boxplus ... \boxplus \pi^{m-1}\tau(b_{m-1}^{q^{-(m-1)}}) \boxplus V_m(B) = \\ = (b_0, 0, ...) \boxplus (0, b_1, 0, ...) \boxplus (0, ..., 0, b_{m-1}, 0, ...) \boxplus V_m(B) \\ = (b_0, ..., b_{m-1}, 0, ...) \boxplus V_m(B) = b \boxplus V_m(B)\end{aligned}$$

   where the last identity follows from Lemma 2.3.6.

3. We have

$$\pi^m W(B) = \{(0, ..., 0, b_m^{q^m}, b_{m+1}^{q^m}, ...) | b_i \in B\}$$

   Because B is perfect, any element in B is a q-th power. And we get $\pi^m W(B) = V_m(B)$. Also, since $\pi W(B) = \{(0, b_1^q, b_2^q, ...) | b_i \in B\}$, Lemma 2.3.5 yields $V_1(B)^2 = \pi V_1(B) = \pi^2 W(B)$. And inductively, we obtain $V_1(B)^m = \pi^m W(B)$.

□

It is also natural to consider the case B is a field extension of k. This can lead to the construction of $\mathbb{Z}_p$ from $\mathbb{F}_p$.

Proposition 2.4.6. *Let B be a field extension of k, then*

1. *$W(B)$ is an integral domain, with a unique maximal ideal $V_1(B)$.*

2. *char$(W(B)) = 0$ if char$(L) = 0$.*

3. *If B is perfect, then $W(B)$ is a DVR with the unique maximal ideal $V_1(B)$, and the residue field B. Moreover, any $b = (b_n)_n$ in $W(B)$ has a unique convergent expansion*

$$b = \sum_{n \geq 0} \pi^n \tau(b_n^{q^{-n}})$$

   with respect to the π-adic topology on $W(B)$ (cf. Corollary 2.4.4).

Proof.

1. For any $\mathcal{O}$-algebra B, we can see from Lemma 2.3.6 that $W(B)/V_1(B) \cong B$. Hence, in the case B is a field extension of k, $V_1(B)$ is a maximal ideal of B. Take any $b = (b_0, b_1, ...)$ in $W(B)$ but not belong to $V_1(B)$, we will prove that b is invertible. First, we can find $a = (a_0, a_1, ...) \in W(B)$ and $c = (0, c_1, ...) \in V_1(B)$ such that

$$a \boxdot b = 1 \boxplus c = (1, 0, ...) \boxplus (0, c_1, ...) = (1, c_1, c_2, ...)$$

   by taking $a_0 = b_0^{-1}$, and $c_i = P_i(a_0, ..., a_i, b_0, ..., b_i)$. Because $c \in V_1(B)$, $c^m \in V_1(B)^m = \pi^{m-1} W(B)$, and $c^m \equiv \pm c^{m-1} \mod \pi^{m-1} W(B)$. This yields the sum $\sum_{i \geq 0} (-1)^i c^i$ is defined in

$W(B)$ (cf. Corollary 2.4.4). This yields b is invertible in $W(B)$, and we get $V_1(B)$ is the unique maximal ideal of $W(B)$.

We now prove that $W(B)$ is an integral domain. Take any $0 \neq a = (0, ..., 0, a_i, a_{i+1}, ...), 0 \neq b = (0, ..., 0, b_j, b_{j+1}, ...)$ in $W(B)$ with $a_i \neq 0, b_j \neq 0$,then $F^j(a_i, a_{i+1}, ...) = (a_i^{q^j}, a_{i+1}^{q^j}, ...), F^i(b) = (b_j^{q^i}, b_{j+1}^{q^i}, ...)$. And from this, $F^j(a_i, a_{i+1}, ...)F^i(b_j, b_{j+1}, ...) = (a_i^{q^j} b_j^{q^i}, ...) \neq 0$. And

$$a \boxdot b = V^i(a) \boxdot V^j(b) = V^{i+j}(F^j(a) \boxdot F^i(b)) = (0, ..., 0, a_i q^j b_j^{q^i}, ...) \neq 0$$

where the second identity follows from the proof of Proposition 2.4.2(2), and this yields $W(B)$ is a local domain.

2. Let $l \neq p$ be a prime number such that $l1_{W(B)} = 0$, then since $W(B)/V_1W(B) = B$ is of characteristic p, necessarily $l = p$. Let e be the raimification index of $L/\mathbb{Q}_p$, we can write $p = u\pi^e$ for some $u \in \mathcal{O}^\times$. And

$$p1_{W(B)} = u\pi^e(1, 0, ...) = u(0, ..., 0, 1, 0, ...) \neq 0$$

And this yields a contradiction. Hence, $\mathrm{char}(W(B)) = 0$, in case $\mathrm{char}(L) = 0$.

3. When B is perfect by Proposition 2.4.5, we obtain

$$\bigcap_{m \geq 1} V_1(B)^m = \bigcap_{m \geq 1} \pi^m W(B) = 0$$

And because $V_1(B) = \pi W(B)$ is the unique maximal ideal of $W(B)$, it follows from a general fact of commutative algebra that $W(B)$ is a DVR. Let $b \in W(B)$, Proposition 2.4.5 again implies that we can represent

$$b = \sum_{i \geq 0} \pi^i \tau(b_i^{q^{-i}})$$

And it is obvious to see that this expansion is unique and convergent due to Corollary 2.4.4.

□

Example 2.4.7. In the case $L := \mathbb{Q}_p$, we have $\mathcal{O} = \mathbb{Z}_p$ and $k = \mathbb{F}_p$, and $W(\mathbb{F}_p)_{\mathbb{Q}_p} \cong \mathbb{Z}_p$ via an isomorphism defined by the Teichmuller representations (recall that we use a subscript to emphasize $W(\mathbb{F}_p)$ is defined with coefficients in $\mathbb{Q}_p$). We will prove later that this isomorphism holds for much more general cases.

Remark 2.4.8. In the case $L := \mathbb{F}_q((t))$, $\pi := t$, and $B := \mathbb{F}_q$. By the first part of Proposition 2.4.6, $W(B)_L$ is an integral domain, and $\pi 1_{W(B)_L}$ is not zero, but $p\pi 1_{W(B)_L} = (p\pi)1_{W(B)_L} = 0$. And this yields $\mathrm{char}(W(B)_L) = p$.

2.5 From residue fields to local fields

Our main applications will focus on the case $\mathcal{O}$. And we can apply results of previous section to $k = \mathcal{O}/\pi\mathcal{O}$. This will lead to an isomorphism $\mathcal{O} \cong W(k)$. In order to this, we begin with an application of Proposition 2.1.4.

Proposition 2.5.1. *Let B be an $\mathcal{O}$-algebra with $\pi 1_B$ is not a zero divisor, and $\sigma \in End_{\mathcal{O}}(B)$ such that $\sigma(b) \equiv b^q \mod \pi B$, then there exists a unique $\mathcal{O}$-algebra $s_B : B \to W(B)$ such that $\Phi_n \circ s_B = \sigma^n$, for all n. Moreover, s_B is injective and is uniquely determined by the two conditions*

$$\Phi_0 \circ s_B = \mathrm{id}_B, F \circ s_B = s_B \circ \sigma$$

Proof. The existence of s_B is equivalent to the commutativity of the following diagram for all n

$$\begin{tikzcd} B \arrow[r, "s_B"] \arrow[dr, "\sigma^n"'] & W(B) \arrow[d, "\Phi_n"] \\ & B \end{tikzcd}$$

And it is equivalent to the commutativity of

$$\begin{tikzcd} B \arrow[r, "s_B"] \arrow[dr, "\Sigma"'] & W(B) \arrow[d, "\Phi_B"] \\ & B^{\mathbb{N}_0} \end{tikzcd}$$

where $\Sigma(b) := (b, \sigma(b), \sigma^2(b), ...)$. Because $\pi 1_B$ is not a zero divisor, Φ_B is injective. And the statement is now equivalent to

- $\Sigma(b) \in \mathrm{im}(\Phi_B)$, for all $b \in B$.
- Σ is an $\mathcal{O}$-algebra homomorphism.

The first condition is clear from the second part of Proposition 2.1.4, and the second condition follows directly from the fact that $\sigma \in \mathrm{End}_{\mathcal{O}}(B)$. Also, the injectivity of s_B is clear, since Σ is clearly injective. We have

$$\Phi_0 \circ s_B = \sigma^0 = id_B$$

Consider the following diagram

$$\begin{tikzcd} B \arrow[r, "\sigma"] \arrow[dr, "s_B"'] & B \arrow[r, "s_B"] & W(B) \arrow[dr, "\Phi_B"] & \\ & W(B) \arrow[ur, "F"'] \arrow[dr, "\Phi_B"'] & & B_0^{\mathbb{N}_0} \\ & & B^{\mathbb{N}_0} \arrow[ur, "f"'] & \end{tikzcd} \tag{2.7}$$

We will prove that it is commutative. Because $\Phi_B \circ s_B = \Sigma$, and they are all injective, it is sufficient to check the commutativity of the following diagram

$$\begin{tikzcd} B \arrow[r, "\Sigma"] \arrow[d, "\sigma"'] & B^{\mathbb{N}_0} \arrow[d, "f"] \\ B \arrow[r, "\Sigma"'] & B^{\mathbb{N}_0} \end{tikzcd} \tag{2.8}$$

But it is trivial, since $\Sigma \circ \sigma(b) = (\sigma(b), \sigma^2(b), ...)$, and $f \circ \Sigma(b) = f(b, \sigma(b), \sigma^2(b), ...) = (\sigma(b), \sigma^2(b), ...)$.

Conversely, assume that we have $s_B : B \to W(B)$ an $\mathcal{O}$-algebra homomorphism such that $\Phi_0 \circ s_B = id_B$ and $s_B \circ \sigma = F \circ s_B$. This yields the diagram 2.7 and 2.8 are commutative. Let us denote

$$s_B(b) = (s_0(b), s_1(b), ...) = (b, s_1(b), ...)$$

then $f \circ \Sigma(b) = \Sigma \circ \sigma(b)$, where $\Sigma := \Phi_B \circ s_B$. Let $\Sigma(b) = (b_0, b_1, ...)$, then because $\Sigma = \Phi_B \circ s_B$, we have $b_0 = b$. This yields $\Sigma(b) = (b, ...)$ for all $b \in B$, and hence, $\Sigma(\sigma(b)) = (\sigma(b), ...)$. Furthermore, $f \circ \Sigma(b) = (b_1, b_2, ...)$. And $f \circ \Sigma(b) = \Sigma \circ \sigma(b)$ implies that $b_1 = \sigma(b)$, and the second coordinate of $\Sigma(\sigma(b))$ is b_2. If we replace b by $\sigma(b)$, we get

$$(b_2, ...) = f \circ \Sigma(\sigma(b)) = \Sigma \circ \sigma^2(b) = \Phi_B \circ s_B \circ \sigma^2(b) = (\sigma^2(b), ...)$$

And this yields $b_2 = \sigma^2(b)$, and so on. Therefore, by our previous argument, it is the characterization of s_B. $\square$

We are now ready for the main proposition

Proposition 2.5.2. *Let B, s_B be defined as in Proposition 2.5.1, then for all $m \geq 1$, there exists a unique map $s_{B,m}$ making the following diagram commute*

$$\begin{tikzcd}
B \arrow[r, "s_B"] \arrow[d, "pr"'] & W(B) \arrow[r, "W(pr)"] & W(B/\pi B) \arrow[d, "pr"] \\
B/\pi^m B \arrow[rr, "s_{B,m}"'] & & W_m(B/\pi B)
\end{tikzcd}$$

Moreover, when $B/\pi B$ is perfect, then $s_{B,m}$ is an isomorphism for all $m \geq 1$.

Proof. Take any $b \in \pi^m B$, we can write

$$s_B(b) = (b_0, b_1, ...)$$

and the conditions of s_B yields that

$$\Phi_n \circ s_B(b) = \Phi_n(b_0, ..., b_n) = \sigma^n(b) \equiv b^{q^n} \mod \pi^{n+1}B$$

We know that $b_0 = b$, and $\Phi_1(b_0, b_1) = b_0^q + \pi b_1 \equiv b_0^q \mod \pi^2 B$. This yields $b_1 \in \pi B$, and by induction, we get all $b_i \in \pi B$, and this yields $\mathrm{pr} \circ W(\mathrm{pr}) \circ s_B(b) = 0$. So one can define a map $s_{B,m}$ making the diagram above commute. Denote $s_B(b) = (s_0(b), s_1(b), ...)$, we have $W(\mathrm{pr})(s_B(b)) = (s_0(b) \mod \pi, s_1(b) \mod \pi, ...)$ and $\mathrm{pr} \circ W(\mathrm{pr}) \circ s_B(b) = (s_0(b) \mod \pi, ..., s_m(b) \mod \pi, 0, ...)$. And it follows from the commutativity of the diagram above that $s_{B,m}(b \mod \pi^m) = (s_0(b) \mod \pi, ..., s_m(b) \mod \pi, 0, ...)$. And this yields the uniqueness of $s_{B,m}$.

For the second statement, when $m = 1$, we have

$$s_0(b) = \Phi_0 \circ s(b) = b$$

So, $s_{B,1}(b \mod \pi B) = (b \mod \pi, 0, ...)$, and it is an $\mathcal{O}$-algebra isomorphism. For $m > 1$, we have the following commutative diagram, where rows are exact

$$\begin{tikzcd}
0 \arrow[r] & \pi^m B/\pi^{m+1}B \arrow[r] \arrow[d, "s_{B,m+1}"] & B/\pi^{m+1}B \arrow[r] \arrow[d, "s_{B,m+1}"] & B/\pi^m B \arrow[r] \arrow[d, "s_{B,m}"] & 0 \\
0 \arrow[r] & V_m(B/\pi B)/V_{m+1}(B/\pi B) \arrow[r] & W_{m+1}(B/\pi B) \arrow[r] & W_m(B/\pi B) \arrow[r] & 0
\end{tikzcd}$$

The arrow in the LHS is well-defined since we have

$$s_{B,m+1}(\pi^m b \mod \pi^{m+1}B) = \mathrm{pr} \circ W(\mathrm{pr}) \circ s(\pi^m b) = \pi^m \mathrm{pr} \circ W(\mathrm{pr}) \circ s(b)$$

$$= \pi^m(b \mod \pi B, b_1 \mod \pi B, ..., 0, ...) = (0, ..., 0, (b \mod \pi B)^{q^m}, (b_1 \mod \pi B)^{q^m}, ...)$$

Therefore, by taking modulo $V_{m+1}(B)$, we obtain a map

$$\begin{aligned} s_{B,m+1} : \pi^m B/\pi^{m+1}B &\longrightarrow V_m(B/\pi B)/V_{m+1}(B/\pi B) \\ \pi^m b \mod \pi^{m+1}B &\longmapsto (0, ..., 0, (b \mod \pi B)^{q^m}, 0, ...) \end{aligned}$$

Under the assumption that $B/\pi B$ is perfect, the map above is an isomorphism. By induction, this yields the map in the middle is an isomorphism, too. $\square$

As a corollary, we get

Corollary 2.5.3. *Let B be an $\mathcal{O}$-algebra, assume that*
(i) $B/\pi B$ is perfect.
(ii) $\pi 1_B$ is not a zero divisor of B.
(iii) There exists $\sigma \in End_{\mathcal{O}}(B)$ such that $\forall b \in B$, $\sigma(b) \equiv b^q \mod \pi B$.
(iv) $B \cong \varprojlim_m B/\pi^m B$
then

$$B \cong W(B/\pi B)$$

Proof. Due to the conditions, we obtain by the proposition above that

$$s_{B,m} : B/\pi^m B \xrightarrow{\sim} W_m(B/\pi B) = W(B/\pi B)/\pi^m W(B/\pi B)$$

where the last identity follows from Proposition 2.4.5. Taking the limit both sides, we get the statement. □

Example 2.5.4. Let $L/\mathbb{Q}_p$ be a finite extension, and $B := \mathcal{O}$, then B satisfies the conditions of Corollary 2.5.3 with $\sigma := id_B$. This yields $W(\mathbb{F}_q)_L \cong \mathcal{O}$. Note that we have to denote the subscript in this case, since if we change the base ring, we will obtain another ring of Witt's vectors as the example below illustrates.

Example 2.5.5. Let $L := \mathbb{F}_q((t))$, with uniformizer $\pi := t$ and $B := \mathbb{F}_q[[t]] = \mathcal{O}_L$, then again B satisfies the conditions of Corollary 2.5.3 with $\sigma := id_B$. It follows in this case that $W(\mathbb{F}_q)_L \cong \mathbb{F}_q[[t]]$, and this yields $\mathrm{char}(W(\mathbb{F}_q)_L) = p$.

2.6 Weak topology on Witt's vectors

In this section, we will discuss about the topology on the ring of Witt's vectors. Instead of using the π-adic topology, we will make use of the product topology on $W(B)$, where B is a perfect topological k-algebra. It is weaker than the π-adic topology as we will see later, but it is easier to deal with, since the operations among Witt's vectors are complicated. For simplicity, we will denote the addition and multiplication on $W(B)$ as usual, instead of $\boxplus, \boxdot$.

For any open ideal $\mathfrak{a}$ of B, we define

$$V_{\mathfrak{a},m} := \ker(W(B) \xrightarrow{pr} W_m(B) \xrightarrow{W(pr)} W_m(B/\mathfrak{a})) =$$

$$= \{(b_0, ..., b_{m-1}, ...) \in W(B) | b_0, ..., b_{m-1} \in \mathfrak{a}\}$$

We can see that $V_{\mathfrak{a},m}$ is an ideal of $W(B)$, and

$$V_{\mathfrak{a}\cap\mathfrak{b},\max\{m,n\}} \subseteq V_{\mathfrak{a},m} \cap V_{\mathfrak{b},n}$$

For any open ideal $\mathfrak{b}$ of B. And hence, there exists a unique topological structure on $W(B)$ such that $W(B)$ is a topological ring and that such $V_{\mathfrak{a},m}$ become a fundamental system of open neighborhoods around 0. If we consider

$$W_m := \pi^m W(B) = \{(0, ..., 0, b_m, ...) \in W(B) | b_m, b_{m+1}, ... \in B\}$$

then for any $V_{\mathfrak{a},m}$, we always have $W_m \subseteq V_{\mathfrak{a},m}$. So, the topology on $W(B)$ we have equipped is weaker than the π-adic topology on $W(B)$. We call it the **weak topology on** $W(B)$.

Lemma 2.6.1. *For any $a = (a_0, a_1, ...) \in W(B)$, we have*

$$a + W_{\mathfrak{a},m} = \{(b_0, b_1, ...) \in W(B) | b_i \equiv a_i \mod \mathfrak{a}, 0 \leq i \leq m-1\}$$

Hence, the weak topology on $W(B)$ coincides with the product topology on $B \times B \times ...$

Proof. Take any $(c_0, c_1, ...) \in V_{\mathfrak{a},m}$, i.e. $c_0, ..., c_{m-1} \in \mathfrak{a}$, we have

$$(a_0, a_1, ...) + (c_0, c_1, ...) = (a_0 + c_0, ...) =: (b_0, b_1, ...)$$

We can see that $b_0 = a_0 + c_0 \equiv a_0 \mod \mathfrak{a}$. Assume that $b_i \equiv a_i \mod \mathfrak{a}$ holds to $n-1$ where $1 \leq n \leq m-1$, we will prove that this holds for n. By the addition formula for Witt vectors, we have

$$\Phi_n(a_0, ..., a_n) + \Phi_n(c_0, ..., c_n) = \Phi_n(b_0, ..., b_n)$$

Assume that $b_i = a_i + d_i$ for $d_i \in \mathfrak{a}$, $0 \leq i \leq n-1$, we deduce from the definition of Witt polynomials that

$$\Phi_{n-1}(a_0^q, ..., a_{n-1}^q) + \Phi_{n-1}(c_0^q, ..., c_{n-1}^q) + \pi^n(a_n + c_n) = \Phi_{n-1}(b_0^q, ..., b_{n-1}^q) + \pi^n b_n$$

And this yields

$$\frac{\Phi_{n-1}(a_0^1, ..., a_{n-1}^q) + \Phi_{n-1}(c_0^q, ..., c_{n-1}^q) - \Phi_{n-1}(b_0^q, ..., b_{n-1}^q)}{\pi^n} + a_n + c_n = b_n(*)$$

And we know that

$$\Phi_{n-1}(b_0^q, ..., b_{n-1}^q) = \Phi_{n-1}((a_0 + d_0)^q, ..., (a_{n-1} + d_{n-1})^q) =$$

$$= \Phi_{n-1}(a_0^q + d_0^q, ..., a_{n-1}^q + d_{n-1}^q) = (a_0^q + d_0^q)^{q^{n-1}} + ... + \pi^{n-1}(a_{n-1}^q + d_{n-1}^q)$$

$$= \Phi_{n-1}(a_0^q, ..., a_{n-1}^q) + \Phi_{n-1}(d_0^q, ..., d_{n-1}^q)$$

And from $(*)$, we get

$$d + a_n + c_n = b$$

for some $d \in \mathfrak{a}$, and this yields $b_n \equiv a_n \mod \mathfrak{a}$, since c_n is also in $\mathfrak{a}$. We then get

$$a + V_{\mathfrak{a},m} \subseteq \{(b_0, ..., b_{m-1}, ...) | b_i \equiv a_i \mod \mathfrak{a}, 0 \leq i \leq m-1\}$$

For the converse direction, with the same argument, we deduce that for $b_i \equiv a_i \mod \mathfrak{a}$, for all $0 \leq i \leq m-1$,

$$(b_0, ..., b_{m-1}, ...) - (a_0, ..., a_{m-1}, ...) = (c_0, ..., c_{m-1}, ...)$$

with $c_i \in \mathfrak{a}$, for $0 \leq i \leq m-1$. For the second statement, we can see by the first statement that the set

$$a + V_{\mathfrak{a},m} = \{(b_0, ..., b_{m-1}) \in W(B) | b_i \equiv a_i \mod \mathfrak{a}, 0 \leq i \leq m-1\}$$

forms a fundamental system of open neighborhoods around a. And this follows directly that the weak topology on $W(B)$ is the same as the product topology $B \times B \times ....$ □

Via this lemma, we can prove

Proposition 2.6.2. *If B is Hausdorff (complete), then $W(B)$ is Hausdorff (complete, resp.).*

Proof. It follows easily that if B is Hausdorff then the product topology $B \times B \times ...$ is also Hausdorff. Now, assume that B is complete. In this case, the canonical map

$$\phi : B \to \varprojlim_{\mathfrak{a}} B/\mathfrak{a}$$

is surjective. Let $\mathfrak{c}$ be its kernel, we have $B/\mathfrak{c} \cong \varprojlim_{\mathfrak{a}} B/\mathfrak{a}$. And this yields

$$W_m(B/\mathfrak{c}) \cong W_m(\varprojlim_{\mathfrak{a}} B/\mathfrak{a}) \cong \varprojlim_{\mathfrak{a}} W_m(B/\mathfrak{a}) = \varprojlim_{\mathfrak{a}} W(B)/V_{\mathfrak{a},m}$$

where the second isomorphism comes from the functorial properties of Witt vectors, and the last isomorphism follows from the fact that the map $W(B) \xrightarrow{W(pr)} W(B/\mathfrak{a}) \xrightarrow{pr} W_m(B/\mathfrak{a})$ has kernel $V_{\mathfrak{a},m}$.

Now, it follows from Corollary 2.3.7 that

$$W(B/\mathfrak{c}) \cong \varprojlim_m W_m(B/\mathfrak{c}) \cong \varprojlim_m \varprojlim_{\mathfrak{a}} W(B)/V_{\mathfrak{a},m}$$

And so, we obtain the following surjective map

$$W(B) \xrightarrow{W(pr)} W(B/\mathfrak{c}) \cong \varprojlim_m \varprojlim_{\mathfrak{a}} W(B)/V_{\mathfrak{a},m}$$

And this yields $W(B)$ is complete. □

Proposition 2.6.3. *In the case B is complete and Hausdorff, we can equip the induced topological structure on the quotient ring $W_m(B)$, with m is fixed, such that $W_m(B)$ is Hausdorff and complete.*

Proof. In this case, the canonical map $B \to \varprojlim_{\mathfrak{a}} B/\mathfrak{a}$ is bijective, and this yields by the previous proof that

$$W(B)/V_m(B) = W_m(B) \cong \varprojlim_{\mathfrak{a}} W_m(B/\mathfrak{a}) \cong$$

$$\cong \varprojlim_{\mathfrak{a}} W(B)/V_{\mathfrak{a},m} \cong \varprojlim_{\mathfrak{a}} (W(B)/V_m(B))/(V_{\mathfrak{a},m}/V_m(B))$$

From this, there exists a unique topological structure on $W_m(B)$, such that $\{V_{\mathfrak{a},m}/V_m(B) | \mathfrak{a} \subseteq B :$ open ideal $\}$ becomes a fundamental system of open neighborhood around 0. And $W_m(B)$ is also Hausdorff, and complete. □

Example 2.6.4. When B is a perfect field extension of k, with discrete topology. Then it follows directly that the weak topology on $W(B)$ is exactly the π-adic topology on $W(B)$. And if we apply this to $B := k$, we will obtain $W(k) \cong \mathcal{O}_L$ topologically.

We will be mainly interested in the case $B := \mathcal{O}_F$, where F is a complete, non-archimedean, perfect field containing k. In this case, we get $W(B)$ is Hausdorff, complete, and is a subring of $W(F)$.

Lemma 2.6.5. *Let $\mathcal{O}_F$ be as above, then an ideal $\mathfrak{a}$ of $\mathcal{O}_F$ is open iff $\mathfrak{a}$ is non-zero.*

Proof. Assume that $\mathfrak{a}$ is open, then it is obvious that $\mathfrak{a}$ is non-zero. Now, let $\mathfrak{a} \subseteq \mathcal{O}_F$ be any non-zero ideal. Take $0 \neq x \in \mathfrak{a}$, it is sufficient to prove that (x)-the ideal generated by x is open in $\mathcal{O}_F$. We can see that

$$(x) = \{y \in \mathcal{O}_F | |y| \leq |x|)\}$$

Let us take any $z \in \mathcal{O}_F$, such that $|y - z| < |x - y|$. This yields $|y - z| < \max\{x, y\} \leq |x|$. From this, we have $|z| \leq |x|$, and $z \in (x)$. This yields (x) is open, and hence, $\mathfrak{a}$ is open. □

We can define for any open ideal $\mathfrak{a}$ of $\mathcal{O}_F$, and any $m \geq 1$ an $\mathcal{O}_F$-submodule

$$U_{\mathfrak{a},m} := V_{\mathfrak{a},m} + \pi^m W(F) := \{(b_0, ..., b_{m-1}, ...) \in W(F) | b_0, ..., b_{m-1} \in \mathfrak{a}\}$$

We note that $U_{\mathfrak{a},m}$ are not ideals of $W(F)$, and we again have

$$U_{\mathfrak{a}\cap\mathfrak{b},\max\{m,n\}} \subseteq U_{\mathfrak{a},m} \cap U_{\mathfrak{b},n}$$

This yields there exists a unique topology on $W(F)$, such that $W(F)$ is a topological group, and $U_{\mathfrak{a},m}$ forms a fundamental system of neighborhoods around 0. Also, one can see that the weak topology on $W(\mathcal{O}_F)$ is the subspace topology on $W(F)$. We recall from Proposition 2.4.6 that since F is an perfect extension of k, $W(F)$ is a D.V.R, with maximal ideal generated by π. Again, the topology we have equipped for $W(F)$ is weaker that the π-adic topology. We can call it **the weak topology on** $W(F)$. We actually want to prove that this topology actually defines a structure of topological ring on $W(F)$, and that when $\mathcal{O}_F$ admits a filtered fundamental system, then $W(F)$ is complete.

We will need the multiplicative property of Teichmuller's representatives.

Lemma 2.6.6.

1. *Let* $a_1, ..., a_r \in W(F)$*, then there exists* $0 \neq \alpha \in \mathcal{O}_F$*, such that*
$$\tau(\alpha)a_1, ..., \tau(\alpha)a_r \in U_{\mathcal{O}_F,m}$$
2. *Let* $\mathfrak{a}$ *be an open ideal of* $\mathcal{O}_F$*, then for any* $0 \neq \alpha \in \mathcal{O}_F$*, and* $m \geq 1$*, we have*
$$\tau(\alpha^{-1})U_{\alpha^{q^{m-1}}\mathfrak{a},m} \subseteq U_{\mathfrak{a},m}$$

Proof.

1. By Proposition 2.4.6, we can represent
$$a_i = \sum_{j\geq 0} \tau(a_{i,j})\pi^j$$
And from this
$$\tau(\alpha)a_i = \sum_{j\geq 0} \tau(\alpha a_{i,j})\pi^j = (\alpha a_{i,0}, \alpha a_{i,1}, ...)$$
And we can choose α such that $\alpha a_{i,j} \in \mathcal{O}_F$, for all $1 \leq i \leq r, 0 \leq j \leq m-1$.
2. Take $a = (a_0, a_1, ...) \in \alpha^{q^{m-1}}\mathfrak{a}$, we can represent
$$(\alpha_0, \alpha_1, ...) = \sum_{i\geq 0} \tau(a_i^{1/q^i})\pi^i$$
Hence
$$\tau(\alpha^{-1})a = \sum_{i\geq 0} \tau(\alpha^{-1}a_i^{1/q^i})\pi^i = \sum_{i\geq 0}(\alpha^{-q^i}a_i)$$
And hence, $\alpha^{-q^i}a_i \in U_{\mathfrak{a},m}$, for all $0 \leq i \leq m-1$.

□

We are now ready for the main result of this section.

Proposition 2.6.7.

$W(F)$ is a complete, Hausdorff topological ring.

Proof.

We will prove that the multiplication map
$$W(F) \times W(F) \to W(F)$$
is continuous. Take any $a, b \in W(F)$, and an open neighborhood of $ab + U_{\mathfrak{a},m}$, for some open ideal $\mathfrak{a}$ of $\mathcal{O}_F$, and $m \geq 1$. By Lemma 2.6.6, one can find $0 \neq \alpha \in \mathcal{O}_F$ such that $\tau(\alpha)a, \tau(\alpha)b \in U_{\mathcal{O}_F,m}$, which is equivalent to $a, b \in \tau(\alpha^{-1})U_{\mathcal{O}_F,m}$. By Lemma 2.6.6 again, we have
$$(a + U_{\alpha^{q^{m-1}}\mathfrak{a},m})(b + U_{\alpha^{q^{m-1}}\mathfrak{a},m}) \subseteq ab + U_{\mathcal{O}_F,m}U_{\mathfrak{a},m} + U_{\mathfrak{a},m} \subseteq ab + U_{\mathfrak{a},m}$$

And by Lemma 2.6.5, $U_{\alpha^{q^{m-1}}\mathfrak{a},m}$ is open. Hence, $W(F)$ is a topological ring. Moreover, one get easily that
$$\bigcap_{\mathfrak{a},m} U_{\mathfrak{a},m} = \bigcap_{\mathfrak{a},m}\{(b_0, ..., b_{m-1}, ...) \in W(F) | b_i \in \mathfrak{a}\} = 0$$

since $\mathcal{O}_F$ is Hausdorff, and the intersection of all open ideals is just 0.

Now, to prove that $W(F)$ is complete, t is sufficient to prove any Cauchy sequence in $W(F)$ converges in $W(F)$. The main ideal of the proof is that we will use Lemma 2.6.6 to reduce the induced Cauchy sequence to $W_m(\mathcal{O}_F)$, which is complete, by Proposition 2.6.3. And then, by the completeness of the π-adic topology on $W(F)$, we will prove that our sequence converges in $W(F)$.

Take any $(a_n)_n$ is a Cauchy sequence in $W(F)$. Fix an integer $m \geq 1$, then for any $\mathfrak{a}$: open ideal in $\mathcal{O}_F$, there exists an integer $n_{\mathfrak{a}}$ such that for all $n, n' \geq n_{\mathfrak{a}}$, $a_n - a_{n'} \in U_{\mathfrak{a},m}$. Then by Lemma 2.6.6, we can choose $0 \neq \alpha \in \mathcal{O}_F$, such that

$$\tau(\alpha)a_1, ..., \tau(\alpha)a_{n_{\mathfrak{a}}} \in U_{\mathcal{O}_F,m}$$

And hence, for all $n \geq n_{\mathfrak{a}}$, we have

$$\tau(\alpha)(a_n - a_{n_{\mathfrak{a}}}) \in \tau(\alpha)U_{\mathcal{O}_F,m} \subseteq U_{\mathcal{O}_F,m}$$

And hence $(\tau(\alpha)a_n)_n \in U_{\mathcal{O}_F,m}$, and for $n, n' \geq n_{\mathfrak{a}}$, we have

$$\tau(\alpha)(a_n - a_{n'}) \in \tau(\alpha)U_{\mathfrak{a},m} \subseteq U_{\mathfrak{a},m}$$

Take $(b_n)_n \in W(\mathcal{O}_F)$ such that $\tau(\alpha) - b_n \in \pi^m W(F)$. We then have

$$b_n - b_{n'} \in (\tau(\alpha)(a_m - a_n) + \pi^m W(F)) \cap W(\mathcal{O}_F) \subseteq (U_{\mathfrak{a},m} + \pi^m W(F)) \cap W(\mathcal{O}_F) = V_{\mathfrak{a},m}$$

for all $n, n' \geq n_\alpha$. This yields the sequence $(b_n \mod V_m(\mathcal{O}_F))_n$ is Cauchy, and hence, converges to some $b \mod V_m(\mathcal{O}_F)$ in $W_m(\mathcal{O}_F)$. Hence, for any open ideal $\mathfrak{b} \subseteq \mathcal{O}_F$, there exists $n_{\mathfrak{b}}$ such that for all $n \geq n_{\mathfrak{b}}$, we have $b - b_n \in V_{\alpha^{q^{m-1}}\mathfrak{b},m}$. Let us denote $a(m) := \tau(\alpha^{-1})b$, then

$$\begin{aligned} a(m) - a_n = \tau(\alpha^{-1})b - a_n = \tau(\alpha^{-1})(b - \tau(\alpha)a_n) = \tau(\alpha^{-1})(b - b_n + b_n - \tau(\alpha)a_n) \\ \subseteq \tau(\alpha^{-1})(V_{\alpha^{q^{m-1}}\mathfrak{b},m} + \pi^m W(F)) \subseteq U_{\mathfrak{b},m} + \pi^m W(F) \subseteq U_{\mathfrak{a},m} \end{aligned}$$

for all $n \geq n_{\mathfrak{a}}$. Now, if we vary m, then we will get

$$a(m+1) - a(m) = (a(m+1) - a_n) - (a(m) - a_n) \in U_{\mathfrak{b},m}$$

for n is sufficiently large. That means

$$a(m+1) - a(m) \in \{(b_0, ..., b_{m-1}) \in W(B) | b_0, ..., b_{m-1} \in \mathfrak{b}, \forall \mathfrak{b} \subseteq \mathcal{O}_F : \text{ open}\}$$

And this yields $a(m+1) - a(m) \in \pi^m W(F)$. Now, this yields $(a(m))_m$ is a Cauchy sequence with respect to the π-adic topology, and hence, a Cauchy sequence in the weak topology. Let a be the convergent value of $(a(m))_m$ in the π-adic topology, we will prove that a is also the convergent value of $(a_n)_n$. For any ideal $\mathfrak{a} \subseteq \mathcal{O}_F$: open, and any m, we have $\pi^m W(F) \subseteq U_{\mathfrak{a},m}$, and there exists some n' such that $a - a(n') \in \pi^m W(F)$ and $a(n') - a_n \in U_{\mathfrak{a},m}$, for some $n \geq n_{\mathfrak{a}}$. Hence, $(a - a_n) \in U_{\mathfrak{a},m}$. This yields a is the convergent value of $W(F)$, and $W(F)$ is complete. $\square$

Chapter 3

Tilts and Field of Norms

Let us fix these notations, $L/\mathbb{Q}_p$ a finite extension, with $\mathcal{O} := \mathcal{O}_L$ its ring of integers, $\pi := \pi_L$ a uniformizer, with $q := \#k$, where $k = k_L$ is the residue field of L. $\overline{\mathbb{Q}_p}$ denotes an algebraic closure of $\mathbb{Q}_p$, and $\mathbb{C}_p$ the completion of $\overline{\mathbb{Q}_p}$. Let L_∞/L be a Lubin-Tate extension associated to a given Frobenius series. When $L := \mathbb{Q}_p$, and $L_\infty := \mathbb{Q}_p^\infty$ (cf. Example 1.3.9), a theorem of Fontaine-Winterberger [FW79] yields $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}^\infty)$ is isomorphic (as topological groups) to $\mathrm{Gal}(\mathbb{F}_p((t))^{\mathrm{sep}}/\mathbb{F}_p((t)))$. In fact, the theorem of Fontaine-Wintenberger holds for all arithmetically profinite field extension of L. It was generalized by Peter Scholze [Sch12] by the notions of perfectoid fields and their tilts. The titlting correspondences are then simplified by the work K. S. Kedlaya [Ked15], which is the main goal of this chapter. At the end of this chapter, as an application, we will prove that the $\mathbb{F}_p$-cohomological dimension of $G_{\mathbb{Q}_p}$-the absolute Galois group of $\mathbb{Q}_p$ is not larger than 2.

3.1 Perfectoid fields and tilts

Definition. Let $K \subseteq \mathbb{C}_p$ be a field, then K is said to be a **perfectoid field** if

(i) K is complete.

(ii) $|K|^\times$ is dense in $\mathbb{R}^\times_{>0}$.

(iii) The map

$$\begin{aligned}(.)^p : K/p\mathcal{O}_K &\longrightarrow K/p\mathcal{O}_K\\ x &\longmapsto x^p\end{aligned}$$

is surjective.

The main goal of this section is to construct the tilt $K^\flat$ of a perfectoid field K. It turns out that $K^\flat$ is a complete, perfect field of characteristic p. In this chapter, we are **always** interested in perfectoid fields K such that $L_\infty \subseteq K \subseteq \mathbb{C}_p$. As we will see, in this case, the first axiom of perfectoid fields is automatically satisfied. When $K \subseteq \overline{\mathbb{Q}_p}$ is complete, $K/\mathbb{Q}_p$ is a finite extension (since an infinite algebraic extension of a local field is not complete). An example of perfectoid fields is $\mathbb{C}_p$. Another example is the completion of L_∞ as the lemma below points out.

Lemma 3.1.1. *Let $L_\infty \subseteq K \subseteq \mathbb{C}_p$ be an intermediate complete field, whose absolute value group $|K|^\times$ is dense in $\mathbb{R}^\times_{>0}$. Assume that there exists ω is an element of K, such that $1 > |\omega| \geq |\pi|$, and $(\mathcal{O}_K/\omega\mathcal{O}_K)^q = \mathcal{O}_K/\omega\mathcal{O}_K$, then K is perfectoid.*

Proof. Due to the dense of the absolute value group, we can find $\omega_1 \in K$, such that $|\omega|^{1/q} \leq |\omega_1| < 1$, i.e. $\omega\mathcal{O}_K \subseteq \omega_1^q\mathcal{O}_K$. For any $a \in \mathcal{O}_K$, we can write $a = a_0^q + \omega b_0'$, where $b_0' \in \mathcal{O}_K$ and $|\omega| \leq |\omega_1^q|$ implies that one can write

$$a = a_0^q + \omega_1^q b_0$$

with $a_0, b_0 \in \mathcal{O}_K$, and inductively

$$b_0 = a_1^q + \omega_1^q b_1$$

$$b_i = a_i^q + \omega_1^q b_{i+1}$$

$$...$$

For all $a_i, b_i \in \mathcal{O}_K$. And we can write $a = a_0^q + \omega_1^q a_1^q + \omega_1^{2q} a_2^q + ...$, and when n sufficient large, we have $|p| > |\omega_1|^{q(n+1)}$. And hence, $a \equiv (a_0 + \omega a_1 + ... + \omega^n a_n)^q \mod p\mathcal{O}_K$. This yields K is perfectoid. □

Corollary 3.1.2. *The completion $\widehat{L_\infty}$ of L_∞ is perfectoid.*

Proof. We recall that there exists a uniformizer z_n of L_n satisfying $|z_n| = |\pi|^{1/(q-1)q^{n-1}}$. And this yields easily that the absolute value group of $|L_\infty|^\times$ is dense in $\mathbb{R}_{>0}^\times$. Also, since L_n are totally ramified extension of L, for all n, we obtain $\mathcal{O}_{L_\infty}/\pi\mathcal{O}_{L_\infty} = k_L$. And because $\mathcal{O}_{\widehat{L_\infty}}/\pi\mathcal{O}_{\widehat{L_\infty}} \cong \mathcal{O}_{L_\infty}/\pi\mathcal{O}_{L_\infty}$, we obtain $(\mathcal{O}_{\widehat{L_\infty}}/\pi\mathcal{O}_{\widehat{L_\infty}})^q = \mathcal{O}_{\widehat{L_\infty}}/\pi\mathcal{O}_{\widehat{L_\infty}}$. And by Lemma 3.1.1, $\widehat{L_\infty}$ is perfectoid. □

We will now construct the tilt of a perfectoid field.

Lemma 3.1.3. . *Let K be a perfectoid field and $a \in K^\times$, then there exists $b \in K^\times$, such that $|a| = |b|^p$.*

Proof. Because $K^\times$ is dense in $\mathbb{R}_{>0}^\times$, there exists some $\omega \in K^\times$ such that $|p| < |\omega| < 1$, and some $m \in \mathbb{Z}$, such that $|\omega|^{m+1} < |a| \leq |\omega|^m$. From this, $|\omega| < |a\omega^{-m}| \leq 1$, and hence $|p| < |a\omega^{-m}| \leq 1$, and $|a| = |\omega^m||a\omega^{-m}|$. And it is sufficient to prove that whenever $|p| < |a| \leq 1$, there exists $b \in K^\times$, such that $|a| = |b|^p$. The condition (iii) of the definition above yields there exists some $b \in K^\times$, such that $|a - b^p| \leq |p|$. If $|a| \neq |b^p|$, then $|a - b^p| = \max\{|a|, |b^p|\} \geq |a| > |p|$, a contradiction. Hence, $|a| = |b|^p$. □

Let us fix some $\omega \in K^\times$, where K is a perfectoid fields, such that $1 > |\omega| \geq |\pi|$ (so that $\omega\mathcal{O}_K \supset \pi\mathcal{O}_K \supset p\mathcal{O}_K$. We consider the following projective limit

$$\mathcal{O}_{K^\flat} := \varprojlim(... \xrightarrow{(.)^q} \mathcal{O}_K/\omega\mathcal{O}_K \xrightarrow{(.)^q} \mathcal{O}_K/\omega\mathcal{O}_K \xrightarrow{(.)^q} \mathcal{O}_K/\omega\mathcal{O}_K) =$$

$$= \{(..., \alpha_i, ..., \alpha_1, \alpha_0) | \alpha_i \in \mathcal{O}_K/\omega\mathcal{O}_K, \alpha_{i+1}^q = \alpha_i\}$$

Lemma 3.1.4. . *$\mathcal{O}_{K^\flat}$ is a perfect k_L-algebra.*

Proof. There is a map from $(\mathcal{O} \mod \pi\mathcal{O})$ to $\mathcal{O}_{K^\flat}$ defined as

$$(a \mod \pi\mathcal{O}) \mapsto (..., a \mod \omega\mathcal{O}_K, ..., a \mod \omega\mathcal{O}_K)$$

Because $a^q \equiv a \mod \pi\mathcal{O}$ for all $a \in \mathcal{O}$, we have $a^q \equiv a \mod \omega\mathcal{O}_K$, this yields a well-defined map from k_L to $\mathcal{O}_K/\omega\mathcal{O}_K$. It is easy to check that this map is a ring homomorphism. Hence, $\mathcal{O}_{K^\flat}$ is a k_L-algebra.

Let us consider the map $\mathcal{O}_{K^\flat} \to \mathcal{O}_{K^\flat}$ defined as $\alpha \mapsto \alpha^q$. Assume that $\alpha^q := (..., \alpha_i^q, ..., \alpha_1^q, \alpha_0^q) = 0$. The fact that $\alpha_{i+1}^q = \alpha_i$ yields $\alpha_i = 0$, for all i, and hence, $\alpha = 0$. Also, it is easy to see that $(..., \alpha_i, ..., \alpha_1, \alpha_0) = (..., \alpha_i, ..., \alpha_1)^q$. So, the map is also surjective. This yields $\mathcal{O}_{K^\flat}$ is perfect. □

Now, for any $\alpha = (..., \alpha_i, ..., \alpha_1, \alpha_0)$, we can lift α_i to $a_i \in \mathcal{O}_K$, such that $a_i \mod \omega\mathcal{O}_K = \alpha_i$, and we have $a_{i+1}^q = a_i \mod \omega\mathcal{O}_K$. And this yields

$$a_{i+1}^{q^{i+1}} \equiv a_i^{q^i} \mod \omega^{i+1}\mathcal{O}_K$$

so that the sequence $(a_i^{q^i})$ converges in $\mathcal{O}_K$. It can be checked easily that the limit of this sequence does not depend on the choice of a_i. And we denote this limit as $\alpha^\sharp$.

Lemma 3.1.5. . *The map*

$$\varprojlim_{(.)^q} \mathcal{O}_K \xrightarrow{\psi} \mathcal{O}_{K^\flat}$$

defined by

$$(..., a_i, ..., a_1, a_0) \mapsto (..., a_i \mod \omega\mathcal{O}_K, ..., a_1 \mod \omega\mathcal{O}_K, a_0 \mod \omega\mathcal{O}_K)$$

and the map

$$\mathcal{O}_{K^\flat} \xrightarrow{\theta} \varprojlim_{(.)^q} \mathcal{O}_K$$

defined by $\alpha \mapsto (..., (\alpha^{1/q^i})^\sharp, ..., (\alpha^{1/q})^\sharp, \alpha^\sharp)$ *are multiplicative inverse of each other.*

Proof. We can see that ψ is well-defined. Also, if we denote $\alpha := (..., \alpha_i, ..., \alpha_1, \alpha_0)$, then it can be seen that $\alpha^{1/q^i} = (..., \alpha_{i+1}, \alpha_i)$, and

$$(\alpha^{1/q^i})^\sharp = \lim_{j\to\infty} (a_{i+j}^{q^j}) = (\lim_{k\to\infty} (a_k)^{q^k})^{1/q^i} = (\alpha^\sharp)^{1/q^i}$$

when we change variables $k = i + j$, and a_i are lifts of α_j. And this yields θ is also well-defined. Now, if we begin with $(..., a_i, ..., a_1, ..., a_0) \in \varprojlim_{(.)^q} \mathcal{O}_K$, then

$$\theta\psi(..., a_i, ..., a_1, a_0) = \theta(..., a_i \mod \omega\mathcal{O}_K, ..., a_0 \mod \omega\mathcal{O}_K) =$$

$$= \theta(..., \alpha_i, ..., \alpha_1, \alpha_0) = (..., (\alpha^{1/q^i})^\sharp, ..., (\alpha^{1/q})^\sharp, \alpha^\sharp)$$

where $\alpha_i = a_i \mod \omega\mathcal{O}_K$, and $\alpha = (..., \alpha_i, ..., \alpha_0)$. We have $(\alpha^{1/q^i})^\sharp = \lim_{j\to\infty}(a_{i+j}^{q^j})$. Because $a_{i+1}^q = a_i$, we have $a_j^{q^{i+j}} = a_i$. And hence $(\alpha^{1/q^i})^\sharp = a_i$. And hence, $\theta \circ \psi$ is just the identity map.

Now, if we begin with $\alpha = (..., \alpha_i, ..., \alpha_1, \alpha_0) \in \mathcal{O}_{K^\flat}$, then we first note that $\alpha^\sharp \equiv \alpha_0 \mod \omega\mathcal{O}_K$, hence

$$\psi \circ \theta(\alpha) = \psi(..., (\alpha^{1/q^i})^\sharp, ..., (\alpha^{1/q})^\sharp, \alpha^\sharp) = \alpha$$

So, this yields ψ and θ are inverse of each other. The multiplicative properties are easy to check. □

Our net goal is to prove that in fact $\mathcal{O}_{K^\flat}$ is an integral domain of characteristic p, and that it is complete. We first introduce the following map on $\mathcal{O}_{K^\flat}$

$$|.|_\flat : \mathcal{O}_{K^\flat} \to \mathbb{R}$$

defined as $|\alpha|_\flat := |\alpha^\sharp|$.

Proposition 3.1.6.

(i) $|.|_\flat$ *is non-archimedean norm on* $\mathcal{O}_{K^\flat}$.

(ii) $|\mathcal{O}_{K^\flat}| = |\mathcal{O}_K|$

(iii) For $\alpha, \beta \in \mathcal{O}_{K^\flat}$, $\alpha\mathcal{O}_{K^\flat} \subset \beta\mathcal{O}_{K^\flat}$ *iff* $|\alpha|_\flat \le |\beta|_\flat$.

(iv) $\mathcal{O}_{K^\flat}$ *is a local domain of char. p, with the unique maximal ideal* $\mathfrak{m}_{K^\flat} = \{\alpha \in \mathcal{O}_{K^\flat} | |\alpha|_\flat < 1\}$.

(v) $\mathcal{O}_{K^\flat}/\mathfrak{m}_{K_\flat} \cong \mathcal{O}_K/\mathfrak{m}_K$.

(vi) Let $\omega^\flat \in \mathcal{O}_{K^\flat}$*, such that* $|\omega^\flat|_\flat = |\omega|$*, then the map* $\mathcal{O}_{K^\flat}/\omega^\flat\mathcal{O}_{K^\flat} \to \mathcal{O}_K/\omega\mathcal{O}_K$ *defined as* $\alpha \mapsto \alpha^\sharp \mod \omega\mathcal{O}_K$ *is an isomorphism of rings.*

Proof. We first fix $\alpha := (..., \alpha_i, ..., \alpha_1, \alpha_0), \beta := (..., \beta_i, ..., \beta_1, \beta_0)$ in $\mathcal{O}_{K^\flat}$, and $a_i := (\alpha^{1/q^i})^\sharp, b_i := (\beta^{1/q^i})^\sharp$, we know that $b_{i+1}^q = b_i, a_{i+1}^q = a_i$.

(i) We have

$$|\alpha+\beta|_\flat = |(\alpha+\beta)^\sharp| = |\lim_{i\to\infty}(a_i+b_i)^{q^i}| = \lim_{i\to\infty}|(a_i+b_i)^{q^i}|$$

$$\leq \lim_{i\to\infty}\max\{|a^{q^i}|, |b^{q^i}|\} = \lim_{i\to\infty}\{|a_0|, |b_0|\} = \max\{|\alpha|^\sharp|, |\beta^\sharp|\} = \max\{|\alpha|_\flat, |\beta|_\flat\}$$

Also, assume that $|\alpha|_\flat = 0$, this yields $\alpha^\sharp = a_0 = 0$, and $\alpha = 0$. The multiplicative property of $|.|_\flat$ is easy to check. So, it is a non-archimedean norm on $\mathcal{O}_{K^\flat}$.

(ii) From the definition, we have $|\mathcal{O}_{K^\flat}|_\flat \subseteq |\mathcal{O}_K|$. Take any $a \in \mathcal{O}_K$, we know that there exists some b, such that $|\omega| < |b| \leq 1$, and $|a| = |b|^{q^m}$. We can find $\alpha \in \mathcal{O}_{K^\flat}$ such that $\alpha_0 \equiv b \mod \omega\mathcal{O}_K$. This yields $\alpha^\sharp \equiv b \mod \omega\mathcal{O}_K$, and $|\beta^\sharp - b| \leq |\omega|$. It follows that $|\beta^\sharp| = |b|$. So, we get $|\alpha|_\flat = |b|$, and $|a| = |\beta^{q^m}|_\flat$. So $\mathcal{O}_{K^\flat} = \mathcal{O}_K$.

(iii) Assume that $\alpha\mathcal{O}_{K^\flat} \subseteq \beta\mathcal{O}_{K^\flat}$. Then there exists some $\gamma \in \mathcal{O}_{K^\flat}$, such that $\alpha = \beta\gamma$, and this yields $|\alpha|_\flat \leq |\beta|_\flat$. Conversely, assume $|\alpha|_\flat \leq |\beta|_\flat$, which yields $|(\alpha^{1/q^i})^\sharp| \leq |(\beta^{1/q^i})^\sharp|$, because $|\alpha^{1/q^i}|_\flat \leq |\beta^{1/q^i}|_\flat$. And this yields $|a_i| \leq |b_i|$, and there exists some $c_i \in \mathcal{O}_K$, such that $c_i a_i = b_i$. It follows directly that $c_{i+1}^q = c_i$. And hence, $\gamma := (..., c_i \mod \omega\mathcal{O}_K, ..., c_1 \mod \omega\mathcal{O}_K, c_0 \mod \omega\mathcal{O}_K)$ defines an element in $\mathcal{O}_{K^\flat}$. And it is clear that $\alpha\gamma = \beta$, and $\alpha\mathcal{O}_{K^\flat} \subseteq \beta\mathcal{O}_{K^\flat}$.

(iv) Now, if we take any element $\gamma \in \mathcal{O}_{K^\flat} \setminus \mathfrak{m}_{K^\flat}$, then we can see by our recent argument that $\gamma\mathcal{O}_{K^\flat} = \mathcal{O}_{K^\flat}$, i.e. γ is invertible. This yields $\mathcal{O}_{K^\flat}$ is local with maximal ideal $\mathfrak{m}_{K^\flat}$. Assume for now, $\alpha\beta = 0$, this yields $|\alpha\beta|_\flat = |a_0 b_0| = 0$, and hence, $a_0 = 0$ or $b_0 = 0$. From this $\alpha = 0$ or $\beta = 0$. This implies $\mathcal{O}_{K^\flat}$ is a domain.

(v) Let us consider the map $\psi : \mathcal{O}_{K^\flat} \to \mathcal{O}_K/\mathfrak{m}_K$ defined by $\psi(\alpha) = \alpha^\sharp \mod \mathfrak{m}_K$. We can see easily that $\psi(\alpha\beta) = \psi(\alpha)\psi(\beta)$. Also,

$$\psi(\alpha+\beta) \equiv (\alpha+\beta)^\sharp \equiv a_0 + b_0 \mod \omega\mathcal{O}_K \equiv a_0 + b_0 \mod \mathfrak{m}_K$$

So, ψ is a ring homomorphism. Take any $a_0 \in \mathcal{O}_K$, we can find $a_1 \in \mathcal{O}_K$ such that $a_1^q \equiv a_0 \mod p\mathcal{O}_K$. It follows $a_1^q \equiv a_0 \mod \mathfrak{m}_K$ and $a_1^q \equiv a_0 \mod \omega\mathcal{O}_K$. Continuing this process, we get $\alpha := (..., a_i \mod \omega\mathcal{O}_K, ..., a_0 \mod \omega\mathcal{O}_K) \in \mathcal{O}_{K^\flat}$, and $\alpha^\sharp \equiv a_0 \mod \omega\mathcal{O}_K \equiv a_0 \mod \mathfrak{m}_K$. And ψ is surjective. From (iii), we have

$$\ker\psi = \{\alpha \in \mathcal{O}_{K^\flat} | \alpha^\sharp \in \mathfrak{m}_K\} = \{\alpha \in \mathcal{O}_{K^\flat} | |\alpha^\sharp| < 1\} = \{\alpha \in \mathcal{O}_{K^\flat} | |\alpha|_\flat < 1\} = \mathfrak{m}_{K^\flat}$$

And this yields $\mathcal{O}_{K^\flat}/\mathfrak{m}_{K^\flat} = \mathcal{O}_K/\mathfrak{m}_K$.

(vi) It follows from (v) that the map $\theta : \mathcal{O}_{K^\flat} \to \mathcal{O}_K/\omega\mathcal{O}_K$ is surjective, with

$$\ker\theta = \{\alpha \in \mathcal{O}_{K^\flat} | \alpha^\sharp| \leq |\omega|\} = \{\alpha \in \mathcal{O}_{K^\flat} | |\alpha|_\flat \leq |\omega^\flat|_\flat\} = \omega^\flat\mathcal{O}_{K^\flat}$$

So, $\mathcal{O}_{K^\flat}/\omega^\flat\mathcal{O}_{K^\flat} \cong \mathcal{O}_K/\omega\mathcal{O}_K$. □

With this kind of topology, we can prove

Proposition 3.1.7. $\mathcal{O}_{K^\flat}$ *is complete with respect to the norm* $|.|_\flat$.

Proof. We have $\mathcal{O}_{K^\flat} = \varprojlim_{(.)^q} \mathcal{O}_K/\omega\mathcal{O}_K$, and we can equip each $\mathcal{O}_K/\omega\mathcal{O}_K$ the discrete topology, and $\prod_{\mathbb{N}} \mathcal{O}_K/\omega\mathcal{O}_K$ the product topology, and $\mathcal{O}_{K^\flat}$ is a topological subgroup of $\prod_{\mathbb{N}} \mathcal{O}_K/\omega\mathcal{O}_K$, which has a fundamental system of open neighborhoods around 0 defined as

$$U_m := \{(..., a_{m+1}, 0, ..., 0)\}(m \geq 1)$$

and $U_1 \supset U_2 \supset ...$ forms a filtration. We will prove that with this topology, $\mathcal{O}_{K^\flat}$ is complete, and it coincides with the topology defined by $|.|_\flat$. For the first statement, it is sufficient to prove any Cauchy sequence converges in $\mathcal{O}_{K^\flat}$.

Let $(x_n)_n$ be a Cauchy sequence in $\mathcal{O}_{K^\flat}$. We can represent each x_n as $(..., x_{n,i}, ..., x_{n,1}, x_{n,0})$, with $x_{n,i+1}^q = x_{n,i}$. And for all $k \geq 0$, there exists some m_k such that $\forall m, n \geq m_k$, $x_m - x_n \in U_{k+1}$, and $m_{k+1} > m_k$. This yields $x_{m,i} - x_{n,i} = 0(\forall 0 \leq i \leq k+1; m, n \geq m_k)$.

Let $x := (..., x_{m_i,i}, ..., x_{m_1,1}, x_{m_0,0})$. We can see that $x_{m_i,i+1} = x_{m_{i+1},i+1}$, and hence $x_{m_i,i+1}^q = x_{m_i,i} = x_{m_{i+1},i+1}^q$. So, $x \in \mathcal{O}_{K^\flat}$. Now, for any $k \geq 0$, $n \geq m_k$, we have $x - x_n = (x - x_{m_k}) - (x_n - x_{m_k})$. It can be seen that for any $0 \leq i \leq k+1$, we have $x_{m_k,i} - x_{m_i,i} = 0$, so $x - x_{m_k} \in U_{k+1}$, and $x_n - x_{m_k} \in U_{k+1}$. And this yields $(x_n)_n$ converges to x. Hence, with this topology, $\mathcal{O}_{K^\flat}$ is complete. On the other hand, we have

$$U_m = \{\alpha \in \mathcal{O}_{K^\flat} | (\alpha^{1/q^m})^\sharp \in \omega\mathcal{O}_K\} = \{\alpha \in \mathcal{O}_{K^\flat} || \alpha^{1/q^m}|_\flat \leq |\omega^\flat|_\flat\} = (\omega^\flat)^{q^m}\mathcal{O}_{K^\flat}$$

And hence $\{U_m\}_{m\geq 1}$ also forms a fundamental system of open neighborhoods around 0 with the topology induced by $|.|_\flat$. It follows that the two topology coincide. And this yields $\mathcal{O}_{K^\flat}$ is complete. □

For now, it makes sense to talk about $K^\flat$, the fraction field of $\mathcal{O}_{K^\flat}$. It is a field of characteristic p. By extending the norm $|.|_\flat$ to $K^\flat$, it is complete and non-archimedean. Also, the inverse map of ψ in 3.1.5 can be extended to a multiplicative bijection

$$K^\flat \xrightarrow{\cong} \varprojlim_{(.)^q} K$$

defined by $\alpha \mapsto (..., (\alpha^{1/q^i})^\sharp, ..., (\alpha^{1/q})^\sharp, \alpha^\sharp)$.

Definition. . $K^\flat$ is called the **tilt** of K.

An important observation is that

Proposition 3.1.8. *$\mathbb{C}_p^\flat$ is algebraically closed.*

Proof. See [Sch17](Lemma 1.4.10). □

3.2 Galois actions and field of norms

In this section, we will construct the field of norm E_L of L, and discuss about the actions of Galois groups on E_L. We first explain how $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ acts on $\mathbb{C}_p$. We know that any element in $a \in \mathbb{C}_p$ is actually a Cauchy sequence $(a_n)_n$ in $\overline{\mathbb{Q}_p}$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, we then have $|a_n| = |\sigma(a_n)|$, for all n, and $|a_m - a_n| = |\sigma(a_m) - \sigma(a_n)|$. From this, we can see that σ acts on $\mathbb{C}_p$ as a continuous field automorphism.

Lemma 3.2.1. *Let $a \in \mathbb{C}_p$, then for any integer m, there exists $b \in \overline{\mathbb{Q}_p}$, such that $a - b \in p^m\mathcal{O}_{\mathbb{C}_p}$.*

Proof. The statement is equivalent to find $b \in \overline{\mathbb{Q}_p}$, such that $|a - b| \leq 1/p^m$. Because $\overline{\mathbb{Q}_p}$ is dense in $\mathbb{C}_p$, we can easily find such a b. □

Lemma 3.2.2. *Let $\sigma \in Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, then σ preserves $p^m\mathcal{O}_{\mathbb{C}_p}$, for all integer m.*

Proof. Take any $a \in p^m \mathcal{O}_{\mathbb{C}_p}$, i.e. $|a| \le 1/p^m$, we have to prove that $|\sigma(a)| \le 1/p^m$. One can represent $a = (a_n)_n$, where $(a_n)_n$ is a Cauchy sequence in $\overline{\mathbb{Q}_p}$, then

$$|a| = \lim_{n\to\infty} |a_n| = \lim_{n\to\infty} |\sigma(a_n)| = |\sigma(a)|$$

Hence, $\sigma(a) \in p^m \mathcal{O}_{\mathbb{C}_p}$ $\square$

As a corollary, we get

Corollary 3.2.3. *The action Gal$(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \times \mathbb{C}_p \to \mathbb{C}_p$ is continuous.*

Proof. For any $a \in \mathbb{C}_p$, a fundamental system of open neighborhoods around a is of the form $\{a + p^m\mathcal{O}_{\mathbb{C}_p} | m \ge 1\}$. Take $W := \sigma(a) + p^m\mathcal{O}_{\mathbb{C}_p}$ as an open neighborhood of $\sigma(a) \in \mathbb{C}_p$. By Lemma 3.2.1, there exists $b \in \overline{\mathbb{Q}_p}$, such that $a + p^m\mathcal{O}_{\mathbb{C}_p} = b + p^m\mathcal{O}_{\mathbb{C}_p}$. We then take F a finite Galois extension of $\mathbb{Q}_p$ containing b, and $U := \mathrm{Gal}(\overline{\mathbb{Q}_p}/F)$, then U is an open neighborhood of *id* in $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, and U fixes b. By using Lemma 3.2.2, we have

$$\sigma U \times (a + p^m\mathcal{O}_{\mathbb{C}_p}) = \sigma U \times (b + p^m\mathcal{O}_{\mathbb{C}_p}) = \sigma(b) + p^m\mathcal{O}_{\mathbb{C}_p} = \sigma(a) + p^m\mathcal{O}_{\mathbb{C}_p}$$

And this yields the action above is continuous. $\square$

Let L_∞ be the Lubin-Tate extension of L, and $\widehat{L_\infty}$ its completion. We can see $G_L := \mathrm{Gal}(\overline{\mathbb{Q}_p}/L)$ preserves $\pi\mathcal{O}_{\mathbb{C}_p}$, and it acts on $\mathcal{O}_{\mathbb{C}_p}/\pi\mathcal{O}_{\mathbb{C}_p}$ as ring automorphisms. They induce an action

$$\begin{aligned} G_L \times \mathcal{O}_{\mathbb{C}_p^\flat} &\longrightarrow \mathcal{O}_{\mathbb{C}_p^\flat} \\ (\sigma, (..., a_i \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., a_0 \mod \pi\mathcal{O}_{\mathbb{C}_p})) &\longmapsto (..., \sigma(a_i) \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., \sigma(a_0) \mod \pi\mathcal{O}_{\mathbb{C}_p}) \end{aligned}$$

as ring automorphisms.

Let $\alpha := (..., a_i \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., a_0 \mod \pi\mathcal{O}_{\mathbb{C}_p})$, we have $\alpha^\sharp = \lim_{i\to\infty} a_i^{q^i}$, and $\sigma(\alpha) = (..., \sigma(a_i) \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., \sigma(a_0) \mod \pi\mathcal{O}_{\mathbb{C}_p})$, and $\sigma(\alpha)^\sharp = \lim_{i\to\infty} \sigma(a_i)^{q^i} = \sigma(\lim_{i\to\infty} a_i^{q^i}) = \sigma(\alpha^\sharp)$. Also, from this $|\alpha|_\flat = |\alpha^\sharp|$ and $|\sigma(\alpha)|_\flat = |\sigma(\alpha)^\sharp| = |\sigma(\alpha^\sharp)| = |\alpha^\sharp|$. So, σ preserves $|.|_\flat$.

Lemma 3.2.4. *The action $G_L \times \mathcal{O}_{\mathbb{C}_p^\flat} \to \mathcal{O}_{\mathbb{C}_p^\flat}$ is continuous.*

Proof. We first note that $\mathcal{O}_{\mathbb{C}_p}/\pi\mathcal{O}_{\mathbb{C}_p} \cong \mathcal{O}_{\overline{\mathbb{Q}_p}}/\pi\mathcal{O}_{\overline{\mathbb{Q}_p}}$, because $\mathcal{O}_{\mathbb{C}_p}$ is the completion of $\mathcal{O}_{\overline{\mathbb{Q}_p}}$. From this, $\mathcal{O}_{\mathbb{C}_p^\flat} = \varprojlim_{(.)^q} \mathcal{O}_{\overline{\mathbb{Q}_p}}/\pi\mathcal{O}_{\overline{\mathbb{Q}_p}}$, with $\mathcal{O}_{\overline{\mathbb{Q}_p}}/\pi\mathcal{O}_{\overline{\mathbb{Q}_p}}$ is equipped with discrete topology (Proposition 3.1.7). But then, it follows easily that G_L acts continuously on the product $\prod_{\mathbb{N}_0} \mathcal{O}_{\overline{\mathbb{Q}_p}}/\pi\mathcal{O}_{\overline{\mathbb{Q}_p}}$. In particular, G_L acts continuously on $\mathcal{O}_{\mathbb{C}_p^\flat}$. $\square$

And we can now extend the action from G_L to $\mathbb{C}_p^\flat$.

Proposition 3.2.5. *The action $G_L \times \mathbb{C}_p^\flat \to \mathbb{C}_p^\flat$ is continuous.*

Proof. Due to the previous lemma, for any $b \in \mathcal{O}_{\mathbb{C}_p^\flat}$, the map

$$\begin{aligned} \psi_b : G_L &\longrightarrow \mathcal{O}_{\mathbb{C}_p^\flat} \\ \sigma &\longmapsto \sigma(b) \end{aligned}$$

is continuous. Now, let $b \in \mathbb{C}_p^\flat \setminus \mathcal{O}_{\mathbb{C}_p^\flat}$, i.e. $|b|_\flat > 1$, so $|1/b|_\flat < 1$, and $1/b \in \mathcal{O}_{\mathbb{C}_p^\flat}$. So the map ψ_b is the composition of $\psi_{1/b} : G_L \to \mathcal{O}_{\mathbb{C}_p^\flat}$ and $\mathcal{O}_{\mathbb{C}_p^\flat} \xrightarrow{x \mapsto 1/b} \mathbb{C}_p^\flat$, and both are continuous. So, for all $b \in \mathbb{C}_p^\flat$, the map ψ_b is continuous.

Let us take $U := U_m = \{...a_{m+1}, 0, ..., 0\}$ as in Proposition 3.1.7, which forms a fundamental system of open neighborhoods around 0, then because ψ_b is continuous, for any fixed $\sigma \in G_L$, there exists V:

open neighborhood of σ such that $\psi_b(V) \subset \sigma(b) + U_m$. This yields for any $\theta \in V, \theta(b) \in \sigma(b) + U_m$. It also follows easily that any $\theta \in G_L$ preserves U_m. So, we get

$$V \times (b + U_m) \subset \sigma(b) + U_m$$

And hence, the action from G_L to $\mathbb{C}_p^\flat$ is continuous. $\square$

Let us denote $H_L := \mathrm{Gal}(\overline{\mathbb{Q}_p}/L_\infty)$, then by continuity, H_L fixes $\widehat{L_\infty}$, and it also fixes $\widehat{L_\infty}^\flat$. Hence, the actions from G_L to $\widehat{L_\infty}^\flat$ can be reduced to the continuous actions from $\Gamma_L := \mathrm{Gal}(L_\infty/L)$ to $\widehat{L_\infty}^\flat$. And the action from $\overline{\sigma} \in \Gamma_L$ to $\widehat{L_\infty}^\flat$ is induced from the action of $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/L)$, where $\sigma|_{L_\infty} = \overline{\sigma}$.

Our next goal is to construct the field of norm E_L of L, and see how Γ_L acts on it. We first fix ϕ a Frobenius series on $\mathcal{O}[[X]]$ as in Chapter I. We recall from our first chapter about Lubin-Tate theory that there exists an isomorphism of topological group

$$\begin{aligned} \chi_L : \Gamma_L &\longrightarrow \mathcal{O}^\times \\ \sigma &\longmapsto \chi_L(\sigma) \end{aligned}$$

.

Let us define the **Tate module**

$$T := \varprojlim(\dots \xrightarrow{[\pi]_\phi} \mathscr{F}_n \xrightarrow{[\pi]_\phi} \dots \xrightarrow{[\pi]_\phi} \mathscr{F}_1)$$

Take any $\sigma \in \Gamma_L$, then for any $y := (y_n)_n \in T$, we can define the action from G_L to Tate module as follows

$$\sigma((y_n)_n) := (\sigma(y_n))_n$$

It is well-defined since $[\pi]_\phi(\sigma(y_{n+1})) = \sigma([\pi]_\phi(y_{n+1})) = \sigma(y_n)$. Also, T is a free $\mathcal{O}$-module of rank 1, and the action from $a \in \mathcal{O}$ on T is give by

$$a((y_n)_n) = ([a]_\phi(y_n))_n$$

This is again well-defined since $[\pi]_\phi \circ [a]_\phi = [a]_\phi \circ [\pi]_\phi$. Hence, for any $\sigma \in \Gamma_L$, we have

$$\sigma(y) = [\chi_L(\sigma)]_\phi(y) \tag{3.1}$$

.

We will next construct E_L as follows. Let $y \in T$, then because $[\pi]_\phi = \phi$ and $\phi(X) \equiv X^q \mod \pi\mathcal{O}[[X]]$, we have

$$y_n = \phi(y_{n+1}) \equiv y_{n+1}^q \mod \pi\mathcal{O}_{L_\infty}$$

and $\phi(y_1) = 0 \equiv y_1^q \mod \pi\mathcal{O}_{L_\infty}$, so that the map

$$\begin{aligned} \iota : T &\longrightarrow \mathcal{O}_{\widehat{L_\infty}^\flat} \\ (y_n)_n &\longmapsto (, \dots, y_i \mod \pi\mathcal{O}_{L_\infty}, \dots, y_1 \mod \pi\mathcal{O}_{L_\infty}, 0) \end{aligned}$$

is well-defined. Let us fix a generator (of $\mathcal{O}$-module) t of T, where $t = (\dots, z_n, \dots, z_1)$, and z_n is a generator for $\mathcal{O}/\pi^n\mathcal{O}$-module. Let $\omega := \iota(t) = (\dots, z_n \mod \pi\mathcal{O}_{L_\infty}, \dots, z_1 \mod \pi\mathcal{O}_{L_\infty}, 0)$. We have

Lemma 3.2.6. $|\omega|_\flat = |\pi|^{q/q-1}$

Proof. We have $|\omega|_\flat = \lim_{i\to\infty} |z_i|^{q^i}$, and we know that $|z_i| = |\pi|^{1/(q-1)q^{i-1}}$, so that $|\omega|_\flat = |\pi|^{q/q-1}$. $\square$

Because of this $|\omega|_\flat < 1$, and since $\mathcal{O}_{\widehat{L_\infty}^\flat}$ is complete, the map

$$\begin{aligned} k[[X]] &\longrightarrow \mathcal{O}_{\widehat{L_\infty}^\flat} \\ f(x) &\longmapsto f(\omega) \end{aligned}$$

is well-defined. And it is extended to the field embedding $k((X)) \hookrightarrow \widehat{L_\infty}$. The image is denoted E_L, and it is called the **field of norms** of L.

We now see how Γ_L acts on E_L. First, let $\sigma \in \Gamma_L$, we have for any $y := (y_n)_n \in T$

$$\iota(\sigma(y)) = \iota((\sigma(y_n))_n) = (\sigma(y_n) \mod \pi\mathcal{O}_{L_\infty})_n = \sigma((y_n \mod \pi\mathcal{O}_{L_\infty})_n) = \sigma(\iota(y))$$

So, we get

$$\iota \circ \sigma = \sigma \circ \iota \tag{3.2}$$

And we are now ready to prove the main results of this section

Proposition 3.2.7.

(i) For $a \in \mathcal{O}$, let us define $\overline{[a]}(X) := [a]_\phi(X) \mod \pi \in k[[X]]$, then $\forall \sigma \in \Gamma_L$, we have $\sigma(\omega) = \overline{[\chi_L(\sigma)]}(\omega)$.

(ii) The action from Γ_L preserves E_L.

(iii) E_L does not depend on the choice of the generator $t \in T$.

Proof.

(i) By 3.2, and 3.1, respectively, we have

$$\sigma(\omega) = \sigma(\iota(t)) = \iota(\sigma(t)) = \iota([\chi_L(\sigma)]_\phi(t)) = (..., [\chi_L]_\phi(z_n) \mod \pi\mathcal{O}_{L_\infty}, ..., 0) =$$
$$= \overline{[\chi_L(\sigma)]}(..., z_n \mod \pi\mathcal{O}_{L_\infty}, ..., 0) = \overline{[\chi_L(\sigma)]}(\omega)$$

(ii) This follows easily since $E_L \cong k((x))$ is complete, and $|\omega|_\flat < 1$, this yields by (i) that $\sigma(\omega) = \overline{[\chi_L(\sigma)]}(\omega) \in E_L$.

(iii) If we replace t by at, where $a \in \mathcal{O}^\times$, then there exists $\sigma \in \Gamma_L$, such that $\chi_L(\sigma) = a$, and by 3.1

$$at = [\chi_L(\sigma)]_\phi(t) = \sigma(t)$$

And by 3.2

$$\iota(at) = \iota(\sigma(t)) = \sigma(\iota(t)) = \sigma(\omega)$$

And due to (i), $\sigma(\omega) \in E_L$, and so is $\iota(at)$. This yileds the field obtained by at is a subfield of E_L. By symmetry, they are the same.

□

We can briefly explain why E_L is called the field of norms. Let us denote $\Gamma_n := \mathrm{Gal}(L_n/L)$, we can define the ramification subfroups of Γ_n

$$\Gamma_{n,i} := \{\sigma \in \Gamma_n | \sigma(z_n) \equiv z_n \mod z_n^{i+1}\mathcal{O}_{L_n}\}$$

where $z_n \in \mathscr{F}_n$ is a generator for $\mathscr{F}_n$ as $\mathcal{O}_L/\pi^n\mathcal{O}_L$-module. And it can be computed without difficulty [...] that for $1 \leq m \leq n, q^{m-1} \leq i < q^m$, $\Gamma_{m,i} = \mathrm{Gal}(L_n/L_m)$. And in particular,

$$\begin{aligned}\mathrm{Gal}(L_{n+1}/L_n) = \Gamma_{n+1,q^n-1} = \{\sigma \in \Gamma_{n+1} | \sigma(z_{n+1}) \equiv z_{n+1} \mod z_{n+1}^{q^n}\mathcal{O}_{L_{n+1}}\} = \\ = \{\sigma \in \Gamma_{n+1} | \sigma(z_{n+1}) \equiv z_{n+1} \mod z_1\mathcal{O}_{L_{n+1}}\}\end{aligned}$$

And this yields for any $y \in \mathcal{O}_{L_{n+1}}$, we have

$$\mathrm{Norm}_{L_{n+1}/L_n}(y) = \prod_{\sigma \in \mathrm{Gal}(L_{n+1}/L_n)} \sigma(y) \equiv y^q \mod z_1\mathcal{O}_{L_{n+1}} \tag{3.3}$$

Let us consider the map

$$\begin{aligned}\mathcal{O}_{L_n} &\longrightarrow \mathcal{O}_{L_{n+1}}/z_1\mathcal{O}_{L_{n+1}} \\ a &\longmapsto a \mod z_1\mathcal{O}_{L_{n+1}}\end{aligned}$$

This map has kernel $z_1\mathcal{O}_{L_n}$, so we have an embedding $\psi : \mathcal{O}_{L_n}/z_1\mathcal{O}_{L_n} \hookrightarrow \mathcal{O}_{L_{n+1}}/z_1\mathcal{O}_{L_{n+1}}$. And this yields for any $b \in \mathcal{O}_{L_{n+1}}$, $b \mod z_1\mathcal{O}_{L_{n+1}}$ is in $\psi(\mathcal{O}_{L_n}/z_1\mathcal{O}_{L_n})$ iff there exists some $a \in \mathcal{O}_{L_n}$ such that

$$b \mod z_1\mathcal{O}_{L_{n+1}} = a \mod z_1\mathcal{O}_{L_{n+1}}$$

It follows that the map $\mathcal{O}_{L_{n+1}}/z_1\mathcal{O}_{L_{n+1}} \xrightarrow{(.)^q} \mathcal{O}_{L_{n+1}}/z_1\mathcal{O}_{L_{n+1}}$ has the image contained in $\psi(\mathcal{O}_{L_n}/z_1\mathcal{O}_{L_n})$ by 3.3. Let us consider the map

$$\begin{aligned}\varprojlim_{\mathrm{Norm}} \mathcal{O}_{L_n}/z_1\mathcal{O}_{L_n} &\longrightarrow \varprojlim_{(.)^q} \mathcal{O}_{L_\infty}/z_1\mathcal{O}_{L_\infty} \\ (y_n \mod z_1\mathcal{O}_{L_n)_n} &\longmapsto (y_n \mod z_1\mathcal{O}_{L_\infty})_n\end{aligned}$$

Take any y_{n+1}, we have $y_n = \mathrm{Norm}_{L_{n+1}/L_n}(y_{n+1}) \equiv y_{n+1}^q \mod z_1\mathcal{O}_{L_{n+1}}$. So the map above is well-defined. Furthermore, we have for any n the injectivity $\mathcal{O}_{L_n}/z_1\mathcal{O}_{L_n} \hookrightarrow \mathcal{O}_{L_\infty}/z_1\mathcal{O}_{L_\infty}$. So the map above is injective. Also, because $|z_1| = |\pi|^{1/q-1} \geq |\pi|$, we have $\varprojlim_{(.)^q} \mathcal{O}_{L_\infty}/z_1\mathcal{O}_{L_\infty} = \mathcal{O}_{\widehat{L_\infty}^\flat}$, and so, we obtain an embedding

$$\varprojlim_{\mathrm{Norm}} \mathcal{O}_{L_n}/z_1\mathcal{O}_{L_n} \hookrightarrow \mathcal{O}_{\widehat{L_\infty}^\flat}$$

And it is showed by Wintenberger [Win83] that $\varprojlim_{\mathrm{Norm}} \mathcal{O}_L/z_1\mathcal{O}_L \cong \mathcal{O}_{E_L}$. And that is why E_L is called field of norms.

3.3 Un-tilting

We have seen that from a perfectoid field, we can construct its tilt, which is a perfect, complete subfield of $\mathbb{C}_p^\flat$. In this section, we will prove that there is a bijective map (note that we are always interested perfectoid fields containing L_∞).

$$\{\text{perfectoid fields}\} \leftrightarrow \{\text{complete, perfect field } \widehat{L_\infty}^\flat \subseteq F \subseteq \mathbb{C}_p^\flat\}\}$$

Let us begin with a perfectoid field K. We know that $\mathcal{O}_{K^\flat}$ is complete and perfect by Proposition 3.1.7. We will construct a surjective $\mathcal{O}$-algebra homomorphism

$$\Theta_K : W(\mathcal{O}_{K^\flat}) \to \mathcal{O}_K$$

via several steps.

Step 1. Consider the following diagram of $\mathcal{O}$-algebra

$$\begin{array}{ccccc} W_{n+1}(\mathcal{O}_K) & \xrightarrow{\Phi_n} & \mathcal{O}_K & \xrightarrow{pr} & \mathcal{O}_K/\pi^n\mathcal{O}_K \\ \big\downarrow \text{pr} & & & & \\ W_n(\mathcal{O}_K) & & \xrightarrow{W(\text{pr})} & & W_n(\mathcal{O}_K/\pi\mathcal{O}_K) \end{array}$$

we have

$$\Phi_n(a_0, ..., a_n) = a_0^{q^n} + ... + \pi^{n-1}a_{n-1}^q + \pi^n a_n$$

From this, if $a_i = \pi b_i (i = 0, ..., n-1)$, then

$$\Phi_n(a_0, ..., a_n) \equiv 0 \mod \pi^n\mathcal{O}_K$$

And the map $W(\text{pr}) \circ \text{pr} : W_{n+1}(\mathcal{O}_K) \to W_n(\mathcal{O}_K/\pi\mathcal{O}_K)$ has the kernel $\{(\pi b_0, ..., \pi b_{n-1}, a_n)\}$, so there exists only one $\mathcal{O}$-algebra homomorphism $\theta_n : W_n(\mathcal{O}_K/\pi\mathcal{O}_K) \to \mathcal{O}_K/\pi^n\mathcal{O}_K$ making the diagram above commute. And it follows that

$$\theta_n(a_0 \mod \pi\mathcal{O}_K, ..., a_{n-1} \mod \pi\mathcal{O}_K) = a_0^{q^n} + ... + \pi^{n-1}a_{n-1}^q \mod \pi^n\mathcal{O}_K$$

From this, we obtain the following diagram

$$\begin{array}{ccc} W_{n+1}(\mathcal{O}_K/\pi\mathcal{O}_K) & \xrightarrow{\theta_{n+1}} & \mathcal{O}_K/\pi^{n+1}\mathcal{O}_K \\ \big\downarrow \text{pr} & & \\ W_n(\mathcal{O}_K/\pi\mathcal{O}_K) & & \big\downarrow \text{pr} \\ \big\downarrow F & & \\ W_n(\mathcal{O}_K/\pi\mathcal{O}_K) & \xrightarrow[\theta_n]{} & \mathcal{O}_K/\pi^n\mathcal{O}_K \end{array} \tag{3.4}$$

This diagram is commutative since

$$\begin{aligned} \theta_{n+1}(a_0 \mod \pi\mathcal{O}_K, ..., a_n \mod \pi\mathcal{O}_K) = a_0^{q^{n+1}} + ... + \pi^n a_n^q \mod \pi^{n+1}\mathcal{O}_K = \\ = a_0^{q^{n+1}} + ... + \pi^{n-1}a_{n-1}^{q^2} \mod \pi^n\mathcal{O}_K \end{aligned}$$

Also,

$$\theta_n \circ F \circ \text{pr}(a_0 \mod \pi\mathcal{O}_K, ..., a_n \mod \pi\mathcal{O}_K) = \theta_n(a_0^q \mod \phi\mathcal{O}_K, ..., a_{n-1}^q \mod \pi\mathcal{O}_K) =$$

$$= a_0^{q^{n+1}} + ... + \pi^{n-1}a_{n-1}^{q^2} \mod \pi^n\mathcal{O}_K$$

Step 2. Let us consider the projection map

$$\text{pr}_i : \mathcal{O}_{K^\flat} = \varprojlim_{(.)^q} \mathcal{O}_K/\pi\mathcal{O}_K \longrightarrow \mathcal{O}_K/\pi\mathcal{O}_K$$
$$(\ldots, \alpha_i, \ldots, \alpha_1, \alpha_0) \longmapsto \alpha_i$$

It can be lifted to the map

$$W(\text{pr}_i) : W(\mathcal{O}_{K^\flat}) \longrightarrow W(\mathcal{O}_K/\pi\mathcal{O}_K)$$
$$(\alpha^{(0)}, ..., \alpha^{(n)}, ...) \longmapsto (\alpha_i^{(0)}, ..., \alpha_i^{(n)})$$

where $\alpha^{(n)} = (\ldots, \alpha_i^{(n)}, \ldots, \alpha_1^{(n)}, \alpha_0^{(n)}) \in \mathcal{O}_{K^\flat}$. And this yields the map

$$W_n(\text{pr}_n) : W_n(\mathcal{O}_{K^\flat}) \longrightarrow W_n(\mathcal{O}_K/\pi\mathcal{O}_K)$$
$$(\alpha^{(0)}, ..., \alpha^{(n-1)}) \longmapsto (\alpha_n^{(0)}, ..., \alpha_n^{(n-1)})$$

And for each n, we can also form the map

$$p_n: \qquad W(\mathcal{O}_{K^\flat}) \xrightarrow{pr} W_n(\mathcal{O}_{K^\flat}) \xrightarrow{W(pr)} W_n(\mathcal{O}_K/\pi\mathcal{O}_K)$$

$$(\alpha^{(0)}, ..., \alpha^{(i)}, ...) \longrightarrow (\alpha_n^{(0)}, ..., \alpha_n^{(n-1)})$$

And for each n, we have this diagram

$$\begin{tikzcd} & W_{n+1}(\mathcal{O}_K/\pi\mathcal{O}_K) \arrow[d, "\mathrm{pr}"] \\ W(\mathcal{O}_{K^\flat}) \arrow[ur, "p_{n+1}"] \arrow[dr, "p_n"'] & W_n(\mathcal{O}_K\pi\mathcal{O}_K) \arrow[d, "F"] \\ & W_n(\mathcal{O}_K/\pi\mathcal{O}_K) \end{tikzcd} \tag{3.5}$$

The diagram above is commutative since

$$p_n(\alpha^{(0)}, ..., \alpha^{(n-1)}) = (\alpha_n^{(0)}, ...\alpha_n^{(n-1)})$$

And

$$F \circ \mathrm{pr} \circ \theta_{n+1}(\alpha^{(0)}, ...\alpha^{(i)}, ...) = F \circ \mathrm{pr}(\alpha_{n+1}^{(0)}, ..., \alpha_{n+1}^{(n)}) = F(\alpha_{n+1}^{(0)}, ...\alpha_{n+1}^{(n-1)}) =$$

$$= ((\alpha_{n+1}^{(0)})^q, ..., (\alpha_{n+1}^{(n-1)})^q) = (\alpha_n^{(0)}, ...\alpha_n^{(n-1)})$$

Via 3.4 and 3.5, we obtain the following commutative digram

$$\begin{tikzcd} & W_{n+1}(\mathcal{O}_K/\pi\mathcal{O}_K) \arrow[d, "\mathrm{pr}"] \arrow[r, "\theta_{n+1}"] & \mathcal{O}_K\pi^{n+1}\mathcal{O}_K \arrow[dd, "\mathrm{pr}"] \\ W(\mathcal{O}_{K^\flat}) \arrow[ur, "p_{n+1}"] \arrow[dr, "p_n"'] & W_n(\mathcal{O}_K/\pi\mathcal{O}_K) \arrow[d, "F"] & \\ & W_n(\mathcal{O}_K/\pi\mathcal{O}_K) \arrow[r, "\theta_n"'] & \mathcal{O}_K/\pi^n\mathcal{O}_K \end{tikzcd}$$

And hence, we actually obtain a map of $\mathcal{O}$-algebra

$$\Theta_K : W(\mathcal{O}_{K^\flat}) \to \varprojlim \mathcal{O}_K/\pi^n\mathcal{O}_K = \mathcal{O}_K$$

such that $\Theta_K \mod \pi^n\mathcal{O}_K = \phi_n \circ p_n$. Now, because $K^\flat$ is a perfect extension field of k, and $W(\mathcal{O}_{K^\flat})$ is a subring of $W(K^\flat)$, we have for any $\alpha \in W(\mathcal{O}_{K^\flat})$, it can be uniquely represented as $\sum_{i\geq 0} \tau(\alpha^{(i)})\pi^i = (\alpha^{(0)}, ..., (\alpha^{(i)})^{q^i}, ...)$, where $\alpha^{(i)} \in \mathcal{O}_{K^\flat}$, and τ is the Teichmuler map. And for any integer n, we have

$$\Theta_K(\alpha^{(0)}, ..., (\alpha^{(i)})^{q^i}, ...) \mod \pi^n\mathcal{O}_K = \theta_n \circ p_n(\alpha^{(0)}, ..., (\alpha^{(i)})^{q^i}, ...) = \theta_n \circ W_n(\mathrm{pr}_n) \circ \mathrm{pr}(\alpha^{(0)}, ..., (\alpha^{(i)})^{q^i}, ...) =$$

$$= \theta_n \circ W_n(\mathrm{pr}_n)(\alpha^{(0)}, ..., (\alpha^{(n-1)})^{q^{n-1}}, ...) = \theta_n(\alpha_n^{(0)}, ..., (\alpha_n^{(n-1)})^{q^{n-1}}, ...) = (\alpha_n^{(0)})^{q^n} + ... + \pi^{n-1}((\alpha_n^{(n-1)})^{q^{n-1}})^q =$$

$$(\alpha^{(0)})^\sharp + \pi(\alpha^{(1)})^\sharp + ... + \pi^{n-1}(\alpha^{n-1})^\sharp \mod \pi^n\mathcal{O}_K$$

And hence, this yields Θ_K can be defined as

$$\Theta_K\Big(\sum_{i\geq 0} \tau(\alpha^{(i)})\pi^i\Big) = \sum_{i\geq 0} \pi^i(\alpha^{(i)})^\sharp$$

Proposition 3.3.1. *Let K be a perfectoid field, then the map*

$$\begin{aligned}\Theta_K : W(\mathcal{O}_{\mathbb{C}_p^\flat}) &\longrightarrow \mathcal{O}_K\\ \sum_{i\geq 0}\tau(\alpha_i)\pi^i &\longmapsto \sum_{i\geq 0}\alpha_i^\sharp\pi^i\end{aligned}$$

is a surjective $\mathcal{O}$-algebra.

Proof. It is sufficient to prove that Θ_K is surjective. Take any $a \in \mathcal{O}_K$, because K is perfectoid, we can find $\alpha_0 \in \mathcal{O}_{K^\flat}$, such that $\alpha_0 = (..., a \mod \pi\mathcal{O}_K)$, and hence, $\alpha_0^\sharp \equiv a \mod \pi\mathcal{O}_K$, and we can write $a - \alpha_0\sharp = \pi a_1$, for some $a_1 \in \mathcal{O}_K$. Again, we can write $a_1 - \alpha_1^\sharp = \pi a_2$. And inducetively, we get

$$a = \alpha_0^\sharp + \pi\alpha_1^\sharp + \pi^2 a_2 = \sum_{i\geq 0}\alpha_i^\sharp\pi^i$$

And we have

$$\Theta_K(\tau(\alpha_0) + \pi\tau(\alpha_1) + ...) = \sum_{i\geq 0}\alpha_i^\sharp\pi^i = a$$

Hence, Θ_K is surjective. □

We can characterize the kernel of Θ_K in a particular important case.

Proposition 3.3.2. *Let K be a perfectoid field, and Θ_K is defined as above. If there exists some $c \in \ker\Theta_K$, such that $c = (\gamma_0, \gamma_1, ...)$ and $|\gamma_0|_\flat = |\pi|$, then $\ker\Theta_K = cW(\mathcal{O}_{K^\flat})$.*

Proof. First, we will prove that $\ker\Theta_K \subset cW(\mathcal{O}_{K^\flat}) + \pi W(\mathcal{O}_{K^\flat})$. Take any $a = \sum_{i\geq 0}\tau(\alpha_i)\pi^i \in \ker\Theta_K$, we have

$$0 = \Theta_K\Big(\sum_{i\geq 0}\tau(\alpha_i)\pi^i\Big) = \sum_{i\geq 0}\alpha_i^\sharp\pi^i$$

It then follows that $|\alpha_0^\sharp| \leq |\pi|$, i.e. $|\alpha_0|_\flat \leq |\pi| = |\gamma_0|_\flat$. So, there exists $b \in \mathcal{O}_{K^\flat}$ such that $\alpha_0 = \gamma_0 b$, then

$$a - \tau(b)c = (0, ...) \in \pi W(\mathcal{O}_{K^\flat})$$

And hence, $\ker\Theta_K \subseteq cW(\mathcal{O}_{K^\flat}) + \pi W(\mathcal{O}_{K^\flat})$. Take any $\alpha \in \ker\Theta_K$, we can represent $a = cb_0 + \pi a_1$, and this yields $\pi a_1 \in \ker\Theta_K$, and $\Theta_K(\pi a_1) = \pi\Theta_K(a_1) = 0$. That means $a_1 \in \ker\Theta_K$, and inductively, $a_1 = cb_1 + \pi a_2$, ..., and we get

$$a = cb_0 + \pi a_1 = cb_0 + \pi cb_1 + \pi^2 a_2 = c(b_0 + \pi b_1 + ...)$$

Because $W(\mathcal{O}_{K^\flat})$ is complete w.r.t the π-adic topology, we get $\ker\Theta_K \subseteq cW(\mathcal{O}_{K^\flat})$. Therefore, $\ker\Theta_K = cW(\mathcal{O}_{K^\flat})$. □

Important Convention. From now on, we will assume that there exists $c = (\gamma_0, \gamma_1, ...) \in \ker\Theta_{\widehat{L_\infty}}$, and $|\gamma_0|_\flat = |\pi|$. The existence of c will be proved later in the chapter about (ϕ_L, Γ_L)-module. And this yields by the previous lemma that for all perfectoid field K, $\ker\Theta_K$ is generated by c.

By the commutative diagram for all perfectoid field K

$$\begin{tikzcd} W(\mathcal{O}_{K^\flat}) \arrow[r, "\Theta_K"] \arrow[d, "\subseteq"'] & \mathcal{O}_K \\ W(\mathcal{O}_{\widehat{L_\infty}^\flat}) \arrow[r, "\Theta_{\widehat{L_\infty}}"'] & \mathcal{O}_{\widehat{L_\infty}} \arrow[u, "\subseteq"'] \end{tikzcd}$$

We have $\ker \Theta_K = cW(\mathcal{O}_{K^\flat})$. We also obtain the map

$$\begin{aligned}\widetilde{\Theta_K} : W(\mathcal{O}_{K^\flat}) \otimes_{W_{\mathcal{O}_{\widehat{L_\infty}^\flat}}} \mathcal{O}_{\widehat{L_\infty}} &\longrightarrow \mathcal{O}_{K^\flat}\\ a \otimes b &\longmapsto \Theta_K(a)b\end{aligned}$$

Lemma 3.3.3. *The map $\widetilde{\Theta_K}$ defined above is an isomorphism.*

Proof. We have

$$W(\mathcal{O}_{K^\flat}) \otimes_{W_{\mathcal{O}_{\widehat{L_\infty}^\flat}}} \mathcal{O}_{\widehat{L_\infty}} \cong W(\mathcal{O}_{K^\flat}) \otimes_{W_{\mathcal{O}_{\widehat{L_\infty}^\flat}}} \mathcal{O}_{\widehat{L_\infty}}/cW(\mathcal{O}_{\widehat{L_\infty}^\flat}) = W(\mathcal{O}_{K^\flat})/cW(\mathcal{O}_{K^\flat}) \cong \mathcal{O}_K$$

□

And now, due to these isomorphisms, we can construct the un-tilt of a given complete, perfect field $\widehat{L_\infty}^\flat \subseteq F \subseteq \mathbb{C}_p^\flat$. We will first construct its ring of integers. It can be seen that the following commutative diagram is commutative

$$\begin{tikzcd} W(\mathcal{O}_{\mathbb{C}_p^\flat})/cW(\mathcal{O}_{\mathbb{C}_p^\flat}) \arrow[r, "\Theta_{\mathbb{C}_p}"] & \mathcal{O}_{\mathbb{C}_p} \\ W(\mathcal{O}_F)/cW(\mathcal{O}_F) \arrow[u, "\subseteq"] & \\ W(\mathcal{O}_{\widehat{L_\infty}^\flat})/cW(\mathcal{O}_{\widehat{L_\infty}^\flat}) \arrow[u, "\subseteq"] \arrow[r, "\Theta_{\widehat{L_\infty}}"'] & \mathcal{O}_{\widehat{L_\infty}} \arrow[uu, "\subseteq"'] \end{tikzcd} \tag{3.6}$$

Let us define

$$\begin{cases}\mathcal{O}_F^\sharp := \Theta_{\mathbb{C}_p}(W(\mathcal{O}_F)/cW(\mathcal{O}_F)) = \widetilde{\Theta_{\mathbb{C}_p}}(W(\mathcal{O}_F) \otimes_{W(\mathcal{O}_{\widehat{L_\infty}^\flat})} \mathcal{O}_{\widehat{L_\infty}}) \\ F^\sharp := \Theta_{\mathbb{C}_p}(W(\mathcal{O}_F) \otimes_{W(\mathcal{O}_{\widehat{L_\infty}^\flat})} \widehat{L_\infty}) = \mathcal{O}_F^\sharp \otimes_{\mathcal{O}_{\widehat{L_\infty}}} \widehat{L_\infty} = \widetilde{\Theta_{\mathbb{C}_p}}(W(\mathcal{O}_F) \otimes_{W(\mathcal{O}_{\widehat{L_\infty}^\flat})} \widehat{L_\infty})\end{cases} \tag{3.7}$$

Note that if we extend $\widetilde{\Theta_K}$ in Lemma 3.3.3 then $W(\mathcal{O}_{K^\flat}) \otimes_{W_{\mathcal{O}_{\widehat{L_\infty}^\flat}}} \widehat{L_\infty} \cong K$. And this yields

Corollary 3.3.4. $(K^\flat)^\sharp = K$.

Our goal is to prove that $F^\sharp$ is a perfectoid field, with $\mathcal{O}_{F^\sharp} = \mathcal{O}_F^\sharp$ and $(F^\sharp)^\flat = F$. Note that the diagram 3.6 comes from the diagram

$$\begin{tikzcd} W(\mathcal{O}_{\mathbb{C}_p^\flat}) \arrow[r, "\Theta_{\mathbb{C}_p}"] & \mathcal{O}_{\mathbb{C}_p} \\ W(\mathcal{O}_F) \arrow[u, "\subseteq"] & \\ W(\mathcal{O}_{\widehat{L_\infty}^\flat}) \arrow[u, "\subseteq"] \arrow[r, "\Theta_{\widehat{L_\infty}}"'] & \mathcal{O}_{\widehat{L_\infty}} \arrow[uu, "\subseteq"'] \end{tikzcd} \tag{3.8}$$

Lemma 3.3.5. *$\mathcal{O}_F^\sharp$ is π-adically complete.*

Proof. We can se immediately that the following short exact sequence

$$0 \to W(\mathcal{O}_F) \xrightarrow{.c} W(\mathcal{O}_F) \to W(\mathcal{O}_F)/cW(\mathcal{O}_F) \to 0$$

yields the short exact sequence

$$0 \to W(\mathcal{O}_F)/\pi^m W(\mathcal{O}_F) \xrightarrow{.c} W(\mathcal{O}_F)/\pi^m W(\mathcal{O}_F) \to W_c/\pi^m W_c \to 0$$

where $W_c := W(\mathcal{O}_F)/cW(\mathcal{O}_F)$, and it is compatible with the inverse system

$$\begin{tikzcd}
0 \arrow[r] & \varprojlim W(\mathcal{O}_F)/\pi^m W(\mathcal{O}_F) \arrow[r, ".c"] & \varprojlim W(\mathcal{O}_F)/\pi^m W(\mathcal{O}_F) \arrow[r] & \varprojlim W_c/\pi^m W_c \arrow[r] & 0 \\
0 \arrow[r] & W(\mathcal{O}_F) \arrow[r, ".c"] \arrow[u] & W(\mathcal{O}_F) \arrow[r] \arrow[u] & W_c \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

where the two first vertical arrows are isomorphisms. This yields $W_c \cong \varprojlim W_c/\pi^m W_c$, and this yields $\mathcal{O}_F^\sharp$ is π-adically complete. □

Lemma 3.3.6. *Let $x \in \mathcal{O}_F^\sharp$, then $|x| \leq |\pi|$ iff $x \in \pi\mathcal{O}_F^\sharp$.*

Proof. One can see that $\Theta_{\mathbb{C}_p}(W_c) \subseteq \mathcal{O}_{\mathbb{C}_p} = \{y \in \mathcal{O}_{\mathbb{C}_p}, |y| \leq 1\}$. So in particular, $\forall x \in \mathcal{O}_F^\sharp, |x| \leq 1$, and if $x \in \pi\mathcal{O}_F^\sharp$, we obviously have $|x| \leq |\pi|$.

Conversely, assume that $|x| \leq |\pi|$. Because $x \in \mathcal{O}_F^\sharp$, we can find $a = \sum_{i\geq 0} \tau(\alpha_i)\pi^i \in W(\mathcal{O}_F)$, such that

$$\Theta_{\mathbb{C}_p}\Big(\sum_{i\geq 0} \tau(\alpha_i)\pi^i\Big) = \sum_{i\geq 0} \alpha_i^\sharp \tau^i = x$$

And it follows that $|\alpha_0^\sharp| \leq |\pi| = |\gamma_0|_\flat$. So, there exists some $\beta \in \mathcal{O}_F$ such that $\alpha_0 = \beta\gamma_0$, and we have $a - c\tau(\beta) \in \pi W(\mathcal{O}_F)$. Also, because $\Theta_{\mathbb{C}_p}$ is a ring homomorphism and $c \in \ker \Theta_{\mathbb{C}_p}$, we get

$$\Theta_{\mathbb{C}_p}(a - c\tau(\beta)) = \Theta_{\mathbb{C}_p}(a) - \Theta_{\mathbb{C}_p}(c\tau(\beta)) = \Theta_{\mathbb{C}_p}(a) \in \Theta_{\mathbb{C}_p}(\pi W(\mathcal{O}_F)) = \pi\Theta_{\mathbb{C}_p}(W(\mathcal{O}_F)) = \pi\mathcal{O}_F^\sharp$$

□

By Lemma 3.3.5 and Lemma 3.3.6, we can see that any Cauchy sequence in $\mathcal{O}_F^\sharp$ converges. In fact, let $(x_n)_n$ be a Cauchy sequence in $\mathcal{O}_F^\sharp$, then for all $\epsilon > 0$, there exists some N_ϵ, such that for all $m, n \geq N_\epsilon$, we have $|x_m - x_n| < \epsilon$. We can find some integer l such that $\epsilon \leq |\pi|^l$, and this yields by Lemma 3.3.6 that $x_m - x_n \in \pi^l\mathcal{O}_F^\sharp$. Due to Lemma 3.3.5, $\mathcal{O}_F^\sharp$ is π-adically complete, so we can find some $x_0 \in \mathcal{O}_F^\sharp$ such that $\forall m$, there exists n_m such that for all $n \geq n_m$, $x_n - x_0 \in \pi^m\mathcal{O}_F^\sharp$, i.e. $|x_n - x_0| \leq |\pi|^m$. So x_0 is the limit of $(x_n)_n$ w.r.t the usual metric on $\mathbb{C}_p$.

Corollary 3.3.7. *$\mathcal{O}_F^\sharp$ is a complete metric space.*

We can a further step to prove that $F^\sharp$ is complete. We first have that

Lemma 3.3.8. $\mathcal{O}_F^\sharp = \{x \in F^\sharp, |x| \leq 1\}$.

Proof. Note that $\mathcal{O}_F^\sharp \subseteq F^\sharp$ by 3.7, and so it is obvious that $\mathcal{O}_F^\sharp \subset \{x \in F^\sharp, |x| \leq 1\}$. Conversely, take any $x \in F^\sharp$, such that $|x| \leq 1$. Because $\mathcal{O}_{\widehat{L_\infty}} \subset \mathcal{O}_F^\sharp$, and $F^\sharp = \mathcal{O}_F^\sharp \otimes_{\mathcal{O}_{\widehat{L_\infty}}} \widehat{L_\infty}$, we can find $y' \in \mathcal{O}_F^\sharp$, $z' \in \mathcal{O}_{\widehat{L_\infty}}$, and an integer $m \geq 0$, such that $x = y'\pi^{-m}z' = y/\pi^m$, where $y = y'z'$. And this yields $|y| \leq |\pi^m|$. Applying Lemma 3.3.6, we get $y \in \pi^m\mathcal{O}_F^\sharp$, and hence $x \in \mathcal{O}_F^\sharp$. □

We are now ready to prove

Corollary 3.3.9. *$F^\sharp$ is complete.*

Proof. Let us take a Cauchy sequence $(x_n)_n$ in $F^\sharp$. We can fix any integer $l \geq 0$ and n_l such that for all $n, m \geq n_l$, we have $|x_n - x_m| \leq |\pi^l|$, i.e. $x_n - x_m \in \pi^l \mathcal{O}_F^\sharp$. That means, there exists some integer k such that $(\pi^k x_n)_n$ is a Cauchy sequence in $\mathcal{O}_F^\sharp$ by Lemma 3.3.8. Due to Corollary 3.3.7, $(\pi^k x_n)_n$ converges to some $x_0 \in \mathcal{O}_F^\sharp$, and hence $(x_n)_n$ converges to $x_0/\pi^k \in F^\sharp$. □

Next, we will prove $F^\sharp$ is a perfectoid field by using

Lemma 3.3.10.

(i) The image of $\mathcal{O}_F$ under the map $\mathcal{O}_{\mathbb{C}_p^\flat} \xrightarrow{(.)^\sharp} \mathbb{C}_p^\flat$ is contained in $\mathcal{O}_F^\sharp$.

(ii) The composition $\mathcal{O}_F \xrightarrow{(.)^\sharp} \mathcal{O}_F^\sharp \xrightarrow{pr} \mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp$ is surjective.

(iii) $(\mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp)^q = (\mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp)$.

(iv) For any $\alpha \neq 0$ in $\mathcal{O}_F$, $\alpha^\sharp$ is a multiplicative unit in $F^\sharp$.

Proof.

(i) Let $\alpha \in \mathcal{O}_F$, we have $\tau(\alpha) \in W(\mathcal{O}_F)$ and $\Theta_{\mathbb{C}_p}(\tau(\alpha)) = \alpha^\sharp \in \mathcal{O}_F^\sharp$.

(ii) Because $\mathcal{O}_F^\sharp \cong W_c := W(\mathcal{O}_F)/cW(\mathcal{O}_F)$, we have

$$\mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp \cong W_c/\pi W_c = W(\mathcal{O}_F)/(cW(\mathcal{O}_F) + \pi W(\mathcal{O}_F))$$

Consider the composition of maps

$$W(\mathcal{O}_F) \xrightarrow{\Phi_0} \mathcal{O}_F \xrightarrow{\text{pr}} {}_F/\gamma_0\mathcal{O}_F$$

Its kernel is $\{(\gamma_0\alpha_0, \alpha_1, ...) \in W(\mathcal{O}_F)\}$, and we have $(\gamma_0\alpha_0, \alpha_1, ...) - c(\alpha_0, ...) = (0, ...) \in \pi W(\mathcal{O}_F)$ So, the kernel of the surjective map above is $cW(\mathcal{O}_F) + \pi W(\mathcal{O}_F)$, and we get

$$W(\mathcal{O}_F)/(cW(\mathcal{O}_F) + \pi W(\mathcal{O}_F)) \cong \mathcal{O}_F/\gamma_0\mathcal{O}_F$$

And we obtain the following commutative diagram with the first row arrows are isomorphisms

$$\begin{tikzcd}
\mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp & W_c/\pi W_c \arrow[l, "\Theta_{\mathbb{C}_p}"'] \arrow[r, "\Phi_0"] & \mathcal{O}_F/\gamma_0\mathcal{O}_F \\
\mathcal{O}_F^\sharp \arrow[u, "\text{pr}"] & W(\mathcal{O}_F) \arrow[l, "\Theta_{\mathbb{C}_p}"'] \arrow[r, "\Phi_0"] \arrow[u, "\text{pr}"] & \mathcal{O}_F \arrow[u, "\text{pr}"] \\
& \mathcal{O}_F \arrow[ul, "(.)^\sharp"] \arrow[u, "\tau"] \arrow[ur, "id_{\mathcal{O}_F}"'] &
\end{tikzcd} \tag{3.9}$$

And this diagram yields the composition $\mathcal{O}_F \xrightarrow{(.)^\sharp} \mathcal{O}_F^\sharp \to \mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp$ is surjective.

(iii) We have $\mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp = \mathcal{O}_F/\gamma_0\mathcal{O}_F$, because $\mathcal{O}_F$ is perfect, we get $(\mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp)^q = \mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp$.

(iv) For any $\alpha \neq 0$ in $\mathcal{O}_F$, we can choose $\gamma \in \mathcal{O}_{\widehat{L_\infty}}$, such that $\gamma \neq 0$, and $|\alpha| \geq |\gamma|$, since the valuation group of $\mathcal{O}_{\widehat{L_\infty}}$ is dense in $\mathbb{R}_{\geq 0}$. And this yields there exists some $\beta \in \mathcal{O}_F$, such that $\alpha\beta = \gamma$. By multiplicative property of $(.)^\sharp$, we have $(\alpha\beta)^\sharp = \alpha^\sharp\beta^\sharp = \gamma^\sharp \in \widehat{L_\infty}^\flat$, and $\gamma^\sharp \neq 0$, since $|\gamma^\sharp| = |\gamma|_\flat \neq 0$. And hence, $\alpha^\sharp\beta^\sharp = \gamma^\sharp \in (\widehat{L_\infty}^\flat)^\times \subset (F^\sharp)^\times$.

□

As a corollary, we get

Corollary 3.3.11. *$F^\sharp$ is a perfectoid field with $\mathcal{O}_{F^\sharp} = \mathcal{O}_F^\sharp$.*

Proof. We will prove first that $F^\sharp$ is a field. Because $F^\sharp = \mathcal{O}_F^\sharp \otimes_{\mathcal{O}_{\widehat{L_\infty}}} \widehat{L_\infty}$, we have $1/\pi \in F^\sharp$. Also, we know from Lemma 3.3.8 that $\mathcal{O}_F^\sharp = \{x \in F^\sharp, |x| \leq 1\}$, and hence, it is sufficient to prove that any element in $\mathcal{O}_F^\sharp \setminus \pi\mathcal{O}_F^\sharp$ is invertible in $F^\sharp$. Take any $x \in \mathcal{O}_F^\sharp \setminus \pi\mathcal{O}_F^\sharp$, i.e. $|\pi| < |x| < 1$. Due to Lemma 3.3.10 (ii), we can find $y \in \mathcal{O}_F$ such that $x - y^\sharp \in \pi\mathcal{O}_F^\sharp$, i.e. $|x - y^\sharp| \leq |\pi|$. And this yields $|x| = |y^\sharp|$. And due to Lemma 3.3.10 (iv), we have $1/y^\sharp \in (F^\sharp)^\times$, and hence, $|x/y^\sharp| = 1$. This yields $x/y^\sharp \in \mathcal{O}_F^\sharp$, by Lemma 3.3.8. Also, since

$$|1 - \frac{x}{y^\sharp}||y^\sharp| = |x - y^\sharp| \leq |\pi|$$

And $|y^\sharp| = |x| > |\pi|$, we get $|1 - \frac{x}{y^\sharp}| < 1$, and $1 - \frac{x}{y^\sharp} \in \mathcal{O}_F^\sharp$. And this follows that $X := \sum_{n\geq 0}(1 - \frac{x}{y^\sharp})^n$ converges in $\mathcal{O}_F^\sharp$, because it is complete. And

$$\Big(\sum_{n\geq 0}(1 - \frac{x}{y^\sharp})\Big)\Big(1 - (1 - \frac{x}{y^\sharp})\Big) = 1$$

and it yields X is the inverse of $x/y^\sharp$. From this, we obtain $F^\sharp$ is a complete field. By Lemma 3.3.8, we have $\mathcal{O}_{F^\sharp}\mathcal{O}_F^\sharp$. And because $F^\sharp$ contains L_∞, the value group of $(F^\sharp)^\times$ is dense in $\mathbb{R}_{>0}$. And Lemma 3.3.10 (iii) implies that $F^\sharp$ is perfectoid. $\square$

For the last step, we will prove that $(F^\sharp)^\flat = F$. We begin with

Lemma 3.3.12. *Let F be a complete non-archimedean field of characteristic p w.r.t the norm $|.|$, then for any $\gamma \in \mathcal{O}_F$ with $|\gamma| < 1$, the map*

$$\begin{aligned} \varprojlim_{(.)^q} \mathcal{O}_F &\longrightarrow \varprojlim_{(.)^q} \mathcal{O}_F/\gamma\mathcal{O}_F \\ (\ldots, \alpha_i, \ldots, \alpha_1, \alpha_0) &\longmapsto (\ldots, \alpha_i \mod \gamma\mathcal{O}_F, \ldots, \alpha_0 \mod \gamma\mathcal{O}_F) \end{aligned}$$

is an isomorphism of rings.

Proof. Assume that there exists $(\ldots, \alpha_i, \ldots, \alpha_1, \alpha_0) \in \varprojlim_{(.)^q} \mathcal{O}_F$, such that $(\ldots, \alpha_i \mod \gamma\mathcal{O}_F, \ldots, \alpha_0 \mod \gamma\mathcal{O}_F) = 0$. That means, $\alpha_i \in \gamma\mathcal{O}_F$ for all i. This yields $|\alpha_0| \leq |\gamma|^{q^i}$. Hence, $\alpha = 0$. From this, $\alpha_i = 0$, for all i, and we obtain the map above is injective.

Now, let $(\ldots, \alpha_i \mod \gamma\mathcal{O}_F, \ldots, \alpha_0 \mod \gamma\mathcal{O}_F) \in \varprojlim_{(.)^q} \mathcal{O}_F/\pi\mathcal{O}_F$, we have $\alpha_{i+1}^q \equiv \alpha_i \mod \gamma\mathcal{O}_F$. Let us consider for any fixed i a sequence $(\alpha_{i+j}^{q^j})_j$, which is Cauchy in $\mathcal{O}_F$, and hence, converges to some $a_i \in \mathcal{O}_F$. We can see that $a_i \equiv \alpha_i \mod \gamma\mathcal{O}_F$, and that $a_{i+1}^q = \lim_{j\to\infty} \alpha_{i+1+j}^{q^{j+1}} = \lim_{k\to\infty} \alpha_{i+k}^{q^k} = a_i$, when we change $1 + j \leftrightarrow k$. Therefore, $(\ldots, a_i, \ldots, a_1, a_0)$ defines an element in $\varprojlim_{(.)^q} \mathcal{O}_F$ that maps to $(\ldots, \alpha_i \mod \gamma\mathcal{O}_F, \ldots, \alpha_0 \mod \gamma\mathcal{O}_F)$. Hence, the map above is also surjective. $\square$

We are now ready to prove

Proposition 3.3.13. $(F^\sharp)^\flat = F$.

Proof. We will first prove that $\mathcal{O}_F \subseteq \mathcal{O}_{(F^\sharp)^\flat}$. Take any $\alpha \in \mathcal{O}_F \subset \mathcal{O}_{\mathbb{C}_p^\flat}$, we can represent

$$\alpha = (\ldots, a_i \mod \pi\mathcal{O}_{\mathbb{C}_p}, \ldots, a_0 \mod \pi\mathcal{O}_{\mathbb{C}_p}) = (\ldots, (\alpha^{1/q^i})^\sharp \mod \pi\mathcal{O}_{\mathbb{C}_p}, \ldots, \alpha^\sharp \mod \pi\mathcal{O}_{\mathbb{C}_p}) \in \varprojlim_{(.)^q} \mathcal{O}_{\mathbb{C}_p}/\pi\mathcal{O}_{\mathbb{C}_p}$$

Due to Lemma 3.3.10, the later element is $(..., (\alpha^{1/q^i})^\sharp \mod \pi\mathcal{O}_F^\sharp, ..., \alpha^\sharp \mod \pi\mathcal{O}_F^\sharp) \in \varprojlim_{(.)^q} \mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp = \mathcal{O}_{(F^\sharp)^\flat}$.

The converse is a bit more difficult. Take any $\alpha \in \mathcal{O}_{(F^\sharp)^\flat} = \varprojlim_{(.)^q} \mathcal{O}_F^\sharp/\pi\mathcal{O}_F^\sharp$, we can represent

$$\alpha = (..., b_i \mod \pi\mathcal{O}_F^\sharp, ..., b_0 \mod \pi\mathcal{O}_F^\sharp)$$

And by Lemma 3.3.10 (ii), there exists, for all i, $\beta_i \in \mathcal{O}_F$, such that $\beta_i^\sharp \equiv b_i \mod \pi\mathcal{O}_F^\sharp$, and we obtain $(\beta_{i+1}^\sharp)^q \equiv \beta_i^\sharp \mod \pi\mathcal{O}_F^\sharp$. Via the top row isomorphism in 3.9, there exists some $\xi \in \mathcal{O}_F$, such that ξ_i is mapped to β_i via the top row of 3.9, and from this, $\xi_{i+1}^q = \xi_i \mod \gamma_0\mathcal{O}_F$. That means, $\xi_i^\sharp \equiv b_i \mod \pi\mathcal{O}_F^\sharp$. And this yields $\alpha = (..., \xi_i^\sharp \mod \pi\mathcal{O}_F^\sharp, ..., \xi_0^\sharp \mod \pi\mathcal{O}_F^\sharp)$, with $\xi_i \in \mathcal{O}_F$, and $\xi_{i+1}^q \equiv \xi_i \mod \gamma_0\mathcal{O}_F$. So, $(\ldots, \xi_i, \ldots, \xi_1, \xi_0)$ defines an element in $\varprojlim_{(.)^q} \mathcal{O}_F/\gamma_0\mathcal{O}_F$. By using the isomorphism in Lemma 3.3.12, we obtain there exists some $\alpha_i \in \mathcal{O}_F$ such that $\alpha_{i+1}^q = \alpha_i$, and $\alpha_i \equiv \xi_i \mod \gamma_0\mathcal{O}_F^\sharp$. Via the isomorphism in 3.9 again, we get $\alpha_i^\sharp \equiv b_i \mod \pi\mathcal{O}_F^\sharp$ and this also yields $\alpha = (..., \alpha_i \mod \pi\mathcal{O}_F^\sharp, ..., \alpha_0 \mod \pi\mathcal{O}_F^\sharp)$, and $\alpha_i \in \mathcal{O}_F$, with $\alpha_{i+1}^q = \alpha_i$.

Because $\mathcal{O}_F \subseteq \mathcal{O}_{\mathbb{C}_p}$, we can represent

$$\alpha_j = (..., a_{j,i} \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., a_{j,0} \mod \pi\mathcal{O}_{\mathbb{C}_p})$$

And $a_{j,i+1}^q \equiv a_{j,i} \equiv a_{j+1,i}^q \mod \pi\mathcal{O}_{\mathbb{C}_p}$, and then

$$\alpha = (..., \lim_{i\to\infty} a_{j,i}^{q^i}, ..., \lim_{i\to\infty} a_{0,i}^{q^i} \mod \pi\mathcal{O}_{\mathbb{C}_p}) =$$

$$= (..., a_{j,0} \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., a_{0,0} \mod \pi\mathcal{O}_{\mathbb{C}_p}) = \alpha_0 \in \mathcal{O}_F$$

So, we have $\mathcal{O}_{(F^\sharp)^\flat} \subseteq \mathcal{O}_F$. And we obtain $\mathcal{O}_F = \mathcal{O}_{(F^\sharp)^\flat}$. It follows that $(F^\sharp)^\flat = F$. □

For now, we can deduce the first tilting correspondence

Theorem 3.3.14. *There exists a bijection between the two sets*

$$\{\widehat{L_\infty} \subseteq K \subseteq \mathbb{C}_p, K: \textit{ perfectoid}\} \leftrightarrow \{\widehat{L_\infty}^\flat \subseteq F \subseteq \mathbb{C}_p^\flat, F: \textit{ complete, perfect}\}$$

.

defined by $K \mapsto K^\flat$ and the inverse $F \mapsto F^\sharp$.

Proof. By what we have discussed so far, the two maps between the two sets above are well-defined . And by Proposition 3.3.13, we know that $(F^\sharp)^\flat = F$. Also, if we have K is a perfectoid field, $(K^\flat)^\sharp = K$ follows from Corollary 3.3.4. □

We conclude this section by a following useful observation.

Proposition 3.3.15. *Let $\widehat{L_\infty}^\flat \subseteq F \subseteq \mathbb{C}_p^\flat$ be an immediate, complete, perfect field. If F is algebraically closed, then $F^\sharp$ is algebraically closed, and hence, $F = \mathbb{C}_p^\flat$.*

Proof. See [Sch17](Remark 1.4.25). □

3.4 Applications to field of norms

We recall that $k((x)) \hookrightarrow \widehat{L_\infty}^\flat$ by sending x to $\omega = (, ..., z_i \mod \pi\mathcal{O}_{\widehat{L_\infty}}, ..., z_1 \mod \pi\mathcal{O}_{\widehat{L_\infty}}, 0)$, with z_n is a generator of $\mathscr{F}_n$. The image is denoted E_L, the field of norm. In this section, we will give some relations between E_L, and $\widehat{L_\infty}^\flat$ and $\mathbb{C}_p^\flat$. These results will be used again in next section about the second and the third tilting correspondence. We first recall something about perfect hulls.

Remark 3.4.1. Let E be a field of char. $p>0$, $\overline{E}$ its algebraic closure. The perfect hull of E is defined as

$$E^{\text{perf}} := \{a \in \overline{E}, a^{p^m} \in E, \text{ for some } m \geq 0\}$$

then

(i) E^{perf} is the largest immediate field between $\overline{E}$ and E that is purely inseparable.

(ii) E^{perf} is a smallest immediate field between $\overline{E}$ and E that is pefect, and hence $\overline{E}/E^{\text{perf}}$ is Galois.

(iii) $E^{\text{perf}} \cap E^{\text{sep}} = E$, and $\overline{E} = E^{\text{perf}}E^{\text{sep}}$, and $\text{Gal}(\overline{E}/E^{\text{perf}}) \cong \text{Gal}(E^{\text{sep}}/E)$.

Using this remark, we obtain

Proposition 3.4.2. $\widehat{E_L^{perf}} = \widehat{L_\infty}^\flat$.

Proof. We can see easily that $\widehat{E_L^{\text{perf}}} \subseteq \widehat{L_\infty}$, since $\overline{E} \subset \overline{\mathbb{C}_p^\flat} = \mathbb{C}_p^\flat$, $E_L \subset \widehat{L_\infty}$, and $\widehat{L_\infty}$ is also perfect and complete. For the reverse direction, it is enough to prove that $\mathcal{O}_{\widehat{L_\infty}^\flat} \subset \widehat{E_L^{\text{perf}}}$. Take any $\alpha = (..., a_i' \mod \pi\mathcal{O}_{\widehat{L_\infty}}, ..., a_0' \mod \pi\mathcal{O}_{\widehat{L_\infty}}) \in \varprojlim_{(.)^q} \mathcal{O}_{\widehat{L_\infty}}/\pi\mathcal{O}_{\widehat{L_\infty}}$. Because $\mathcal{O}_{\widehat{L_\infty}}/\pi\mathcal{O}_{\widehat{L_\infty}} \cong \mathcal{O}_{L_\infty}/\pi\mathcal{O}_{L_\infty}$, we can find $(a_i)_i \in \mathcal{O}_{L_\infty}$, such that

$$\alpha = (..., a_i \mod \pi\mathcal{O}_{L_\infty}, ..., a_0 \mod \pi\mathcal{O}_{L_\infty})$$

And for any n, there exists some $l>n$, such that $a_n \in \mathcal{O}_{L_l}$, and we can represent

$$a_n = \sum_{j=0}^{(q-1)q^{l-1}} \beta_j z_l^j$$

where $\beta_j \in k$. And we have

$$\beta := \sum_j \beta_j \omega^{j/q^{l-n}} = \sum_j \beta_j(..., z_l^j \mod \pi\mathcal{O}_{L_\infty}, ..., z_{l-n}^j \mod \pi\mathcal{O}_{\widehat{L_\infty}}) =$$

$$= (..., \sum_j \beta_j z_l^j \mod \pi\mathcal{O}_{L_\infty}, ..., \sum_j \beta_j z_{l-n}^j \mod \pi\mathcal{O}_{L_\infty})$$

And we have $a_n - \sum_j \beta_j z_l^j \equiv 0 \mod \pi\mathcal{O}_{L_\infty}$, and

$$a_{n-1} \equiv a_n^q \equiv (\sum_j \beta_j z_l^j)^q \equiv \sum_j \beta_j z_{l-1}^j \mod \pi\mathcal{O}_{L_\infty}$$

And inductively, we get the same equality for $a_{n-2}, ...$ Hence, we get $\alpha - \beta \in U_m$, that means $|\alpha-\beta|_\flat \leq |\omega|_\flat^{q^n}$. Because n is chosen arbitrarily, and $\beta \in E_L^{\text{perf}}$, we get $\alpha \in \widehat{E_L^{\text{perf}}}$, and hence $\widehat{E_L^{\text{perf}}} = \widehat{L_\infty}^\flat$. ☐

We also recall about Krasner's lemma and its corollary.

Remark 3.4.3. Let E be a complete, non-archimedean field, and E^{sep} its algebraic closure. Let $\alpha, \beta \in E^{\text{sep}}$ such that $|\beta - \alpha| < |\alpha' - \alpha|$, for any Galois conjugate α' of α, then $E(\alpha) \subseteq E(\beta)$.

Remark 3.4.4. Let E, E^{sep} be defined as above. For any $f(X) = a_0 + ... + a_nX^n \in E[X]$, we define $||f|| := \max_{0\leq i\leq n}|a_i|$. Assume further that $f(X)$ is monic, irreducible, separable with distinct roots $\alpha_1, ..., \alpha_n$ in E^{sep}, then for any $g(X)$: monic, separable of degree n in $E[X]$, if $||f-g||$ is small enough, then $g(X)$ is also irreducible, and we can number roots $\beta_1, ..., \beta_n$ of g in such a way that $E(\alpha_i) = E(\beta_i)$.

Using this remark, we can prove easily that

Corollary 3.4.5. *$\widehat{\overline{E_L}}$ is separably closed.*

Proof. Take any α: algebraic, separable over $\widehat{\overline{E_L}}$, with its minimal $f(X)$, which is monic, irreducible, separable in $\widehat{\overline{E_L}}$. Because $\overline{E_L}$ is dense in $\widehat{\overline{E_L}}$, we can find $g(X)$: monic, separable of degree equal to $\deg f$ in $\overline{E_L}[X]$, such that $||f-g||$ is arbitrarily small, then $g(X)$ is irreducible over $\overline{E_L}[X]$, but we then have $\deg g = 1 = \deg f$. So $\widehat{\overline{E_L}}$ is separably closed. □

We need the following lemma to deduce the main result of this section.

Lemma 3.4.6. *Let E be a field of char. $p > 0$, and E is separably closed, non-archimedean then E is dense in $\overline{E}$.*

Proof. Because E is separably closed, $\overline{E}/E$ is purely inseparable. Take any $\alpha \in \overline{E}$, then the minimal polynomial of α over E is of the form $X^{p^m} - a$, for some $a \in E$. If $m = 0$, then it is clear that $\alpha \in E$, so we may assume that $m \geq 1$. Note that for any $\epsilon > 0$, there exists $a_1 \in E$ such that $0 < |a_1| < \epsilon$. Consider the following polynomial

$$f(X) := X^{p^m} + a_1 X - a \text{ where } a_1 \in E \text{ and } 0 < |a_1| < \frac{\epsilon^{p^m}}{|\alpha|}$$

for some $\epsilon > 0$. Then $f(X)$ is clear separable over E, and we can write $f(X) = \prod_{i=1}^{p^m}(X - \beta_i)$, and hence $f(\alpha) = \prod_{i=1}^{p^m}(\alpha - \beta_i) = a_1\alpha$. Therefore, there exists some i, such that

$$|\alpha - \beta_i| \leq (a_1\alpha)^{1/p^m} < \epsilon$$

Because E is separably closed, all β_i are in E, and hence, E is dense in $\overline{E}$. □

Corollary 3.4.7. $\widehat{E_L^{sep}} = \mathbb{C}_p^\flat$

Proof. We first have by Lemma 3.4.6 and Proposition 3.4.2 that $\widehat{E_L^{\mathrm{sep}}} = \widehat{\overline{E_L}} \supset \widehat{E_L^{\mathrm{perf}}} = \widehat{L_\infty}$, so it is clear that $\widehat{E_L^{\mathrm{sep}}}$ is a complete subfield of $\mathbb{C}_p^\flat$ containing $\widehat{L_\infty}^\flat$. On the other hand, the automorphism

$$\begin{aligned} \overline{E_L} &\longrightarrow \overline{E_L} \\ \alpha &\longmapsto \alpha^{1/p} \end{aligned}$$

is continuous, since $|\alpha|_\flat^{1/p} = |\alpha^{1/p}|_\flat$, so it can be extended to an automorphism $\widehat{\overline{E_L}} \to \widehat{\overline{E_L}}$. And this yields $\widehat{\overline{E_L}}$ is a perfect, complete, immediate field between $\widehat{L_\infty}^\flat$ and $\mathbb{C}_p^\flat$. Corollary 3.4.5 yields $\widehat{\overline{E_L}}$ is separably closed, and Lemma 3.4.6, and it is dense in its algebraic closure. But $\widehat{\overline{E_L}}$ is complete, we conclude that $\widehat{\overline{E_L}}$ is algebraically closed. By Proposition 3.1.8 and 3.3.15, we have $\widehat{\overline{E_L}} = \mathbb{C}_p^\flat$. □

3.5 Tilting correspondences

We are now ready for further results on tilting correspondence. The first result is about the (topological) isomorphism between the absolute Galois group of L_∞ and the absolute Galois group of E_L. We note that it is a fundamental step to establish the equivalence of categories later. Let $K_1 \subseteq K_2$ be two complete non-archimedean fields, we denote $\mathrm{Aut}^{\mathrm{cont}}(K_2/K_1)$ the group of continuos automorphism of K_2 fixing K_1. We also denote throughout this section $c \in W(\mathcal{O}_{\widehat{L_\infty}^\flat})$, such that $\Theta_{\widehat{L_\infty}}(c) = 0$.

Lemma 3.5.1. *$Gal(\overline{\mathbb{Q}_p}/L_\infty) \cong Aut^{cont}(\mathbb{C}_p/\widehat{L_\infty})$*

Proof. Take any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/L_\infty)$, then we can extend σ to an automorphism, that is continuous on $\mathbb{C}_p$, as described in Section 2 of this chapter about Galois action. By continuity, σ fixes $\widehat{L_\infty}$. This defines a map from $\mathrm{Gal}(\overline{\mathbb{Q}_p}/L_\infty)$ to $\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty})$. The injectivity of this map is clear. For the surjective part, take any $\sigma \in \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty})$, we have $\sigma|_{\overline{\mathbb{Q}_p}} \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/L_\infty)$, and again, we can extend $\sigma|_{\overline{\mathbb{Q}_p}}$ to $\theta \in \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty})$. By continuity, we get $\theta \equiv \sigma$. □

Similarly, we get

Lemma 3.5.2. *$Aut^{cont}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat) \cong Gal(E_L^{sep}/E_L)$*

Proof. By Corollary 3.4.7, we have $\mathbb{C}_p^\flat = \widehat{\overline{E_L}}$, and by Proposition 3.4.2, $\widehat{L_\infty}^\flat = \widehat{E^{\mathrm{perf}}}$. So, by similar argument, we obtain

$$\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat) \cong \mathrm{Gal}(\overline{E_L}/E_L^{\mathrm{perf}}) \cong \mathrm{Gal}(E_L^{\mathrm{sep}}/E_L)$$

□

Our first goal in this section is to prove $H_L := \mathrm{Gal}(\overline{\mathbb{Q}_p}/L_\infty) \cong H_{E_L} := \mathrm{Gal}(E_L^{\mathrm{sep}}/E_L)$ as topological groups via the isomorphism $\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty}) \cong \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$. We recall that the action from G_L on $\mathbb{C}_p^\flat$ is defined as

$$\begin{aligned} G_L \times \mathcal{O}_{\mathbb{C}_p^\flat} &\longrightarrow \mathcal{O}_{\mathbb{C}_p^\flat} \\ (\sigma, (..., a_i \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., a_0 \mod \pi\mathcal{O}_{\mathbb{C}_p})) &\longmapsto (..., \sigma(a_i) \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., \sigma(a_0) \mod \pi\mathcal{O}_{\mathbb{C}_p}) \end{aligned}$$

This action is continuous, and preserves $|.|_\flat$. Take any $\sigma \in H_L$, then σ fixes L_∞, and hence, also fixes $\widehat{L_\infty}$, and $\widehat{L_\infty}^\flat$. We obtain from this the map

$$\begin{aligned} \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty}) &\longrightarrow \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat) \\ \sigma &\longmapsto \sigma^\flat \end{aligned}$$

where $\sigma^\flat(..., a_i \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., a_0 \mod \pi\mathcal{O}_{\mathbb{C}_p}) := (..., \sigma(a_i) \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., \sigma(a_0) \mod \pi\mathcal{O}_{\mathbb{C}_p})$. We also have actions on $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ described as follows.

Lemma 3.5.3. *$Aut^{cont}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$ acts as automorphisms of $\mathcal{O}$-algebras on $W(\mathcal{O}_{\mathbb{C}_p^\flat})$, and it fixes $W(\mathcal{O}_{\widehat{L_\infty}^\flat})$.*

Proof. Because $k \hookrightarrow k((X)) \hookrightarrow \widehat{L_\infty}^\flat$, we have σ fixes k, for $\alpha \in \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$. Because the ring operations in $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ is given by Witt polynomials with coefficients in $\mathcal{O}/\pi\mathcal{O} = k$, we have σ acts as ring automorphism on $W(\mathcal{O}_{\mathbb{C}_p^\flat})$.

Also, the action from $\mathcal{O}$ to $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ factors through k (Section 2 about Witt vectors), we have $\sigma(\lambda b) = \lambda\sigma(b)$ for all $\lambda \in \mathcal{O}, b \in W(\mathcal{O}_{\mathbb{C}_p^\flat})$. And this yields σ acts as automorphism of $\mathcal{O}$-algebra on $W(\mathcal{O}_{\mathbb{C}_p^\flat})$.

The fact that σ fixes $W(\mathcal{O}_{\widehat{L_\infty}^\flat})$ is obvious, since σ fixes $\widehat{L_\infty}^\flat$. □

Lemma 3.5.4. *With the action from Lemma 3.5.3 defined above, the Teichmuler map $\tau : \mathcal{O}_{\mathbb{C}_p^\flat} \to W(\mathcal{O}_{\mathbb{C}_p^\flat})$ and $\Phi_n : W(\mathcal{O}_{\mathbb{C}_p^\flat}) \to \mathcal{O}_{\mathbb{C}_p^\flat}$ are $Aut^{cont}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$-equivariant.*

Proof. Take any $\sigma \in \mathrm{Gal}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$, we have

$$\tau(\sigma(\alpha)) = (\sigma(\alpha), 0, ...) = \sigma(\tau(\alpha))$$

for all $\alpha \in \mathcal{O}_{\mathbb{C}_p^\flat}$. And

$$\Phi_n(\sigma(\alpha_0), ..., \sigma(\alpha_n)) = \sigma(\alpha)^{q^n} = \sigma(\Phi_n(\alpha_0, ..., \alpha_n))$$

□

Lemma 3.5.5. *The action from $H_{E_L} \cong Aut^{cont}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$ to $\mathbb{C}_p^\flat$ is continuous.*

Proof. We can proceed this similarly to the proof of Corollary 3.2.3. □

To deduce the action fron H_{E_L} is also continuous on $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ w.r.t the weak topology, we need the following general lemma

Lemma 3.5.6. *Let B be a perfect topological k_L-algebra, and G a profinite group acts continuously on B as $\mathcal{O}$-algebra automorphism, then the action*

$$\begin{aligned} G \times W(B) &\longrightarrow W(B) \\ (\sigma, (b_0, b_1, ..)) &\longmapsto (\sigma(b_0), \sigma(b_1), ...) \end{aligned}$$

defines an $\mathcal{O}$-algebra automorphism, which is continuous w.r.t the weak topology on $W(B)$.

Proof. Take any $\sigma \in G$, and $b \in W(B)$, where $b = (b_0, b_1, ..)$, we recall that a fundamental system of open neighborhood around b is of the form

$$b + V_{\mathfrak{a},m} = \{(a_0, ..., a_{m-1}, ...), a_i \equiv b_i \mod \mathfrak{a}, 0 \leq i \leq m-1\}$$

where $\mathfrak{a}$ is an open ideal of B. For each $b_i (0 \leq i \leq m-1)$, we can find $U_i \subseteq G$: an open subgroup and $\mathfrak{b}_i$: open ideals of B such that

$$\sigma U_i \times (b_i + \mathfrak{b}_i) \subseteq \sigma(b_i) + \mathfrak{a}$$

Take $U := \bigcap_{i=0}^{m-1} U_i, \mathfrak{b} = \bigcap_{i=0}^{m-1} \mathfrak{b}_i$, we have

$$\sigma U \times V_{\mathfrak{b},m} \subset \sigma(b) + V_{\mathfrak{a},m}$$

Hence, the action from G to $W(B)$ is continuous. □

Using this, we obtain

Corollary 3.5.7. *H_{E_L} acts continuously on $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ w.r.t the weak topology.*

Proof. This follows easily from Lemma 3.5.5 and Lemma 3.5.6. □

To establish the bijective map between $\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$ and $\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty})$ we need the main lemma

Lemma 3.5.8.

(i) The map $\Theta_{\mathbb{C}_p} : W(\mathcal{O}_{\mathbb{C}_p^\flat} \to \mathcal{O}_{\mathbb{C}_p})$ is H_L-equivariant, in the sense that $\forall \sigma \in H_L$, all $\alpha \in W(\mathcal{O}_{\mathbb{C}_p^\flat})$, we have

$$\sigma(\Theta_{\mathbb{C}_p}(\alpha)) = \Theta_{\mathbb{C}_p}(\sigma^\flat(\alpha))$$

(ii) The map $\Theta_{\mathbb{C}_p}$ is open and continuous.

(iii) If we equip $W(\mathcal{O}_{\mathbb{C}_p^\flat})/cW(\mathcal{O}_{\mathbb{C}_p^\flat})$ the quotient topology, then $\Theta_{\mathbb{C}_p}$ induces a topologicali somorphism , H_L equivariant, between $W(\mathcal{O}_{\mathbb{C}_p^\flat})/cW(\mathcal{O}_{\mathbb{C}_p^\flat})$ and $\mathcal{O}_{\mathbb{C}_p}$.

Proof.

(i) We have

$$\Theta_{\mathbb{C}_p}\Big(\sum_{n\geq 0}\sigma^\flat\Big(\pi^n\tau(\alpha_n)\Big)\Big) = \Theta_{\mathbb{C}_p}\Big(\sum_{n\geq 0}\pi^n\sigma^\flat(\tau(\alpha_n))\Big) = \Theta_{\mathbb{C}_p}\Big(\sum_{n\geq 0}\pi^n\tau(\sigma^\flat(\alpha_n))\Big) =$$

$$= \sum_{n\geq 0}\pi^n\sigma(\alpha_n)^\sharp = \sum_{n\geq 0}\pi^n\sigma(\alpha^\sharp) = \sigma\Big(\sum_{n\geq 0}\pi^n\alpha_n^\sharp\Big) = \sigma\Big(\Theta_{\mathbb{C}_p}\Big(\sum_{n\geq 0}\tau(\alpha_n)\pi^n\Big)\Big)$$

where the first identity follows from Lemma 3.5.3, the second is from Lemma 3.5.4, the third is from the fact that $\Theta_{\mathbb{C}_p}(\tau(\sigma^\flat(\alpha_n))) = (\sigma^\flat(\alpha_n))^\sharp = \sigma(\alpha_n)^\sharp$, and the fourth identity follows from $\sigma(\alpha)^\sharp = \sigma(\alpha^\sharp)$.

(ii) Consider $\mathfrak{a}_m := \{\alpha \in \mathcal{O}_{\mathbb{C}_p^\flat}, |\alpha|_\flat \leq \pi^{q^{m-1}}\}$. We have

$$\Theta_{\mathbb{C}_p}(V_{\mathfrak{a}_m,m}) \supseteq \Theta_{\mathbb{C}_p}(\pi^m W(\mathcal{O}_{\mathbb{C}_p^\flat})) = \pi^m\Theta_{\mathbb{C}_p}(W(\mathcal{O}_{\mathbb{C}_p^\flat})) = \pi^m\mathcal{O}_{\mathbb{C}_p}$$

And because $\Theta_{\mathbb{C}_p}$ is surjective $\Theta_{\mathbb{C}_p}(V_{\mathfrak{a}_m,m})$ is an ideal of $\mathcal{O}_{\mathbb{C}_p}$ containing $\pi^m\mathcal{O}_{\mathbb{C}_p}$. This yields for any $a \in \Theta_{\mathbb{C}_p}(V_{\mathfrak{a}_m,m})$, $a + \pi^m\mathcal{O}_{\mathbb{C}_p} \subset \Theta_{\mathbb{C}_p}(V_{\mathfrak{a}_m,m})$. Hence, $\Theta_{\mathbb{C}_p}(V_{\mathfrak{a}_m,m})$ is open in $\mathbb{C}_p$. Since such $V_{\mathfrak{a}_m,m}$ forms a fundamental system of open neighborhood around 0 in $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ w.r.t the weak topology. And this yields the map $\Theta_{\mathbb{C}_p}$ is open.

On the other hand, for any $\alpha = (\alpha_0, \alpha_1, ..) \in V_{\mathfrak{a}_m,m}$, we have $\alpha = \sum_{n\geq 0}\tau(\alpha_n^{1/q^n})\pi^n$, and

$$\Theta_{\mathbb{C}_p}\Big(\sum_{n\geq 0}\pi^n\tau(\alpha_n^{1/q^n})\Big) = \sum_{n\geq 0}(\alpha_n^{1/q^n})^\sharp\pi^n \equiv \sum_{n=0}^{m-1}(\alpha_n^{1/q^n})^\sharp\pi^n \mod \pi^m\mathcal{O}_{\mathbb{C}_p}$$

And

$$|(\alpha_n^{1/q^n})^\sharp| = |\alpha_n|_\flat^{1/q^n} \leq |\pi|^{q^{m-1}/q^n} \leq |\pi|^{m-1-n}$$

for all $0 \leq n \leq m-1$. It turns out that $\Theta_{\mathbb{C}_p}(\alpha) \in \pi^{m-1}\mathcal{O}_{\mathbb{C}_p}$. Hence, $\Theta_{\mathbb{C}_p}(V_{\mathfrak{a}_m,m}) \subseteq \pi^{m-1}\mathcal{O}_{\mathbb{C}_p}$. This yields $\Theta_{\mathbb{C}_p}^{-1}(\pi^{m-1}\mathcal{O}_{\mathbb{C}_p}) \supseteq V_{\mathfrak{a}_m,m}$, and for each $\alpha \in \Theta_{\mathbb{C}_p}^{-1}(\pi^{m-1}\mathcal{O}_{\mathbb{C}_p})$, $\alpha + V_{\mathfrak{a}_m,m} \subseteq \mathcal{O}_{\mathbb{C}_p}^{-1}(\pi^{m-1}\mathcal{O}_{\mathbb{C}_p})$, and this yields $\Theta_{\mathbb{C}_p}^{-1}(\pi^{m-1}\mathcal{O}_{\mathbb{C}_p})$ is open in $W(\mathcal{O}_{\mathbb{C}_p^\flat})$. Because $\{\pi^m\mathcal{O}_{\mathbb{C}_p}\}_{m\geq 1}$ forms a fundamental system of open neighborhood around 0 in $\mathbb{C}_p$, this yields $\Theta_{\mathbb{C}_p}$ is continuous.

(iii) It follows from (ii) that the induced map $\Theta_{\mathbb{C}_p}$ from $W(\mathcal{O}_{\mathbb{C}_p^\flat})/cW(\mathcal{O}_{\mathbb{C}_p^\flat})$ to $\mathcal{O}_{\mathbb{C}_p}$ is continuous, open, and bijective. Hence, we obtain $W(\mathcal{O}_{\mathbb{C}_p^\flat})/cW(\mathcal{O}_{\mathbb{C}_p^\flat}) \cong \mathcal{O}_{\mathbb{C}_p}$ topologically.

□

We are now ready to prove

Proposition 3.5.9. *The map* $Aut^{cont}(\mathbb{C}_p/\widehat{L_\infty}) \xrightarrow{\sigma\mapsto\sigma^\flat} Aut^{cont}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$ *is bijective.*

Proof. For the injectivity, assume that $\sigma \mapsto id$ in $\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$, we then apply Lemma 3.5.8(i) to see that

$$\sigma(\Theta_{\mathbb{C}_p}(\alpha)) = \Theta_{\mathbb{C}_p}(\sigma^\flat(\alpha)) = \Theta_{\mathbb{C}_p}(\alpha)$$

And by the surjectivity of $\Theta_{\mathbb{C}_p}$, we get $\sigma \equiv id$.

We now take any $\sigma \in \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$, by Lemma 3.5.3, and Corollary 3.5.7, σ acts continuously on $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ as an automorphism of $\mathcal{O}$-algebra, that fixes $W(\mathcal{O}_{\widehat{L_\infty}^\flat})$. And hence, σ preserves $cW(\mathcal{O}_{\widehat{L_\infty}^\flat})$, and it induces a continuous action on the quotient topology $W(\mathcal{O}_{\mathbb{C}_p^\flat})/cW(\mathcal{O}_{\mathbb{C}_p^\flat}) \cong \mathcal{O}_{\mathbb{C}_p}$ which fixes $W(\mathcal{O}_{\widehat{L_\infty}^\flat})/cW(\mathcal{O}_{\widehat{L_\infty}^\flat}) \cong \mathcal{O}_{\widehat{L_\infty}}$. And by Lemma 3.5.8 (iii), we obtain $\sigma^\sharp \in \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty})$, which is defined by

$$\sigma^\sharp(\Theta_{\mathbb{C}_p}(-)) := \Theta_{\mathbb{C}_p}(\sigma(-))$$

Now, it is sufficient to prove that $(\sigma^\flat)^\flat = \sigma$. We note that from the construction of $\sigma^\sharp$, the pair $(\sigma, \sigma^\sharp)$ satisfies for all $\alpha \in \mathbb{C}_p^\flat$

$$\Theta_{\mathbb{C}_p}(\tau(\sigma(\alpha))) = \sigma^\sharp(\Theta_{\mathbb{C}_p}(\tau(\alpha)))$$

by Lemma 3.5.4. Take any $\alpha = (..., a_i \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., a_0 \mod \pi\mathcal{O}_{\mathbb{C}_p})$, we have

$$a_i \equiv (\alpha^{1/q^i})^\sharp \mod \pi\mathcal{O}_{\mathbb{C}_p} = \Theta_{\mathbb{C}_p}(\tau(\alpha^{1/q^i}))$$

And we have $\alpha = (..., \Theta_{\mathbb{C}_p}(\tau(\alpha^{1/q^i})) \mod \pi\mathcal{O}_{\mathbb{C}_p}, ...)$, which yields

$$\sigma(\alpha) = (..., \Theta_{\mathbb{C}_p}(\tau(\sigma(\alpha)^{1/q^i})) \mod \pi\mathcal{O}_{\mathbb{C}_p}, ...) = (..., \sigma^\sharp(\Theta_{\mathbb{C}_p}(\tau(\alpha^1/q^i)) \mod \pi\mathcal{O}_{\mathbb{C}_p}, ...) = (\sigma^\sharp)^\flat(\alpha)$$

And hence, $\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat) \cong \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty})$. ☐

To get the second result for the tilting correspondences, we need this

Lemma 3.5.10. *Let E be a complete, perfect, non-archimedean field of characteristic $p > 0$, then any finite extension F/E is also complete and perfect.*

Proof. The fact that F is complete follows from the general fact in the theory of extension of norms. We now prove F is perfect. Let $f(X) := X^p - a = (X - \alpha)^p$, for some $a \in F$ and $\alpha \in \overline{E}$, we have α is separable over E, since E is perfect, and hence, separable over F, and this yields the minimal polynomial of α over F is of degree 1, i.e. $\alpha \in F$. ☐

Proposition 3.5.11. *Let $K_1 \subseteq K_2$ be perfectoid fields. If $K_2^\flat$ is a finite extension of $K_1^\flat$, then $[K_2^\flat : K_1^\flat] = [K_2 : K_1]$. Moreover, if $K_2^\flat/K_1^\flat$ is finite, Galois, then so is K_2/K_1, and Gal$(K_2^\flat/K_1^\flat) \cong$ Gal(K_2/K_1).*

Proof. We first note that since $K_1^\flat$ is perfect, $K_2^\flat/K_1^\flat$ is separable. Let K' be a finite Galois extension of $K_1^\flat$ containing $K_2^\flat$. Then by Lemma 3.5.10, K' is complete, perfect and intermediate between $\widehat{L_\infty}^\flat$ and $\mathbb{C}_p^\flat$, it then follows by Theorem 3.3.14 that there exists some perfectoid field K, such that $K^\flat = K'$.

Let us denote $G := \mathrm{Gal}(K^\flat/K_1^\flat) = \mathrm{Aut}^{\mathrm{cont}}(K^\flat/K_1^\flat) = \mathrm{Aut}(K^\flat/K_1^\flat) \cong \mathrm{Aut}(K/K_1)$, via the similar proof to Proposition 3.5.9. We then have the commutative diagram

$$\begin{array}{ccc} (W(\mathcal{O}_{K^\flat})/cW(\mathcal{O}_{K^\flat}))^G & \xrightarrow{\cong} & \mathcal{O}_K^G \\ {\scriptstyle i}\big\uparrow & & \big\uparrow \\ W(\mathcal{O}_{K_1^\flat})/cW(\mathcal{O}_{K_1^\flat})^G & \xrightarrow{\cong} & \mathcal{O}_{K_1} \end{array} \tag{3.10}$$

From the short exact sequence

$$0 \to W(\mathcal{O}_{K^\flat}) \xrightarrow{\cdot c} W(\mathcal{O}_{K^\flat}) \to W(\mathcal{O}_{K^\flat})/cW(\mathcal{O}_{K^\flat}) \to 0$$

of G-modules, and since $W(\mathcal{O}_{K^\flat})^G = W(\mathcal{O}_{K_1^\flat})$, we obtain the following exact sequence

$$0 \to W(\mathcal{O}_{K_1^\flat}) \xrightarrow{\cdot c} W(\mathcal{O}_{K_1^\flat}) \to (W(\mathcal{O}_{K^\flat})/cW(\mathcal{O}_{K^\flat}))^G \to H^1(G, W(\mathcal{O}_{K_1^\flat}))$$

And this yields the following exact sequence

$$0 \to W(\mathcal{O}_{K_1^\flat})/cW(\mathcal{O}_{K_1^\flat}) \xrightarrow{i} (W(\mathcal{O}_{K^\flat})/cW(\mathcal{O}_{K^\flat}))^G \to H^1(G, W(\mathcal{O}_{K_1^\flat}))$$

And one obtains from this that $\mathcal{O}_K^G/\mathcal{O}_{K_1} \cong \mathrm{coker}(i) \subseteq H^1(G, W(\mathcal{O}_{K_1^\flat}))$, which is killed by $|G|$. On the other hand, this first cohomology group is also an $\mathcal{O}$-module, where a number prime to p is invertible. Hence, $H^1(G, W(\mathcal{O}_{K_1^\flat}))$ is killed by p^n for some integer n. This yields $\mathcal{O}_K^G/\mathcal{O}_{K_1}$ is killed by p^n, which means that for any $a \in \mathcal{O}_K^G$, $p^n x \in \mathcal{O}_{K_1}$. Because p is invertible in K, we get $K^G = K_1$. And it follows from Artin's lemma in Galois theory that K/K_1 is Galois, with $\mathrm{Gal}(K/K_1) = G$. If we replace K_1 by K_2, we obtain easily that

$$[K_2^\flat : K_1^\flat] = [K^\flat : K_1^\flat]/[K^\flat : K_2^\flat] = [K : K_1]/[K : K_2] = [K_2 : K_1]$$

From the above argument, when $K_2^\flat/K_1^\flat$ is finite Galois, then so is K_2/K_1, and $\mathrm{Gal}(K_2^\flat/K_1^\flat) \cong \mathrm{Gal}(K_2/K_1)$. □

To deduce the main theorem, we need a further

Lemma 3.5.12. *For any finite extension E/E_L in E_L^{sep}, we have*
(i) $\widehat{EL_\infty}^\flat = E^{perf}$.
(ii)$\widehat{EL_\infty}^\flat \cap E_L^{sep} = E$.
(iii) If E/E_L is Galois, then so is $\widehat{EL_\infty}^\flat/\widehat{L_\infty}^\flat$ and Gal$(E/E_L) =$ Gal$(\widehat{EL_\infty}^\flat/\widehat{L_\infty}^\flat)$.

Proof. (i) We can see easily that $\widehat{EL_\infty}^\flat = EE^{\mathrm{perf}} \subset \widehat{E^{\mathrm{perf}}}$. Also, since $\widehat{EL_\infty}^\flat/\widehat{L_\infty}^\flat$ is finite, and $\widehat{L_\infty}^\flat$ is perfect, by Lemma 3.5.10, we have $\widehat{EL_\infty}^\flat$ is complete, and perfect, hence $\widehat{EL_\infty}^\flat \supseteq \widehat{E^{\mathrm{perf}}}$. This yields $\widehat{EL_\infty}^\flat = \widehat{E^{\mathrm{perf}}}$.

(ii) Due to (i) and the fact that E/E_L is finite, separable, it is sufficient to prove that there is no proper finite field extension F/E, which is separable, contained in $\widehat{EL_\infty}^\flat = \widehat{E^{\mathrm{perf}}}$. Assume that there exists $F \subseteq \widehat{E^{\mathrm{perf}}}$ and F/E is finite, separable of degree $d \geq 1$. Then there exists d embedding $\sigma_i : F/E \hookrightarrow E^{\mathrm{sep}}/E$. By defining $\sigma_i(\alpha^{1/p^m}) = \sigma_i(\alpha)^{1/p^m}$, we can extend σ_i to embeddings $F^{\mathrm{perf}} \hookrightarrow \overline{E}$. Note that for any $\alpha \in E$, we have $\sigma_i(\alpha^{1/p^m}) = \sigma_i(\alpha)^{1/p^m} = \alpha^{1/p^m}$. So, these embeddings can be seen as $F^{\mathrm{perf}}/E^{\mathrm{perf}} \xrightarrow{\sigma_i} \overline{E}/E^{\mathrm{perf}}$. And because σ_i preserves norms, we can further extend it to

$$\widehat{F^{\mathrm{perf}}}/\widehat{E^{\mathrm{perf}}} \xhookrightarrow{\sigma_i} \widehat{\overline{E}}/\widehat{E^{\mathrm{perf}}} = \mathbb{C}_p^\flat/\widehat{E^{\mathrm{perf}}}$$

But since $\widehat{E^{\mathrm{perf}}} = \widehat{EL_\infty}^\flat$ is perfect, and containing F, it also containing F^{perf}. And since $\widehat{E^{\mathrm{perf}}}$ is complete, we have $\widehat{E^{\mathrm{perf}}} \supseteq \widehat{F^{\mathrm{perf}}}$. The reverse inclusion is clear, since $E \subseteq F$. So, we have $\widehat{F^{\mathrm{perf}}} = \widehat{E^{\mathrm{perf}}}$, and hence, σ_i is just the identity map. And this yields $F = E$.

(iii) When E/E_L is finite, Galois, so is $\widehat{EL_\infty}^\flat/\widehat{L_\infty}^\flat$. We have, by similar argument to (ii), if $\sigma \in \mathrm{Gal}(E/E_L)$, then σ can be extended to an element in $\mathrm{Aut}(\widehat{E^{\mathrm{perf}}}/\widehat{E_L^{\mathrm{perf}}}) = \mathrm{Gal}(\widehat{EL_\infty}^\flat/\widehat{L_\infty}^\flat)$. So, the induced map between the two Galois groups is injection. Take any $\sigma \in \mathrm{Gal}(\widehat{EL_\infty}^\flat/\widehat{L_\infty}^\flat)$, we can see that σ is completely determined by its action on E, i.e. σ is determined by $\sigma|_E$, which is obvious in $\mathrm{Gal}(E/E_L)$. Hence, $\mathrm{Gal}(E/E_L) \cong \mathrm{Gal}(\widehat{EL_\infty}^\flat/\widehat{L_\infty}^\flat)$. □

We are now ready to deduce a fundamental fact, which can be considered as the second tilting correspondence.

Theorem 3.5.13. *The isomorphism Gal$(\overline{\mathbb{Q}_p}/L_\infty) \cong$ Gal(E_L^{sep}/E_L) is a topological isomorphism.*

Proof. We recall that both groups above are profinite, and they have fundamental system of open neighborhoods of *id* contains all open normal subgroups of finite index. Also, they are Hausdorff and complete, and a bijection between them is the combination of Lemma 3.5.1, Lemma 3.5.2 and Proposition 3.5.9. So, it is sufficient for us to prove the induced map between them are continuous.

Let us take $U \subset H_{E_L}$ an open, normal subgroup of finite index, and $E = (E_L^{\mathrm{sep}})^U$, then E/E_L is Galois of degree $[H_{E_L} : U]$. Using Lemma 3.5.12, we can pass it to Galois extension $\widehat{EL_\infty}^\flat/\widehat{L_\infty}^\flat$ of degree $[\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat) : U]$, where U by abusing of notation, is a normal subgroup of finite index of $\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p^\flat/\widehat{L_\infty}^\flat)$.

Using Proposition 3.5.9, we can again pass U to V: a normal subgroup of finite index in $\mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty})$. By Proposition 3.5.11, there is a perfectoid field K containing $\widehat{L_\infty}^\flat$ such that $K/\widehat{L_\infty}$ is finite, Galois and $\mathrm{Gal}(K/\widehat{L_\infty}) \cong \mathrm{Gal}(E\widehat{L_\infty}^\flat/\widehat{L_\infty}^\flat)$, and $\mathrm{Gal}(K/\widehat{L_\infty}) \cong \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty})/V$.

We now use the Ax-Sen-Tate theorem to see that if $K_0 := K \cap \overline{\mathbb{Q}_p}$, then $K = \widehat{K_0}$. Via the isomorphism $H_L \cong \mathrm{Aut}^{\mathrm{cont}}(\mathbb{C}_p/\widehat{L_\infty})$, we can pass V to a normal subgroup W in H_L, which is exactly $\mathrm{Gal}(\overline{\mathbb{Q}_p}/K_0)$, by continuity. And this yields W is both of finite index and closed in H_L. That means W is open in H_L. We therefore obtain $H_L \cong H_{E_L}$. □

We can also look closer into the tilting correspondences, as an application of method in characteristic p.

Lemma 3.5.14. *Let K be a perfectoid field, and K_1/K is a finite extension in $\mathbb{C}_p$, then there exists a Galois extension of finite degree $F/K^\flat$ such that $K_1 \subset F^\sharp$.*

Proof. Let us denote K^{per} the union of all Galois extensions of K coming from $F^\sharp$, where $F/K^\flat$ is finite, Galois, as in Proposition 3.5.11 pointed out. It can be seen that $\widehat{K^{\mathrm{per}}}$ is a perfectoid field inside $\mathbb{C}_p$, and $(\widehat{K^{\mathrm{per}}})^\flat = \widehat{K^{\mathrm{sep}}} = \mathbb{C}_p^\flat$, which means $\widehat{K^{\mathrm{per}}} = \mathbb{C}_p$, and hence, K^{per} is dense in $\mathbb{C}_p$. We also have $\overline{K}/K^{\mathrm{per}}$ is a Galois extension. Take any $\sigma \in \mathrm{Gal}(\overline{K}/K^{\mathrm{per}})$, this is in fact a continuous map from $\overline{K}/K^{\mathrm{per}}$ to $\overline{K}/K^{\mathrm{per}}$, because it preserves absolute values. Hence, it can be extended to $\widehat{\overline{K}}/\widehat{K^{\mathrm{per}}}$ to $\widehat{\overline{K}}/\widehat{K^{\mathrm{per}}}$, which is the identity map on $\mathbb{C}_p$. And hence, $\overline{K} = K^{\mathrm{per}}$.

From this, we have $K_1 \subseteq K^{\mathrm{per}}$, and hence, there exists some $F/K^\flat$: finite, Galois such that $F^\sharp = K_1$. □

Via this lemma, we obtain the third tilting correspondence

Theorem 3.5.15.

1. *If K_1/K is a finite extension, where K is a perfectoid field, then so is K_1.*

2. *If K_1/K is an extension of perfectoid fields, then K_1/K is finite iff $K_1^\flat/K^\flat$ is finite, and in this case, $[K_1 : K] = [K_1^\flat : K^\flat]$.*

3. *Let K_1, K be defined as in (ii), then K_1/K is finite Galois iff $K_1^\flat/K^\flat$ is finite Galois, and in this case, Gal$(K_1/K) \cong$ Gal$(K_1^\flat/K^\flat)$.*

Proof.

1. As in the the proof of Lemma 3.5.14, we can find $F_2/K^\flat$: finite, Galois, such that $F_2^\sharp =: K_2 \supseteq K_1$. And due to Proposition 3.5.11, we have $\mathrm{Gal}(F_2/K^\flat) \cong \mathrm{Gal}(K_2/K)$. Because any intermediate field between $K^\flat$ and F_2 is complete, perfect, its un-tilt is perfectoid. And due to the isomorphism, we conclude that any immediate field between K and K_2 is perfectoid, and in particular, K_1 is perfectoid.

2. Assume that K_1/K is finite, then by Lemma 3.5.14, there exists $F/K^\flat$: finite, Galois, such that $F^\sharp \supseteq K_1$, and hence, $(F^\sharp)^\flat \supseteq K_1^\flat$, i.e. $F \supseteq K_1^\flat$. And this yields $K_1^\flat/K^\flat$ is finite.

   Conversely, if $K_1^\flat/K^\flat$ is finite, we can find $F \supseteq K_1^\flat$, such that $F/K^\flat$ is finite, Galois, and by Proposition 3.5.11, $[F : K^\flat] = [F^\sharp : K]$, and $F^\sharp \supseteq K_1$. This yields K_1/K is finite.

   We have in both cases, by Proposition 3.5.11,

$$[K_1^\flat : K^\flat] = [\mathrm{Gal}(F/K^\flat) : \mathrm{Gal}(F/K_1^\flat)] = [\mathrm{Gal}(F^\sharp/K) : \mathrm{Gal}(F^\sharp/K_1)] = [K_1 : K]$$

3. Assume that K_1/K is finite, Galois, then by (ii) $K_1^\flat/K^\flat$ is finite. By Lemma 3.5.14, there exists $F/K^\flat$: finite, Galois, such that $F^\sharp \supseteq K_1$. By Proposition 3.5.11, we have $\mathrm{Gal}(F^\sharp/K_1) \cong \mathrm{Gal}(F/K_1^\flat)$, and $\mathrm{Gal}(F^\sharp/K) \cong \mathrm{Gal}(F/K^\flat)$. Because K_1/K is Galois, we have $\mathrm{Gal}(F^\sharp/K_1)$ is a normal subgroup of $\mathrm{Gal}(F/K^\flat)$, and this yields $K_1^\flat/K^\flat$ is Galois, and it follows that $\mathrm{Gal}(K_1/K) \cong \mathrm{Gal}(K_1^\flat/K^\flat)$. By Proposition 3.5.11, we easily obtain the isomorphism between the two absoute Galois groups.

$\square$

3.6 Application I: p-cohomological dimension of $G_{\mathbb{Q}_p}$

Let us fix p an odd prime. We will restrict ourselves into the case $L := \mathbb{Q}_p$, we denote $\mathbb{Q}_p^\infty := L_\infty$ the field extension of $\mathbb{Q}_p$ obtained by adjoining all p^n-th roots of unity. In this case, $k_L = \mathbb{F}_p, E_L = \mathbb{F}_p((X)) =: E$, $\Gamma_{\mathbb{Q}_p} = \mathrm{Gal}(\mathbb{Q}_p^\infty/\mathbb{Q}_p)$ and $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p), H_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^\infty) \cong \mathrm{Gal}(E^{\mathrm{sep}}/E) =: G_E$ by Theorem 3.5.13. We will prove that the p-cohomological dimension of $G_{\mathbb{Q}_p}$ is less than or equal to 2, i.e. for any finite dimensional $\mathbb{F}_p$-vector space V, with a continuous action from $G_{\mathbb{Q}_p}$ w.r.t the discrete topology on V, $H^n(G_{\mathbb{Q}_p}, V) = 0$, for $n > 2$.

For the case V has the trivial action from $G_{\mathbb{Q}_p}$, because $H^n(G_{\mathbb{Q}_p}, V) = \oplus H^n(G_{\mathbb{Q}_p}, \mathbb{F}_p)$, where $\mathbb{F}_p$ is equipped with the trivial action from $G_{\mathbb{Q}_p}$. Thus, it is sufficient to prove the statement for the case $\mathbb{F}_p$.

From the short exact sequence

$$0 \to \mathbb{F}_p \to E^{\mathrm{sep}} \xrightarrow{\phi_p - 1} E^{\mathrm{sep}} \to 0$$

of G_E-modules, by Hilbert's theorem 90, we have $H^r(G_E, E^{\mathrm{sep}}) = 0$ for all $r \geq 1$, and this yields $H^s(G_E, \mathbb{F}_p) = 0$, for all $s \geq 2$. It means that the $\mathbb{F}_p$-cohomological dimension of G_E is less than or equal to 1, and it is exactly 1 since $H^1(G_E, \mathbb{F}_p) = E/(\phi_p - 1)E \neq 0$.

Since $G_{\mathbb{Q}_p}/H_{\mathbb{Q}_p} = \Gamma_{\mathbb{Q}_p}$, it is sufficient to prove that the $\mathbb{F}_p$-cohomological dimension of $\Gamma_{\mathbb{Q}_p}$ is smaller than or equal to 1, where $\Gamma_{\mathbb{Q}_p}$ acts trivially on $\mathbb{F}_p$. We note that $\Gamma_{\mathbb{Q}_p} \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p$ and $H_T^0((\mathbb{Z}/p\mathbb{Z})^\times, \mathbb{F}_p) = \mathbb{F}_p/\mathrm{Nm}_{(\mathbb{Z}/p\mathbb{Z})^\times}(\mathbb{F}_p) = 0$, and $H_T^1((\mathbb{Z}/p\mathbb{Z})^\times, \mathbb{F}_p) = \mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})^\times, \mathbb{F}_p) = 0$, where H_T^r denotes the r-th Tate cohomology group. And this yields by the periodicity of cohomology of finite cyclic groups [Mil13](Proposition II.3.4) that $H^r((\mathbb{Z}/p\mathbb{Z})^\times, \mathbb{F}_p) = 0$ for all $r \geq 1$. Hence, one can apply the inflation-restriction sequence [Mil13](Proposition II.1.34) to get

$$H^r(\mathbb{Z}_p, \mathbb{F}_p) \cong H^r(\Gamma_{\mathbb{Q}_p}, \mathbb{F}_p)(\forall r \geq 1)$$

But since, $\mathbb{Z}_p$ is a torsion-free procyclic group, it follows from [NSW00](Proposition 1.6.13) that $H^r(\mathbb{Z}_p, \mathbb{F}_p) = 0$ for all $r \geq 2$. Hence, this yields $H^n(G_{\mathbb{Q}_p}, \mathbb{F}_p) = 0$, for $n > 3$.

To proceed the case of general V, let us denote $G := G_{\mathbb{Q}_p}$, we first note that $c_p(G) = c_p(G_p)$, where $c_p(G)$ is the p-cohomological dimension of G, and G_p is the Sylow p-group of G. So, it is sufficient to prove that $H^n(G_p, V) = 0$, for $n > 3$. It can be seen that

Lemma 3.6.1. $V^{G_p} \neq 0$.

Proof. Because $|V|$ is finite, we can represent $|V| = |V^{G_p}| + \sum_{x \in V} |Orb(x)|$, where $Orb(x)$ denotes the orbit of $x \in V$ under the action of G_p, and the sum runs over all non-trivial equivalence classes of orbits. Because G_p is a pro-p group, $Orb(x)$ is a power of p. And hence, p divides $|V^{G_p}|$. This yields $|V^{G_p}| \neq 0$. $\square$

Now, from the short exact sequence of $\mathbb{F}_p$ vector space

$$0 \to V^{G_p} \to V \to V/V^{G_p} \to 0$$

where V^{G_p} satisfies the statement, and $|V/V^{G_p}| < |V|$ by the previous lemma, we can use induction on $|V|$. And the statement now follows.

Chapter 4

The category $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$

We first fix notations as in the previous chapter. We recall that the main goal of the thesis is to prove the equivalence between $\mathrm{Rep}_{\mathcal{O}}(G_L)$ and $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$. And this chapter is devoted to describe the category $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$, where $\mathscr{A}_L$ is the ring of infinite Laurent series over $\mathcal{O}$, as introduced in the first section. One can define the action from Γ_L to $\mathscr{A}_L$ as follows

$$\begin{aligned} \Gamma_L \times \mathscr{A}_L &\longrightarrow \mathscr{A}_L \\ (\gamma, f(X)) &\longmapsto f([\chi_L(\gamma)]_\phi(X)) \end{aligned}$$

where $\chi_L : \Gamma \xrightarrow{\cong} \mathcal{O}^\times$ as proved in the first chapter, and ϕ is a Frobenius series used to define L_∞. And φ_L is defined to be

$$\begin{aligned} \varphi_L : \mathscr{A}_L &\longrightarrow \mathscr{A}_L \\ f(X) &\longmapsto f([\pi]_\phi(X)) \end{aligned}$$

With respect to the weak topology on $\mathscr{A}_L$, the actions of Γ_L and φ_L is continuous, and one can embed $\mathscr{A}_L$ (topologically) into $W(E_L)$, and the actions of Γ_L and φ_L on $\mathscr{A}_L$ are compatible with the actions of Γ_L and Frobenius on $W(E_L)$. Note that it is a fundamental step to construct the Fontaine ring A defined in the next chapter. To construct this embedding, we will need to lift the Teichmuller map τ and $\iota : T \to \mathfrak{m}_{E_L}$ in a specific way, where T is the Tate module. Via these liftings, we can point out the existence of $c \in W(\mathcal{O}_{\widehat{L_\infty}^\flat})$ such that c satisfies the conditions of Proposition 3.3.2, and this completes the proof of tilting correspondences.

In the last section, we will introduce objects and morphisms in $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$, and give some examples for etale (φ_L, Γ_L)-modules.

4.1 A two dimensional local field

In this section, we will describe the coefficients ring over which (φ_L, Γ_L)-modules are defined.

We first introduce the ring

$$\mathscr{A}_L := \varprojlim_m \mathcal{O}((X))/\pi^m\mathcal{O}((X)) = \varprojlim_m (\mathcal{O}/\pi^m\mathcal{O})((X))$$

We will point out that $\mathscr{A}_L$ is exactly the ring of inifinte Laurent series, where coefficients go to 0 when the indicies go to $-\infty$. First, let $f(X) := \sum_{i\in\mathbb{Z}} a_i X^i$, where $a_i \in \mathcal{O}$, and $\lim_{i\to-\infty} a_i = 0$, and $A_m := \sum_{i\in\mathbb{Z}}(a_i \mod \pi^m\mathcal{O})X^i$. Because $\lim_{i\to-\infty} a_i = 0$, when i is sufficient small, we have $a_i \equiv 0 \mod \pi^m\mathcal{O}$, and this yields, in fact $A_m \in (\mathcal{O}/\pi^m\mathcal{O})((X))$, and it is clear that $A_{m+1} \equiv A_m \mod \pi^m\mathcal{O}$, hence $(A_m)_m \in \mathscr{A}_L$.

Conversely, let $(A_m)_m \in \mathscr{A}_L$, where $A_m = \sum_{i\in\mathbb{Z}}(a_{m,i} \mod \pi^m\mathcal{O})X^i$, where for some $i(m)$, and all $i \le i(m)$, we have $a_{m,i} \equiv 0 \mod \pi^m$. Because $(A_m)_m \in \mathscr{A}_L$, we have $a_{m+1,i} \equiv a_{m,i} \mod \pi^m$. And this yields, there exists $a_i \in \mathcal{O}$, such that $a_i = \lim_{m\to\infty} a_{m,i}$, and it follows that $a_i \equiv a_{m,i} \mod \pi^m$.

Let us denote $f(X) := \sum_{i\in\mathbb{Z}} a_i X_i$, then for any m, and $i < i(m)$, we have $a_{m,i} \equiv 0 \mod \pi^m$. And hence, for such i, $a_i \equiv 0 \mod \pi^m$. And this follows that $\lim_{i\to-\infty} a_i = 0$.

We can see from this that the identification is not just a bijection of sets, it is an $\mathcal{O}$-algebra isomorphism, with the usual Cauchy product on the ring of infinite Laurent series with coefficients in $\mathcal{O}$. And because $\mathscr{A}_L = \varprojlim_m \mathcal{O}((X))/\pi^m\mathcal{O}((X))$, $\pi\mathscr{A}_L$ is a maximal ideal of $\mathscr{A}_L$, and $\mathscr{A}_L/\pi\mathscr{A}_L \cong (\mathcal{O}/\pi\mathcal{O})((X)) = k((X))$.

Lemma 4.1.1. *Any element in $\mathscr{A}_L \setminus \pi\mathscr{A}_L$ is a unit*

Proof. Let $f = \sum_{i\in\mathbb{Z}} a_i X^i \in \mathscr{A}_L \setminus \pi\mathscr{A}_L$, since $\lim_{i\to-\infty} a_i = 0$, we can find a smallest integer i_0, such that $a_{i_0} \neq 0 \mod \pi$, we can see that

$$f(X) = \sum_{i<i_0} a_i X^i + X^{i_0}\Big(\sum_{i\geq i_0} a_i X^{i-i_0}\Big) = g(X) + X^{i_0}u(X)$$

where $g(X) = \sum_{i<i_0} a_i X^i \in \pi\mathscr{A}_L$, $u(X) = \sum_{i\geq i_0} a_i X^{i-i_0}$, which is invertible in $\mathcal{O}[[X]] \subset \mathscr{A}_L$. And hence,

$$f(X) = \Big(\frac{g(X)}{X^{i_0}u(X)} + 1\Big)X^{i_0}u(X)$$

where $\frac{g(X)}{X^{i_0}u(X)} \in \pi\mathscr{A}_L$. But then, $1+\pi a$, for any $a \in \mathscr{A}_L$ is invertible, since $\mathscr{A}_L$ is π-adically complete, and hence, $1 + (-\pi a) + (-\pi a)^2 + ... \in \mathscr{A}_L$, and it is the invert of $1 + \pi a$. This then yields f is invertible. □

By this, $\mathscr{A}_L$ is a local ring with the unique maximal ideal $\pi\mathscr{A}_L$. We can further define the norm of $f = \sum_{i\in\mathbb{Z}} a_i X^i \in \mathscr{A}_L$ as $|f| = \max_{i\in\mathbb{Z}} |a_i|$. One can see that it is in fact well-defined, since the valuation in L is discrete. And it is obvious to see that $|f| = 0$ iff $f = 0$, and $|f+g| \leq \max\{|f|, |g|\}$.

Lemma 4.1.2. *For any $f, g \in \mathscr{A}_L$, we have $|fg| = |f|.|g|$, and it follows that $\mathscr{A}_L$ is an integral domain.*

Proof. We can write $|f| = |\pi^m||a_i|$, for some $f \in \mathscr{A}_L$, $m \geq 0$ and $|a_i| = 1$. So it is sufficient for us to deal with the case $|f| = |g| = 1$. In this case $f, g \in \mathscr{A}_L \setminus \pi\mathscr{A}_L$ and hence, $fg \in \mathscr{A}_L \setminus \pi\mathscr{A}_L$, since $\pi\mathscr{A}_L$ is a maximal ideal of $\mathscr{A}_L$, and this yields $|fg| = |f||g| = 1$. The second statement is immediate. □

Now, via this proof, we can see easily that $\mathscr{A}_L$ is a local domain. Its field of fractions is denoted $\mathscr{B}_L$. By Lemma 4.1.1, we can write

$$\mathscr{B}_L = \bigcup_{m\geq 0} \pi^{-m}\mathscr{A}_L = \{f = \sum_{i\in\mathbb{Z}} a_i X^i, a_i \in L, \sup|a_i| < \infty, \lim_{i\to-\infty} |a_i| = 0\}$$

And it can be seen that $\mathscr{A}_L = \{f \in \mathscr{B}_L, |f| \leq 1\}$, and $f \in \pi^m\mathscr{A}_L$ iff $|f| \leq |\pi|^m$. Hence, with this kind of norm, $\mathscr{A}_L$ is a complete metric space, since this is identical with the π-adic topology.

We are going to explore the action from $\Gamma_L := \mathrm{Gal}(L_\infty/L)$ to $\mathscr{A}_L$. First, for any $g \in \mathcal{O}[[X]]$, we can define

$$\begin{aligned}\psi_g : \mathcal{O}/\pi^m\mathcal{O}[[X]] &\longrightarrow \mathcal{O}/\pi^m\mathcal{O}[[X]]\\ f &\longmapsto f(g \mod \pi^m\mathcal{O})\end{aligned}$$

In order to extend this to $(\mathcal{O}/\pi^m\mathcal{O})((X))$, we need $g(X)$ to be invertible in $(\mathcal{O}/\pi^m\mathcal{O})((X))$. In particular, if we take $g(X) \in X\mathcal{O}[[X]]$, and $g(X) \in \mathscr{A}_L \setminus \pi\mathscr{A}_L$, then we can extend

$$\begin{aligned}\psi_g : \mathscr{A}_L/\pi^m\mathscr{A}_L = \mathcal{O}/\pi^m\mathcal{O}((X)) &\longrightarrow \mathscr{A}_L/\pi^m\mathscr{A}_L = (\mathcal{O}/\pi^m\mathcal{O})((X))\\ f &\longmapsto f(g \mod \pi^m\mathcal{O})\end{aligned}$$

This is a homomorphism of $\mathcal{O}$-algebra, and it is compatible with the inverse system defined $\mathscr{A}_L$. Therefore, we obtain the map

$$\begin{aligned} \psi_g : \mathscr{A}_L &\longrightarrow \mathscr{A}_L \\ f &\longmapsto f(g(X)) \end{aligned}$$

And this also extends to the same map from $\mathscr{B}_L \to \mathscr{B}_L$. And in particular, it is injective. We now apply this to the action from Lubin-Tate theory.

Let ϕ be a Frobenius series defining L_∞, for any $a \in \mathcal{O}^\times$, we have $[a]_\phi(X) = ax \mod \deg 2$, hence $[a]_\phi$ is invertible in $\mathscr{A}_L$, and we then obtain an action

$$\begin{aligned} \mathcal{O}^\times \times \mathscr{A}_L &\longrightarrow \mathscr{A}_L \\ (a, f) &\longmapsto f \circ [a]_\phi(X) \end{aligned}$$

And because $\chi : \Gamma_L \xrightarrow{\sim} \mathcal{O}^\times$, we obtain an action

$$\begin{aligned} \Gamma_L \times \mathscr{A}_L &\longrightarrow \mathscr{A}_L \\ (\sigma, f) &\longmapsto f([\chi(\sigma)]_\phi(X)) \end{aligned}$$

Because $[\pi]_\phi = \phi \equiv X^q \mod \pi\mathcal{O}[[X]]$, it is invertible in $\mathscr{A}_L$, we also have the map

$$\begin{aligned} \varphi_L : \mathscr{A}_L &\longrightarrow \mathscr{A}_L \\ f &\longmapsto f \circ \phi \end{aligned}$$

And because for any $a \in \mathcal{O}^\times$, we have $[a]_\phi \circ [\pi]_\phi = [\pi]_\phi \circ [a]_\phi$, so the map φ_L is Γ_L-equivariant. Also φ_L is an injective map. We can deduce some facts about $\mathscr{A}_L$ as $\phi_L(\mathscr{A}_L)$-module.

Lemma 4.1.3. *$\mathscr{A}_L$ is a free $\varphi_L(\mathscr{A}_L)$-module with basis $1, X, ..., X^{q-1}$.*

Proof. See [Sch17](Proposition 1.7.3). □

We can see that $\mathscr{A}_L$ has a natural π-adic topology, but since $k((X))$ and its subrings $\mathcal{O}[[X]]$ also has their own topology, so called X-adic topology, we want to equip a topology on $\mathscr{A}_L$ with relation to both π and X. We define

$$U_{l,m} := X^l\mathcal{O}[[X]] + \pi^m \mathscr{A}_L (l \geq 0, m \geq 1)$$

They are $\mathcal{O}[[X]]$-submodules of $\mathscr{A}_L$ and it can be checked easily that there exists a unique topology on $\mathscr{A}_L$ such that such $U_{l,m}$ forms a fundamental system of open neighborhoods around 0 in $\mathscr{A}_L$. This topology is weaker than the π-adic topology, and it is said to be **the weak topology on** $\mathscr{A}_L$. If we denote $U_m := U_{m,m}$, then we always have

$$U_{l,m} \supseteq U_{\max\{l,m\}}$$

That means if we choose $\{U_m\}$ as a fundamental system of open neighborhoods around 0 in $\mathscr{A}_L$, then the topology on $\mathscr{A}_L$ is the same as above. Because $\{U_m\}$ is a filtered fundamental system, $\mathscr{A}_L$ is complete w.r.t the weak topology iff all Cauchy sequences in $\mathscr{A}_L$ w.r.t the weak topology converges in $\mathscr{A}_L$. Using this, we prove that

Lemma 4.1.4. *With the weak topology defined as above, $\mathscr{A}_L$ is Hausdorff and complete.*

Proof. Take $f \neq 0, f \in \mathscr{A}_L$, and $m = \max\{m, \pi^m g = f, g \in \mathscr{A}_L\}$, then it can be seen that $f \notin U_{0,m+1}$. That means, $\mathscr{A}_L$ is Hausdorff.

Let $(f_n)_n$ be a Cauchy sequence in $\mathscr{A}_L$, w.r.t the weak topology, we then have $\forall m \geq 1$, there exists n_m such that $n_{m+1} > n_m$, and for all $n, n' \geq n_m$ $f_n - f_{n'} \in X^m\mathcal{O}[[X]] + \pi^m \mathscr{A}_L$. We then form a subsequence $y_m := x_{n_m}$ of $(x_n)_n$, then it can be seen that $y_{m+1} - y_m = X^m g_m + \pi^m h_m$, for some $g_m \in \mathcal{O}[[X]]$, $h_m \in \mathscr{A}_L$. This yields

$$y_{m+1} = X^m g_m + \pi^m h_m + y_m$$

Inductively, we have

$$y_{m+1} = (X^m g_m + X^{m-1} g_{m-1} + ... + X g_1) + (\pi^m h_m + \pi^{m-1} h_{m-1} + ... \pi h_1)$$

where $g_i \in \mathcal{O}[[X]], h_i \in \mathscr{A}_L$. Because $\mathcal{O}[[X]]$ is X-adic complete, $\sum_{i\geq 1} X^i g_i$ is well-defined, and $\mathscr{A}_L$ is π-adically complete, $\sum_{i\geq 1} \pi^i h_i$ is also well-defined. Let

$$y := \sum_{i\geq 1} X^i g_i + \sum_{i\geq 1} \pi^i h_i$$

then y is an element in $\mathscr{A}_L$. And it can be seen easily that y is a convergent value of $(y_n)_n$, and hence, of $(x_n)_n$. This yields $\mathscr{A}_L$ is complete w.r.t the weak topology. $\square$

Proposition 4.1.5. *Restricting the weak topology on $\mathscr{A}_L$ to $\mathcal{O}[[X]]$, we obtain the product topology on $\mathcal{O}^{\mathbb{N}_0}$.*

Proof. The fundamental system around 0 in $\mathcal{O}[[X]]$ by the induced topology from $\mathscr{A}_L$ is

$$V_m := X^m \mathcal{O}[[X]] + \pi^m \mathcal{O}[[X]]$$

If we represent $f \in \mathcal{O}[[X]]$ as a sequence $(a_0, a_1, ...)$ by grading, then it is easy to see that

$$f + V_m = \{(b_0, b_1, ..., b_{m-1}, ...) \in \mathcal{O}^{\mathbb{N}_0} | b_i \equiv a_i \mod \pi^m, 0 \leq i \leq m-1\}$$

And this yields the topology on $\mathcal{O}[[X]]$ is the product topology on $\mathcal{O}^{\mathbb{N}_0}$. $\square$

With the weak topology, we can prove that

Lemma 4.1.6. *$\mathscr{A}_L$ is a topological ring w.r.t the weak topology.*

Proof. It is sufficient for us to prove that the multiplication map is continuous. Let $f, g \in \mathscr{A}_L$, and $m \geq 1$; then because the coefficients of f and g go to 0 when the indices go to $-\infty$, we can find some l such that $X^l f, X^l g \in \mathcal{O}[[X]] + \pi^m \mathscr{A}_L = U_{0,m}$. And we have

$$\begin{aligned}(f + U_{l+m,m})(g + U_{l+m,m}) &= fg + fU_{l+m,m} + gU_{l+m,m} + U_{l+m,m}U_{l+m,m} \\ &\subseteq fg + X^{-l} U_{0,m} U_{l+m,m} + U_m \subseteq fg + U_{0,m} U_m + U_m \subseteq fg + U_m\end{aligned}$$

$\square$

We conclude this section by proving that the action from φ_L and Γ_L is continuous w.r.t the weak topology.

Proposition 4.1.7. *The action from φ_L and Γ_L is continuous w.r.t the weak topology on $\mathscr{A}_L$*

Proof. Because $[\pi]_\phi = \phi(X) \in X\mathcal{O}[[X]]$, we have $\phi(X^m) \in X^m \mathcal{O}[[X]]$, and for any $f \in \mathscr{A}_L$, we have

$$\varphi_L(f + U_m) = \varphi_L(f + X^m \mathcal{O}[[X]] + \pi^m \mathscr{A}_L) \subseteq \varphi_L(f) + U_m$$

So, φ_L acts continuously on $\mathscr{A}_L$. For the action from Γ_L, we will sketch the proof, since $\Gamma_L \cong \mathcal{O}^\times$, it is sufficient to prove that the action $\mathcal{O}^\times \times \mathscr{A}_L \to \mathscr{A}_L$ is continuous. It then follows, by computing the degree, that for al $a \in \mathcal{O}^\times$, $f \in \mathscr{A}_L$ and there exists some $m(f)$ such that for all $b \in 1 + \pi^{m(f)}\mathcal{O}$, we have $(ab, f) \in (a, f + U_m)$, and since $(a, U_m) \subseteq U_m$ this yields

$$ab \times (f + U_m) = (ab, f) + (ab, U_m) \subseteq (a, f + U_m) + U_m \subseteq (a, f) + (a, U_m) + U_m \subseteq (a, f) + U_m$$

Hence, the action from Γ_L to $\mathscr{A}_L$ is also continuous. $\square$

4.2 The kernel of $\Theta_{\widehat{L_\infty}}$

This section has two aims. First, we will prove that there exists $c \in W(\mathcal{O}_{\widehat{L_\infty}^\flat})$, such that $\Theta_{\widehat{L_\infty}}(c) = 0$ and $|\Phi_0(c)| = |\pi|$. Note that this implies $\ker K = cW(\mathcal{O}_{K^\flat})$, for all perfectoid field K, as proved in Proposition 3.3.2. Via doing this, we will introduce the two important maps, so called lifts of Teichmuller map, and ι as introduced in the introduction of this chapter.

We will first begin with the construction of $\ker \Theta_{\mathbb{C}_p}$, and see how we can reduce to the case $\mathcal{O}_{\widehat{L_\infty}^\flat}$. Let us begin with a sequence $\pi_0 = \pi, \pi_{i+1}^q = \pi_i$, where $\pi_i \in \mathcal{O}_{\mathbb{C}_p}$. It can be seen that $(..., \pi_i \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., \pi_0 \mod \pi\mathcal{O}_{\mathbb{C}_p})$ defines an element in $\mathcal{O}_{\mathbb{C}_p^\flat}$. Let us denote this element as $\tilde{\pi}$. We have

$$\Theta_{\mathbb{C}_p}(\tau(\tilde{\pi})) = (\tilde{\pi})^\sharp = \lim_{i\to\infty} \pi_i^{q^i} = \pi$$

Hence, one has $\tau(\tilde{\pi}) - \pi 1_{W(\mathcal{O}_{\mathbb{C}_p^\flat})}$ is in the kernel of $\Theta_{\mathbb{C}_p}$. By abusing of notation, we often denote $\pi 1_{W(\mathcal{O}_{K^\flat})}$ as $\pi 1_W$ for a perfectoid field K. We have

$$\tau(\tilde{\pi}) - \pi 1_W = (\tilde{\pi}, 0, ..., 0) - (0, 1, ...) = (\tilde{\pi}, ...)$$

And $|\tilde{\pi}|_\flat = |\tilde{\pi}^\sharp| = |\pi|$. And this yields by Proposition 3.3.2 that $\tau(\tilde{\pi}) - \pi 1_W$ generates the kernel of $\Theta_{\mathbb{C}_p}$.

To reduce this construction to $\Theta_{\widehat{L_\infty}}$, we first note that $\widehat{L_\infty}^\flat = E_L^{\mathrm{perf}}$, but E_L itself is not perfect. So, if our construction begins from E_L, we will need to extend E_L to $E_L^{1/q^j} := \{\alpha \in \overline{E_L}, \alpha^{q^j} \in E_L\}$. We can see that E_L^{1/q^j} is an extension of E_L, with maximal ideal of $\mathcal{O}_{E_L^{1/q^j}}$ is $\mathfrak{m}_{E_L^{1/q^j}} = \{\alpha \in \mathcal{O}_{E_L^{1/q^j}}, \alpha^{q^j} \in \mathfrak{m}_{E_L}\}$, where $\mathfrak{m}_{E_L}$ is the maximal ideal of $\mathcal{O}_{E_L}$. Note that the Frobenius $x \mapsto x^q$ denote as $Fr : \mathcal{O}_{E_L^{1/q^{j+1}}} \to \mathcal{O}_{E_L^{1/q^j}}$ is now bijective, and the Frobenius on Witt vectors $Fr : W(\mathcal{O}_{E_L^{1/q^{j+1}}}) \to W(\mathcal{O}_{E_L^{1/q^j}})$ is also bijective. To find such an element generating $\ker \Theta_{\widehat{L_\infty}}$, we will also need the Lubin-Tate formal group, applying to the maximal ideal M_{E_L} of $W(\mathcal{O}_{E_L})$. To do this, we need to study further the topology on $W(\mathcal{O}_{\mathbb{C}_p^\flat})$.

Lemma 4.2.1. *Let K be a perfectoid field, $\alpha \in \mathcal{O}_{K^\flat}, \alpha \neq 0$, and $|\alpha|_\flat < 1$, then $(\tau(\alpha), \pi 1_W)^m$ forms a fundamental system of open neighborhoods in $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ w.r.t the weak topology.*

Proof. Because $(\tau(\alpha), \pi 1_W)^{2m} \subseteq (\tau(\alpha)^m, (\pi 1_W)^m) \subseteq (\tau(\alpha), \pi 1_W)^m$, it is sufficient to prove that $(\tau(\alpha)^m, \pi 1_W^m)$ forms such a fundamental system. Take any $(\alpha_0, \alpha_1, ..) \in W(\mathcal{O}_{K^\flat})$, we have

$$\tau(\alpha^m)(\alpha_0, \alpha_1, ..) + \pi^m W(\mathcal{O}_{K^\flat}) = \tau(\alpha)^m(\tau(\alpha_0) + \pi\tau(\alpha_1^{1/q}) + ... + \tau(\alpha_{m-1}^{1/q^{m-1}}) + V_m(\mathcal{O}_{K^\flat}) =$$

$$= \tau(\alpha^m\alpha_0) + \tau(\alpha^{mq}\alpha_1) + ... + \tau(\alpha^{mq^{m-1}}\alpha_{m-1}) + V_m(\mathcal{O}_{K^\flat})$$

And this yields

$$(\tau(\alpha^m), (\pi 1_W)^m) = \alpha^m\mathcal{O}_{K^\flat} \times \alpha^{mq}\mathcal{O}_{K^\flat} \times ... \times \alpha^{mq^{m-1}}\mathcal{O}_{K^\flat} \times \mathcal{O}_{K^\flat} \times \mathcal{O}_{K^\flat}...$$

From this, we obtain

$$V_{\alpha^{mq^{m-1}},m} \subseteq (\tau(\alpha)^m, (\pi 1_W)^m) \subseteq V_{\alpha^m,m}$$

where $V_{\mathfrak{a},m}$ is defined as in Section 6 of Chapter II. And it follows that $(\tau(\alpha^m), \pi 1_W^m)$ forms such a fundamental system. ☐

Via this lemma, we have

Lemma 4.2.2. *Let K be as above, and $\alpha \in W(\mathcal{O}_{K^\flat})$, such that $0 \leq |\Phi_0(\alpha)| < 1$, then $(\alpha, \pi 1_W)^m$ forms a fundamenal system of open neighborhoods around 0 in $W(\mathcal{O}_{K^\flat})$, w.r.t the weak topology*

Proof. We assume that $a = \Phi_0(\alpha)$, then it follows from the previous lemma that $(\tau(a), \pi 1_W)^m$ forms such a fundamental system. But then

$$\alpha - \tau(a) = (0, ...) \in \pi 1_W(\mathcal{O}_{K^\flat})$$

So, $(\alpha, \pi 1_W) = (\tau(a), \pi 1_W)$, and the conclusion now follows. □

We next consider the map $\Phi_0 : W(\mathcal{O}_{E_L}) \to \mathcal{O}_{E_L}$, it is a homomorphism of ring, and $M_{E_L} := \Phi_0^{-1}(\mathfrak{m}_{E_L}) = \{(a_0, a_1, ...) \in W(\mathcal{O}_{E_L}) | a_0 \in \mathfrak{m}_{E_L}\}$ is a maximal ideal of $W(\mathcal{O}_{E_L})$. And one of our main goals is to consider the topology on M_{E_L}. First, we can equip $W(\mathcal{O}_{E_L})$ the product topology on each factor $\mathcal{O}_{E_L}$, and this yields $W(\mathcal{O}_{E_L}) \subset W(\mathcal{O}_{\mathbb{C}_p^\flat})$ is Hausdorff, and complete (Proposition 2.6.2). Due to the characterization of M_{E_L}, it is also closed in $W(\mathcal{O}_{E_L})$, and hence, complete, w.r.t the weak topology.

Corollary 4.2.3. *With respect to the weak topology, any $\alpha \in M_{E_L}$ is topological nilpotent, i.e.* $\lim_{i\to\infty} \alpha^n = 0$

Proof. If $\alpha = 0$, then the conclusion is trivial. Otherwise, by Lemma 4.2.1, we have $(\alpha, \pi 1_W)^m$ forms a fundamental system around 0 in $W(\mathcal{O}_{\mathbb{C}_p^\flat})$, and hence, $(\alpha^n)_n$ forms a Cauchy sequence in $W(\mathcal{O}_{\mathbb{C}_p^\flat})$. It is obvious to see that 0 is a convergent value for $(\alpha^n)_n$. But then, since $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ is Hausdorff, the convergent value is unique, and we conclude that $\lim_{i\to\infty} \alpha^n = 0$. □

Now, let $F := F_\phi$ the Lubin-Tate formal group law w.r.t ϕ. Because M_{E_L} is Hausdorff, complete, and any $\alpha \in M_{E_L}$ is topological nilpotent, we have $(M_{E_L}, +_F)$ is an abelian group. We can then define the action

$$\begin{aligned} \mathcal{O} \times M_{E_L} &\longrightarrow M_{E_L} \\ (a, \alpha) &\longmapsto [a]_\phi(\alpha) \end{aligned}$$

And this turns M_{E_L} into an $\mathcal{O}$-module. Because $E_L \subseteq E_L^{1/q^j} \subset \widehat{L_\infty}^\flat$, we can immitate these constructions above for E_L^{1/q^j}. In particular, we define

$$\begin{aligned} M_{E_L^{1/q^j}} = \Phi_0^{-1}(\mathfrak{m}_{E_L^{1/q^j}}) &= \{(\alpha_0, \alpha_1, ...) \in W(\mathcal{O}_{E_L^{1/q^j}}), \alpha_0 \in \mathfrak{m}_{E_L^{1/q^j}}\} \\ &= \{(\alpha_0, \alpha_1, ...), \alpha_0^{q^j} \in \mathfrak{m}_{E_L}\} = (Fr^i)^{-1}(M_{E_L}) \end{aligned} \tag{4.1}$$

Also, $(M_{E_L^{1/q^j}}, +_F)$ is an $\mathcal{O}$-module. And we have

$$\pi^j W(\mathcal{O}_{E_L^{1/q^j}}) = \{\pi^j(a_0, a_1, ...), a_i^{q^j} \in \mathcal{O}_{E_L}\} = \{(0, ..., 0, a_0^{q^j}, a_1^{q^j}, ...\} = V_j(\mathcal{O}_{E_L}) \tag{4.2}$$

Lemma 4.2.4. *The map $[\pi]_\phi : M_{E_L^{1/q}} \to M_{E_L}$ is well-defined, and $[\pi]_\phi$ is a homomorphism of $\mathcal{O}$-modules.*

Proof. Take any $\alpha \in M_{E_L^{1/q}}$, we have $\alpha^q \in M_{E_L}$, and $\pi\alpha = (0, \alpha_0^q, ...) \in V_1(\mathcal{O}_{E_L}) \subset M_{E_L}$. Hence,

$$[\pi]_\phi(\alpha) = \alpha^q + \pi G(\alpha) = \alpha^q + \pi\beta \in M_{E_L}$$

where $[\pi]_\phi = X^q + \pi G(X) \in \mathcal{O}[[X]]$, and $\beta = G(\alpha) \in M_{E_L^{1/q}}$ □

By the previous lemma, and 4.1, we obtain

$$M_{E_L} \xrightarrow{[\pi]_\phi \circ Fr^{-1}} M_{E_L}$$

is well-defined. We will show that it is in fact an $\mathcal{O}$-module homomorphism.

Lemma 4.2.5. *The maps $Fr : M_{E_L^{1/q}} \to M_{E_L}$, and $Fr^{-1} : M_{E_L} \to M_{E_L^{1/q}}$ are isomorphism of $\mathcal{O}$-modules.*

Proof. We will prove for Fr^{-1}, and because Fr and Fr^{-1} are inverse of each other, this automatically turns out that Fr is an isomorphism, too. Assume that $F(X,Y) = F_\phi(X,Y) = \sum_{r,s} c_{r,s}X^rY^s$, we have

$$F(Fr^{-1}(\alpha), Fr^{-1}(\beta)) = \sum_{r,s} c_{r,s}Fr^{-1}(\alpha)^r Fr^{-1}(\alpha)^s = \sum_{r,s} c_{r,s}Fr^{-1}(\alpha^r\beta^s)$$

$$= \sum_{r,s} Fr^{-1}(c_{r,s}\alpha^r\beta^s) = Fr^{-1}\Big(\sum_{r,s} c_{r,s}\alpha^r\beta^s\Big) = Fr^{-1}(F(\alpha,\beta))$$

where the third identity follows from the fact that $Fr^{-1} : W(\mathcal{O}_{E_L^{1/q}}) \to W(\mathcal{O}_{E_L})$ is an $\mathcal{O}$-algebra homomorphism, and the fourth identity follows from the fact that the map $Fr : \mathcal{O}_{\mathbb{C}_p^\flat} \to \mathcal{O}_{\mathbb{C}_p^\flat}$ is an homeomorphism, and so is the map $W(Fr) = Fr : W(\mathcal{O}_{\mathbb{C}_p^\flat}) \to W(\mathcal{O}_{\mathbb{C}_p^\flat})$, and in particular, Fr is continuous.

Also, if we assume $[a]_\phi = a_1X + a_2X^2 + ...$, then

$$Fr^{-1}([a]_\phi(\alpha)) = Fr^{-1}(a_1\alpha + a_2\alpha^2 + ...) = a_1Fr^{-1}(\alpha) + a_2Fr^{-1}(\alpha)^2 + ... = [a]_\phi(Fr^{-1}(\alpha))$$

And this yields Fr^{-1} is an $\mathcal{O}$-module homomorphism. Because Fr^{-1} is also bijective, it is an $\mathcal{O}$-module isomorphism. □

By combining Lemma 4.2.4, and Lemma 4.2.5, we get

$$[\pi]_\phi \circ Fr^{-1} : M_{E_L} \to M_{E_L}$$

is an $\mathcal{O}$-module homomorphism. We denote this map as $\{.\}_1$. Here are some facts about $\{.\}_1$.

Lemma 4.2.6. *For all $\alpha, \beta \in M_{E_L}$, we have*

(i) $\{\alpha\}_1 \equiv \alpha \mod V_1(\mathcal{O}_{E_L})$.

(ii) If $\alpha \equiv \beta \mod V_i(\mathcal{O}_{E_L})$, *then* $\{\alpha\}_1 \equiv \{\beta\}_1 \mod V_{i+1}(\mathcal{O}_{E_L})$.

(iii) $\{\}_1^{i+1}(\alpha) \equiv \{\}_1^i(\alpha) \mod V_{i+1}(\mathcal{O}_{E_L})$.

Proof.

(i) We can represent $[\pi]_\phi(X) = X^q + \pi G(X)$ for some $G(X) \in X\mathcal{O}[[X]]$, and this yields

$$\{\alpha\}_1 = [\pi]_\phi \circ Fr^{-1}(\alpha) = [\pi]_\phi(\alpha^{1/q}) = (\alpha^{1/q})^q + \pi G(\alpha^{1/q}) \equiv \alpha \mod V_1(\mathcal{O}_{E_L})$$

(ii) Due to 4.2, we have $V_i(\mathcal{O}_{E_L}) = \pi^i W(\mathcal{O}_{E_L^{1/q^i}})$. From the assumption $\alpha \equiv \beta \mod V_i(\mathcal{O}_{E_L})$, we have $\alpha \equiv \beta \mod \pi^i W(\mathcal{O}_{E_L^{1/q^i}})$, and that $Fr^{-1}(\alpha) \equiv Fr^{-1}(\beta) \mod \pi^i W(\mathcal{O}_{E_L^{1/q^{i+1}}})$. And hence, it is sufficient to prove for any $\alpha, \beta \in W(\mathcal{O}_{E_L^{1/q^{i+1}}})$, if $\alpha \equiv \beta \mod \pi^i$, then $[\pi]_\phi(\alpha) \equiv [\pi]_\phi(\beta) \mod \pi^{i+1}$. But it is clear, since $[\pi]_\phi(X) = X^q + \pi G(X)$, and we easily get $\alpha^q \equiv \beta^q \mod \pi^{i+1}$, and $\pi(G(\alpha) - G(\beta)) \equiv 0 \mod \pi^{i+1}$.

(iii) By (i), we have $\{\alpha\}_1 \equiv \alpha \mod V_1(\mathcal{O}_{E_L})$, and by (ii), $\{\{\alpha\}_1\}_1 \equiv \{\alpha\}_1 \mod V_2(\mathcal{O}_{E_L})$. So by induction, we get $\{\}_1^{i+1}(\alpha) \equiv \{\}_1^i(\alpha) \mod V_{i+1}(\mathcal{O}_{E_L})$.

□

Due to (iii) of the lemma above, for any $\alpha \in M_{E_L}$, we have $(\{\}_1^n(\alpha))_n$ forms a Cauchy sequence in the π-adic topology of $W(\mathcal{O}_{\mathbb{C}_p^\flat})$, and hence it is also a Cauchy sequence in the weak topology on M_{E_L}, which is Hausdorff and complete. Hence, we can define

$$\{\alpha\} := \lim_{i\to\infty} \{\}_1^i(\alpha) \in M_{E_L}$$

There is an useful characterization of $\{.\}$.

Lemma 4.2.7.

(i) $\{.\} : M_{E_L} \to M_{E_L}$ *is an* $\mathcal{O}$*-module homomorphism.*

(ii) For $\alpha \in M_{E_L}$, $\{\alpha\}$ *is the unique element such that* $\{\alpha\} \equiv \alpha \mod V_1(\mathcal{O}_{E_L})$ *and* $[\pi]_\phi(\{\alpha\}) = Fr(\{\alpha\})$

Proof.

1. Let $\alpha, \beta \in M_{E_L}$, we have

   $$\{\alpha +_F \beta\} = \lim_{n\to\infty} \{\}_1^n(\alpha +_F \beta) = \lim_{n\to\infty} (\{\}_1^n(\alpha) +_F \{\}_1^n(\beta)) = \lim_{n\to\infty} \{\}_1^n(\alpha) +_F \lim_{n\to\infty} \{\}_1^n(\beta) = \{\alpha\} +_F \{\beta\}$$

   Also, for any $a \in \mathcal{O}$, we have

   $$\{[a]_\phi(\alpha)\} = \lim_{n\to\infty} ([\pi]_\phi \circ Fr^{-1}) \circ \ldots \circ ([\pi]_\phi \circ Fr^{-1})([a]_\phi(\alpha)) = \lim_{n\to\infty} [a]_\phi \{\}_1^n(\alpha) = [a]_\phi \lim_{n\to\infty} \{\}_1^n(\alpha) = [a]_\phi\{\alpha\}$$

   where the second identity follows from the fact that $[a]_\phi$ commutes with $[\pi]_\phi$ and Fr^{-1} (Lemma 4.2.5). And hence $\{.\}$ is a homomorphism of $\mathcal{O}$-module.

2. It can be seen by Lemma 4.2.6 that

   $$\{\alpha\} \equiv \{\alpha\}_1 \equiv \alpha \mod V_1(\mathcal{O}_{E_L})$$

   Also, we have

   $$Fr \circ \{\}_1^n(\alpha) = Fr \circ ([\pi]_\phi \circ Fr^{-1}) \circ \ldots \circ ([\pi]_\phi \circ Fr^{-1})(\alpha) = [\pi]_\phi(\{\}_1^{n-1}(\alpha))$$

   And because Fr and $[\pi]_\phi$ commute with the limit, we have

   $$\lim_{n\to\infty} Fr(\{\}_1^n(\alpha)) = Fr(\lim_{n\to\infty} \{\}_1^n(\alpha)) = Fr(\{\alpha\})$$

   And

   $$\lim_{n\to\infty} [\pi]_\phi(\{\}_1^{n-1}(\alpha)) = [\pi]_\phi \lim_{n\to\infty} \{\}_1^n(\alpha) = [\pi]_\phi(\{\alpha\})$$

   This implies $[\pi]_\phi(\{\alpha\}) = Fr(\{\alpha\})$. For the uniqueness, assume that there exists $\beta_1, \beta_2 \in M_{E_L}$ such that $\beta_1 \equiv \beta_2 \mod V_1(\mathcal{O}_{E_L})$, and $[\pi]_\phi(\beta_j) = Fr(\beta_j)$. This yields $[\pi]_\phi \circ Fr^{-1}(\beta_j) = \beta_j$, i.e. $\{\beta_j\}_1 \equiv \beta_j$. Because $\beta_1 \equiv \beta_2 \mod V_1(\mathcal{O}_{E_L})$, we have $\{\beta_1\}_1 \equiv \{\beta_2\}_1 \mod V_2(\mathcal{O}_{E_L})$, i.e. $\beta_1 \equiv \beta_2 \mod V_2(\mathcal{O}_{E_L})$, and so on. We finally get $\beta_1 \equiv \beta_2 \mod V_i(\mathcal{O}_{E_L})$, for all i, and hence, $\beta_1 = \beta_2$.

□

Via this lemma, we get that if $\beta \in M_{E_L}$, such that $\beta \equiv \alpha \mod V_1(\mathcal{O}_{E_L})$, and $[\pi]_\phi(\beta) = Fr(\beta)$, then $\beta = \{\alpha\}$, say another words, $\{.\}$ is completely determined by modulo $V_1(\mathcal{O}_{E_L})$. As a corollary, we get

Corollary 4.2.8. *For all $\alpha \in M_{E_L}$, we have $\{\alpha\} = \{\tau(\Phi_0(\alpha))\}$*

Proof. We have $\{\tau(\Phi_0(\alpha))\} \equiv \tau(\Phi_0(\alpha)) \equiv \alpha \mod V_1(\mathcal{O}_{E_L})$. And because $\beta := \{\tau(\Phi_0(\alpha))\}$ satisfies $[\pi]_\phi(\beta) = Fr(\beta)$, we obtain the statement by Lemma 4.2.7 (ii). $\square$

We now introduce the two important maps

$$\tau_\phi : \mathfrak{m}_{E_L} \xrightarrow{\tau} M_{E_L} \xrightarrow{\{\}} M_{E_L}$$

$$\iota_\phi : T \xrightarrow{\iota} \mathfrak{m}_{E_L} \xrightarrow{\tau_\phi} M_{E_L}$$

The map τ_ϕ is obviously well-defined, since $M_{E_L} = \Phi_0^{-1}(\mathfrak{m}_{E_L})$. And since T is mapped to $\mathfrak{m}_{E_L}$ via ι, the second map is also well-defined. And the connections between τ_ϕ, ι_ϕ and $\Theta_{\mathbb{C}_p}$ are reflected via the following

Lemma 4.2.9. *For any $\alpha \in \mathfrak{m}_{E_L}$, we have*

$$\Theta_{\mathbb{C}_p}(\tau_\phi(a)) = \lim_{i\to\infty} [\pi^i]_\phi(a_i)$$

where $a = (..., a_i \mod \pi\mathcal{O}_{\mathbb{C}_p}, ..., a_0 \mod \pi\mathcal{O}_{\mathbb{C}_p})$. In particular, $\Theta_{\mathbb{C}_p}(\iota_\phi(t)) = \Theta_{\mathbb{C}_p}(\tau_\phi(\omega))$ where $t = (z_n)_n$ is the generator for the Tate module, and $\omega = \iota((z_n)_n)$

Proof. Because $\Theta_{\mathbb{C}_p}$ is continuous (Lemma 3.5.8), we have

$$\Theta_{\mathbb{C}_p}(\tau_\phi(a)) = \Theta_{\mathbb{C}_p}(\{\tau(a)\}) = \Theta_{\mathbb{C}_p}(\lim_{i\to\infty}[\pi^i]_\phi Fr^{-i}(\tau(a))) = \lim_{i\to\infty} \Theta_{\mathbb{C}_p}([\pi^i]_\phi Fr^{-i}(\tau(a)))$$

And we have

$$[\pi^i]_\phi \circ Fr^{-i}(\tau(a)) = [\pi^i]_\phi((..., a_{i+1} \mod \pi\mathcal{O}_{\mathbb{C}_p}, a_i \mod \pi\mathcal{O}_{\mathbb{C}_p}), 0, 0, ...) = [\pi^i]_\phi(\tau(a^{1/q^i}))$$

And because $\Theta_{\mathbb{C}_p}$ is also an $\mathcal{O}$-algebra homomorphism, we have

$$\Theta_{\mathbb{C}_p}([\pi^i]_\phi(\tau(a^{1/q^i}))) = [\pi^i]_\phi(\Theta_{\mathbb{C}_p}(\tau(a^{1/q^i}))) = [\pi^i]_\phi((a^{1/q^i})^\sharp)$$

We have $(a^{1/q^i})^\sharp \equiv a_i \mod \pi\mathcal{O}_{\mathbb{C}_p}$, and hence $[\pi]_\phi((a^{1/q^i})^\sharp) \equiv [\pi]_\phi(a_i) \mod \pi^2\mathcal{O}_{\mathbb{C}_p}$. Inductively, we get in general $[\pi^i]_\phi((a^{1/q^i})^\sharp) \equiv [\pi^i]_\phi(a_i) \mod \pi^{i+1}\mathcal{O}_{\mathbb{C}_p}$. And this yields

$$\Theta_{\mathbb{C}_p}(\tau_\phi(a)) = \lim_{i\to\infty} \Theta_{\mathbb{C}_p}([\pi^i]_\phi(\tau(a^{1/q^i}))) = \lim_{i\to\infty}[\pi^i]_\phi((a^{1/q^i})^\sharp) = \lim_{i\to\infty}[\pi^i]_\phi(a_i)$$

Because for all i, we have $[\pi^i]_\phi(z_i) = 0$, and $\iota_\phi(t) = \tau_\phi(\omega)$. And this follows from the previous computation that

$$\Theta_{\mathbb{C}_p}(\iota_\phi(t)) = \Theta_{\mathbb{C}_p}(\tau_\phi(\omega)) = \lim_{i\to\infty}[\pi^i]_\phi(z_i) = 0$$

$\square$

We note that $\tau_\phi(\omega) \in \widehat{L_\infty}^\flat$, so we have actually found an element $\tau_\phi(\omega)$ such that $\Theta_{\widehat{L_\infty}}(\tau_\phi(\omega)) = 0$. Furthermore, $\tau_\phi(\omega) = \{\tau(\omega)\} \equiv \tau(\omega) \mod V_1(\mathcal{O}_{E_L})$, so both $\tau_\phi(\omega)$ and $\tau(\omega)$ has the same 0-th coordinate, which is ω. And it follows from Lemma 3.2.6 that

$$|\omega|_\flat = \lim_{i\to\infty}|z_i|^{q^i} = \pi^{q/q-1}$$

And we want to adjust this absolute value. So it is natural to consider $\tau_\phi(\omega^{1/q})$. We have

Lemma 4.2.10.

(i) $[\pi]_\phi(\tau_\phi(\omega^{1/q})) = \tau_\phi(\omega)$.

(ii) $\tau_\phi(\omega)/\tau_\phi(\omega^{1/q}) \in \mathcal{O}_{E_L^{1/q}}$.

Proof.

(i) We have $[\pi]_\phi(\tau_\phi(\omega^{1/q})) = [\pi]_\phi\{\tau(\omega^{1/q})\} = \{[\pi]_\phi(\tau(\omega^{1/q}))\}$, and

$$\{[\pi]_\phi(\tau(\omega^{1/q}))\} \equiv [\pi]_\phi(\tau(\omega^{1/q})) \equiv \tau(\omega^{1/q})^q \equiv \tau(\omega) \mod V_1(\mathcal{O}_{E_L})$$

Since $\{\tau(\omega)\} = \tau_\phi(\omega)$, by Lemma 4.2.7, we get the conclusion.

(ii) This follows directly from (i), since $[\pi]_\phi(X) \in X\mathcal{O}[[X]]$.

□

And it is easy for now to prove that

Corollary 4.2.11. *$c := \tau_\phi(\omega)/\tau_\phi(\omega^{1/q})$ satisfies $\Theta_{\widehat{L_\infty}}(c) = 0$, and $|\Phi_0(c)|_\flat = |\pi|$.*

Proof. We have $\Theta_{\mathbb{C}_p}(c).\Theta_{\mathbb{C}_p}(\tau_\phi(\omega^{1/q})) = 0$, by Lemma 4.2.9, but then

$$\Theta_{\mathbb{C}_p}(\tau_\phi(\omega^{1/q})) = \lim_{i\to\infty} [\pi^i]_\phi(z_{i+1}) = z_1$$

And $z_1 \neq 0$, we so obtain $\Theta_{\mathbb{C}_p}(c) = \Theta_{\widehat{L_\infty}}(c) = 0$. On the other hand, $\{\tau(\omega^{1/q})\} \equiv \tau(\omega^{1/q}) \mod V_1(\mathcal{O}_{E_L})$, so they have the same 0-th coordinate, which is $(...., z_1 \mod \pi\mathcal{O}_{\mathbb{C}_p})$. And that $|\omega^{1/q}|_\flat = |z_1| = |\pi|^{1/q-1}$. So, we get $|\Phi_0(c)|_\flat = |\pi|$. □

Via this proof, we now obtain the complete proof for our tilting correspondences in the previous chapter.

4.3 The coefficient ring

We can now describe a topological embedding from $\mathscr{A}_L$ to $W(E_L)$. We first prove that

Lemma 4.3.1.

(i) The diagam below is commutative.

$$\begin{tikzcd} & M_{E_L} \arrow[dd, "\Phi_0"] \\ T \arrow[ur, "\iota_\phi"] \arrow[dr, "\iota"'] & \\ & \mathfrak{m}_{E_L} \end{tikzcd}$$

(ii) For all $a \in \mathcal{O}$, and $y \in T$, we have

$$[a]_\phi(\iota_\phi(y)) = \iota_\phi([a]_\phi(y)) \text{ and } Fr(\tau_\phi(y)) = [\pi]_\phi(\iota_\phi(y))$$

Proof.

(i) The commutativity of the diagram above is equivalent to say that the 0-th coordinate of $\iota_\phi(y)$ is $\iota(y)$. We have $\iota_\phi(y) = \tau_\phi(\iota(y)) = \{\tau(\iota(y))\} \equiv \tau(\iota(y)) \mod V_1(\mathcal{O}_{E_L})$, and this yields the 0-th coordinate of $\iota_\phi(y)$ and $\tau(\iota(y))$ is the same. But then $\tau(\iota(y)) = (\iota(y), 0, ...)$, and hence, the 0-th coordinate of $\iota_\phi(y)$ is exactly $\iota(y)$.

(ii) For the first equality, we have

$$[a]_\phi(\iota_\phi(y)) = [a]_\phi(\{\tau(\iota(y))\}) = \{[a]_\phi(\tau(\iota(y)))\}$$

where the last identity follows from the proof of Lemma 4.2.7 (i). And

$$\iota_\phi([a]_\phi(y)) = \{\tau(\iota([a]_\phi(y)))\}$$

And it is sufficient to prove that the two elements in $\{.\}$ above has the same 0-th coordinate. For the first element, we have its 0-th coordinate is the 0-the coordinate of $[a]_\phi(\tau(\iota(y))) = [a]_\phi(\iota(y), 0, 0, ...)$. And for the second element, its 0-th coordinate is the 0-th coordinate of $\tau(\iota([a]_\phi(y)))$, which is $\iota([a]_\phi(y))$. But then, since things we are considering are in the maximal ideal M_{E_L}, where series converge, so $\iota([a]_\phi(y)) = [a]_\phi \iota(y)$. And this also follows easily that the 0-th coordinate of the first element is also $[a]_\phi \iota(y)$.

For the second identity, we have

$$Fr(\iota_\phi(y)) = Fr(\{\tau(\iota(y))\}) = [\pi]_\phi(\{\tau(\iota(y))\}) = [\pi]_\phi(\iota_\phi(y))$$

where the second identity follows from Lemma 4.2.7 (ii).

□

Let us denote $\omega_\phi := \iota_\phi(t)$, where t is a generator for the Tate module. We can extend ι_ϕ to the map

$$\begin{aligned} \mathcal{O}[[X]] &\longrightarrow W(\mathcal{O}_{E_L}) \\ f(X) &\longmapsto f(\omega_\phi) \end{aligned}$$

Because $\omega_\phi \in M_{E_L}$, which is topological nilpotent, the map above is a well-defined $\mathcal{O}$-algebra homomorphism, and it makes the diagram

$$\begin{tikzcd} \mathcal{O}[[X]] \arrow[r] \arrow[d, "\mathrm{pr}"] & W(\mathcal{O}_{E_L}) \arrow[d, "\Phi_0"] \\ k[[X]] \arrow[r, "\sim"] & \mathcal{O}_{E_L} \end{tikzcd}$$

commute by Lemma 4.3.1(i). Because $W(E_L)$ is a local domain, since E_L is a field extension of k, with the unique maximal ideal $V_1(E_L) = \ker \phi_0$, and X is mapped to $\omega_\phi = \iota_\phi(t)$, that satisfies $\Phi_0(\omega_\phi) = \omega \neq 0$. So ω_ϕ is invertible in $W(E_L)$. And hence, the diagram above can be extended to

$$\begin{tikzcd} \mathcal{O}((X)) \arrow[r] \arrow[d, "\mathrm{pr}"] & W(E_L) \arrow[d, "\Phi_0"] \\ k((X)) \arrow[r, "\sim"] & E_L \end{tikzcd}$$

And that $\pi^m f(X)$ in $\mathcal{O}((X))$ is mapped to $\pi^m f(\omega_\phi)$ in $W(E_L)$. So the induced map

$$\mathcal{O}((X))/\pi^m\mathcal{O}((X)) \to W(E_L)/\pi^m W(E_L)$$

is well-defined, and compatible with the inverse system. So, we obtain the map

$$\begin{aligned} j : \mathscr{A}_L = \varprojlim_m \mathcal{O}((X))/\pi^m\mathcal{O}((X)) &\longrightarrow \varprojlim_m W(E_L)/\pi^m W(E_L) = W(E_L) \\ X &\longmapsto \omega_\phi \end{aligned}$$

We recall that $\mathscr{A}_L$ is a D.V.R with the the unique maximal ideal generated by π, so the kernel of j is either 0 of $\pi^m\mathscr{A}_L$. If the latter case occurs, we have $j(\pi^m) = 0 = \pi^m 1_W$, which is absurd. Hence j is an embedding. Actually, j is a topological embedding w.r.t the weak topology on both $\mathscr{A}_L$ and $W(E_L)$ [Sch17](Proposition 2.1.16(i)). We denote the image of j as A_L. We will conclude this section by proving the compatibility between (ϕ_L, Γ_L) action on $\mathscr{A}_L$ and (Fr, Γ_L) actions on A_L. At this point, we recall that any $\sigma \in G_L = \mathrm{Gal}(\overline{\mathbb{Q}_p}/L)$ acts continuously on $\widehat{L_\infty}^\flat$ and $H_L = \mathrm{Gal}(\overline{\mathbb{Q}_p}/L_\infty)$ fixes L_∞, and hence, fixes $\widehat{L_\infty}^\flat$. So, this action is reduced to Γ_L. And the induced action from Γ_L to $W(\widehat{L_\infty}^\flat)$ is defined on each coordinate, which turns out to be continuous as the following lemma points out.

Lemma 4.3.2. *The action from Γ_L to $W(\widehat{L_\infty}^\flat)$ is also continuous.*

Proof. Note that Γ_L is a profinite group, that acts on $\widehat{L_\infty}^\flat$ as automorphisms of $\mathcal{O}$-algebra, and this action is continuous. This then follows by Lemma 3.5.6 that Γ_L acts continuously on $W(\mathcal{O}_{\widehat{L_\infty}^\flat})$. We also recall that due to the notions of Section 6, Chapter II about topology on Witt vectors

$$U_{\mathfrak{a},m} = V_{\mathfrak{a},m} + \pi^m W(\widehat{L_\infty}^\flat)$$

where $\mathfrak{a}$ is an open ideal of $\mathcal{O}_{\widehat{L_\infty}^\flat}$, forms a fundamental system in $W(\widehat{L_\infty}^\flat)$, and that for any $\sigma \in \Gamma_L$, we have $\sigma(\pi^m W(\widehat{L_\infty}^\flat)) = \pi^m W(\widehat{L_\infty}^\flat)$. Hence, Γ_L acts continuously on $W(\widehat{L_\infty}^\flat)$. □

Proposition 4.3.3. *For all $f \in \mathscr{A}_L$, $\gamma \in \Gamma_L$, we have*
(i) $j(\varphi_L(f)) = Fr(j(f))$
(ii) $j(\gamma(f)) = \gamma(j(f))$

Proof. Assume that $f = f = \sum_{i\in\mathbb{Z}} a_i X^i$ with $\lim_{i\to-\infty} = 0$, then for all $m \geq 1$, there exists some n_m such that for all $n \leq n_m$, $a_n \equiv 0 \mod \pi^m$. We can define $f_m := \sum_{i\leq n_m}^{m-1}$. Then it can be seen that $f - f_m = \sum_{i<n_m} a_i X_i + \sum_{j\geq m} a_j X^j \in U_m$, where we recall that $U_m = X^m\mathcal{O}[[X]] + \pi^m\mathscr{A}_L$. Because $\mathscr{A}_L$ is Hausdorff, we have $\lim m f_m = 0$, where $f_m \in \mathcal{O}[[X, X^{-1}]]$. Also, since all maps we are considering are continuous, it is sufficient to prove both statements for $f \in \mathcal{O}[X, X^{-1}]$. But then, because all the maps are also $\mathcal{O}$-algebre homomorphism, it is sufficient to check for $f = X$. And the statements are now reduced to

(i) $j(\varphi_L(X)) = Fr(j(X))$.
(ii) $j(\gamma(X)) = \gamma(j(X))$.

For (i), we have $j(X) = \omega_\phi = \iota_\phi(t)$ and $\phi_L(X) = [\pi]_\phi(X)$, so it is equivalent to say

$$[\pi]_\phi(\iota_\phi(t)) = Fr(\iota_\phi(X))$$

which holds due to Lemma 4.3.1 (i). It is a little more difficult to prove (ii). We have

$$j(\gamma(X)) = j([\chi(\gamma)]_\phi(X)) = [\chi(\gamma)]_\phi(j(X)) = [\chi(\gamma)]_\phi(\iota_\phi(t)) = \iota_\phi([\chi(\gamma)]_\phi(t)) = \iota_\phi(\gamma(t))$$

where the fourth identity follows from the action from Γ_L to T. So it is now sufficient to prove that $\iota_\phi(\gamma(t)) = \gamma(\iota_\phi(t))$. Because ι_ϕ is the composition of τ, ι and $\{.\}$, it is sufficient to check that the three maps is Γ_L-equivariant. For both τ, ι, this follows directly from the definitions of the actions. For $\{.\}$, by Lemma 4.3.2, Γ_L acts continously, hence, it is sufficient to check that $[\pi]_\phi : M_{E_L^{1/q}} \to M_{E_L}$ and $Fr^{-1} : M_{E_L} \to M_{E_L^{1/q}}$ are Γ_L-equivariant. But this is also clear, since Γ_L acts continuously, we then deduce the statement for $[\pi]_\phi$. And for Fr^{-1}, it follows from the fact that $Fr : W(\mathcal{O}_{\mathbb{C}_p^\flat}) \to W(\mathcal{O}_{\mathbb{C}_p^\flat})$ is Γ_L-equivariant. □

4.4 (φ_L, Γ_L)-modules

Because $\mathscr{A}_L \cong A_L$ as topological rings, we can study the topology on A_L via $\mathscr{A}_L$. We recall that a fundamental system of open neighborhoods around 0 in $\mathscr{A}_L$ is given by

$$U_{l,m} = X^l \mathcal{O}[[X]] + \pi^m \mathscr{A}_L (l \geq 0, m \geq 1)$$

There is another characterization of $U_{l,m}$

Lemma 4.4.1. $U_{l,m} = \{f = \sum_{i \in \mathbb{Z}} a_i X^i \in \mathscr{A}_L, a_i \equiv 0 \mod \pi^m, \forall i < l\}$.

Proof. Assume that $f = f = \sum_{i \in \mathbb{Z}} a_i X^i$ satisfies $a_i \equiv 0 \mod \pi^m$, for all $i < l$, we can write

$$f = \sum_{i<l} a_i X^i + \sum_{j \geq l} a_j X^j \in U_{l,m}$$

Conversely, let $f = f = \sum_{i \in \mathbb{Z}} a_i X^i \in U_{l,m}$, we can represent

$$f = X^l g(X) + \pi^m h(X)$$

for $g \in \mathcal{O}[[X]], h \in \mathscr{A}_L$. And this yields the part of degree smaller than l of f is the part of degree $< l$ of $\pi^m h(X)$, and this implies $a_i \equiv 0 \mod \pi^m$ for all $i < l$. We therefore obtain the statement. □

Via this characterization, we can see

Lemma 4.4.2. *Let $f = f = \sum_{i \in \mathbb{Z}} a_i X^i, g = \sum_{i \in \mathbb{Z}} b_i X^i$ in $\mathscr{A}_L$, then $f \equiv g \mod U_{l,m}$ iff $a_i \equiv b_i \mod \pi^m$, for all $i < m$.*

Proof. It is obvious from the previous lemma. □

Lemma 4.4.3. *Let R be a commutative ring, we have*

$$R((X)) \cong \varprojlim_l R((X))/X^l R[[X]]$$

as $R[[X]]$-modules.

Proof. We can see that the map

$$\begin{aligned} R((X)) &\longrightarrow \varprojlim_l R((X))/X^l R[[X]] \\ f &\longmapsto (f \mod X^l R[[X]])_l \end{aligned}$$

is a well-defined $R[[X]]$-module homomorphism. So $f \in R((X))$ maps to 0 in the limit iff $f \in X^l R[[X]]$ for all $l \geq 0$. And this yields $f = 0$.

For the surjectivity, take any $(f_l)_l \in \varprojlim_l R((X))/X^l R[[X]]$, then $f_{l+1} \equiv f_l \mod X^l R[[X]]$, for all l, i.e. f_l and f_{l+1} has the same part of deree less than l. Hence, for any l, we can define $F_l := f_l - f_0$. It can be seen that $F_l \in R[[X]]$, and $F_{l+1} - F_l \in X^l R[[X]]$. Hence $\lim_{l \to \infty} F_l$ exists in $R[[X]]$, which is denoted F. Let $f := F + f_0$, we can see easily that the image of f via the map above is $(f_l)_l$. □

Remark 4.4.4. We can now deduce another proof for the fact that $\mathscr{A}_L$ is Hausdorff and complete w.r.t the weak topology.

Proof. We have

$$\varprojlim_{l,m} \mathscr{A}_L/U_{l,m} = \varprojlim_m \varprojlim_l (\mathcal{O}/\pi^m \mathcal{O})((X))/X^l((\mathcal{O}/\pi^m \mathcal{O})[[X]]) = \varprojlim_m (\mathcal{O}/\pi^m \mathcal{O})((X)) = \mathscr{A}_L$$

where the second identity follows from Lemma 4.4.3. □

Because $\mathscr{A}_L$ is a D.V.R, any finitely generated $\mathscr{A}_L$-module has a free part and a torsion part, where the torsion part is of the form $\mathscr{A}_L/\pi^{n_1}\mathscr{A}_L \oplus ... \oplus \mathscr{A}_L/\pi^{n_m}\mathscr{A}_L$. We can equip any free finitely generated $\mathscr{A}_L$-module M the product on each factor $\mathscr{A}_L$ via the isomorphism $\mathscr{A}_L^n \xrightarrow{\sim} M$. And for any finitely generated $\mathscr{A}_L$-module, there is a surjective map $\mathscr{A}_L^n \twoheadrightarrow M$, and we can equip M the quotient topology. This kind of topology is said to be the **weak topology** on M. We will prove that, in fact, the topology on finitely generated $\mathscr{A}_L$-modules behaves in a nice way.

Lemma 4.4.5. *$U_{l,m}$ is also closed in $\mathscr{A}_L$.*

Proof. It is clear, since $U_{l,m}$ is a $\mathcal{O}[[X]]$-submodule of $\mathscr{A}_L$, so if we take any $f \notin U_{l,m}$, we have $(f + U_{l,m}) \cap (U_{l,m}) = \emptyset$. So $\mathscr{A}_L \setminus U_{l,m}$ is open, and $U_{l,m}$ is closed. $\square$

We are now ready for the following important

Proposition 4.4.6. *Let M be a finitely generated $\mathscr{A}_L$-module, then M is also Hausdorff, and complete. Let $N \subseteq M$ be a submodule, then N is closed in M, and the weak topology on N is the same as the subspace topology on N induced from M.*

Proof. **Step 1.** We will check the proposition for $\mathscr{A}_L$ itself. The first statement is already proved. Let $N \subseteq \mathscr{A}_L$ is an $\mathscr{A}_L$-submodule, then N is of the form $\pi^m\mathscr{A}_L$. We can see first that $\pi^m\mathscr{A}_L = \cap_{l\geq m} U_{l,m}$, which is closed in $\mathscr{A}_L$, by the previous lemma.

The map

$$\begin{aligned} \mathscr{A}_L &\longrightarrow \pi^m\mathscr{A}_L \\ a &\longmapsto \pi^m a \end{aligned}$$

is an isomorphism of $\mathscr{A}_L$-modules, and it turns out that $\pi^m U_{l,n} = \pi^m X^l\mathcal{O}[[X]] + \pi^{m+n}\mathscr{A}_L$ forms a fundamental system around 0 in $\pi^m\mathscr{A}_L$, by the definition. In the subspace topology, we have the fundamental system around 0 in $\pi^m\mathscr{A}_L$ is of the form

$$(X^l\mathcal{O}[[X]] + \pi^{n+m}\mathscr{A}_L) \cap (\pi^m\mathscr{A}_L) = \pi^m(X^l\mathcal{O}[[X]] + \pi^{m-n}\mathscr{A}_L) = \pi^m X^l\mathcal{O}[[X]] + \pi^n\mathscr{A}_L$$

This yields the weak topology on $\pi^m\mathscr{A}_L$ is the same as the subspace topology.

Step 2. Let M be a free generated $\mathscr{A}_L$-module, then we have $\mathscr{A}_L^n \xrightarrow{\sim} M$ for some n, and this yields by the definition that the weak topology on M is the same as the product topology on $\mathscr{A}_L^n$. From this M is complete and Hausdorff. Let N be any submodule of M, then N is of the form $\pi^{n_1}\mathscr{A}_L \oplus ... \oplus \pi^{n_k}\mathscr{A}_L (k \leq m)$, which is closed in M by Step 1, and the weak topology on N is also the subspace topology on M, by Step 1 again.

Step 3. For the case $M = \mathscr{A}_L/\pi^j\mathscr{A}_L$, where M is equipped with the quotient topology from via the projection from $\mathscr{A}_L$. Let us denote $\mathscr{A}_j := \mathscr{A}_L/\pi^j\mathscr{A}_L$, $\mathcal{O}_j := \mathcal{O}/\pi^j\mathcal{O}$, then the fundamental system in $\mathscr{A}_L$ is of the form

$$V_{l,m} = X^l\mathcal{O}_j[[X]] + \pi^m\mathscr{A}_j$$

By the same arguments as in Remark 4.4.4, we obtain M is Hausdorff and complete. Note that any submodule N of M is of the form $\pi^m\mathscr{A}_L/\pi^j\mathscr{A}_L (m \leq j)$, which is isomorphic to $\mathscr{A}_L/\pi^{j-m}\mathscr{A}_L$ as $\mathscr{A}_L$-modules, which is complete, and Hausdorff since we can replace M by $\mathscr{A}_L/\pi^{j-m}\mathscr{A}_L$ in the beginning of Step 3. And proceeding similarly to Step 1, the weak topology on N is the same as the subspace topology induced from M.

Step 4. Now, if M is an arbitrary finitely generated $\mathscr{A}_L$-module, then M is of the form $M = \mathscr{A}_L^m \oplus \mathscr{A}_L/\pi^{m_1}\mathscr{A}_L \oplus ... \oplus \mathscr{A}_L/\pi^{m_k}\mathscr{A}_L$. And by combining all previous steps, we get M satisfies the statement. $\square$

As a corollary, we obtain

Corollary 4.4.7. *Let M, N be two finitely generated $\mathscr{A}_L$-modules, then any $\mathscr{A}_L$-module homomorphism $\alpha : M \to N$ is continuous w.r.t the weak topology.*

Using this, we can deduce

Lemma 4.4.8. *Let $\alpha : \mathscr{A}_L \to \mathscr{A}_L$ be a continuous ring homomorphism, and M, N are two finitely generated $\mathscr{A}_L$-module, and $\beta : M \to N$ an α-linear homomorphism, i.e. $\beta(m_1 + m_2) = \beta(m_1) + \beta(m_2), \beta(fm) = \alpha(f)\beta(m)$, for all $f \in \mathscr{A}_L, m_1, m_2 \in M$, then β is continuous.*

Proof. Because β is α-linear, we want to linearize this map, so that we can use Corollary 4.4.7. We denote $\mathscr{A}_L \otimes_{\varphi_L, \mathscr{A}_L} M$ the tensor product with the base ring $\mathscr{A}_L$, and $\mathscr{A}_L$ on the left is considered as $\mathscr{A}_L$-module via the map α. We note that, for this $a \otimes b.m = b.a \otimes m = \alpha(b)a \otimes m$. We can define

$$\begin{aligned} \beta^{\mathrm{lin}} : \mathscr{A}_L \otimes_{\varphi_L, \mathscr{A}_L} M &\longrightarrow N \\ f \otimes m &\longmapsto f\beta(m) \end{aligned}$$

. The map β^{lin} is now $\mathscr{A}_L$-linear. And there exists an $\mathscr{A}_L$-linear map $\tilde{\beta}$ making the following diagram commute

$$\begin{tikzcd} \mathscr{A}_L^m \arrow[r, "\alpha^m"] \arrow[d, "\lambda_M"] & \mathscr{A}_L^m = \mathscr{A}_L \otimes_{\varphi_L, \mathscr{A}_L} \mathscr{A}_L^m \arrow[r, "\tilde{\beta}"] \arrow[d, "id\otimes\lambda_m"] & \mathscr{A}_L^n \arrow[d, "\lambda_N"] \\ M \arrow[r, "m\mapsto 1\otimes m"] \arrow[rr, bend right, "\beta"'] & \mathscr{A}_L \otimes_{\varphi_L, \mathscr{A}_L} M \arrow[r, "\beta^{\mathrm{lin}}"] & N \end{tikzcd}$$

We note that for term in the middle, if we consider $\alpha : \mathscr{A}_L \to \mathscr{A}_L$ and denote $B := \mathscr{A}_L$ on the left, then $\mathscr{A}_L$ has the structure of a bi-module ${}_{\mathscr{A}_L}(\mathscr{A}_L)_B$ and $\mathscr{A}_L^m$ has structure of a bi-module ${}_B(\mathscr{A}_L{}^m)_{\mathscr{A}_L}$. And hence, ${}_{\mathscr{A}_L}(\mathscr{A}_L)_B \otimes_B {}_B(\mathscr{A}_L{}^m)_{\mathscr{A}_L}$ has the structure of $\mathscr{A}_L$-module, this yields the map

$$\begin{aligned} {}_{\mathscr{A}_L}(\mathscr{A}_L)_B \otimes_B {}_B(\mathscr{A}_L{}^m)_{\mathscr{A}_L} &\longrightarrow {}_{\mathscr{A}_L}\mathscr{A}_L^m \\ a \otimes (a_1, ..., a_m) &\longmapsto (aa_1, ..., aa_m) \end{aligned}$$

is hence, an isomorphism of $\mathscr{A}_L$-module.

This yields by Corollary 4.4.7 that all maps in the diagram above, except β and $m \mapsto 1 \otimes m$ is continuous. But due to the universal property of quotient topology, we get β must be continuous as well. $\square$

We are now turning to the definition of (φ_L, Γ_L)-modules.

Definition. Let M be a finitely generated $\mathscr{A}_L$-module, then M is said to be a (φ_L, Γ_L)**-module** if

(i) Γ_L acts on M as semilinear continuous automorphism, where semilinear means that for all $\gamma \in \Gamma_L, f \in \mathscr{A}_L, m, m_2, m_2 \in M$, we have $\gamma(fm) = \gamma(f)\gamma(m)$, and $\gamma(m_1 + m_2) = \gamma(m_1) + \gamma(m_2)$.

(ii) There exists a φ_L-linear endomorphism $\varphi_M : M \to M$ which commutes with the action of Γ_L.

A (φ_L, Γ_L)-module M is said to be **etale** if the linearized map $\varphi_M^{\mathrm{lin}} : \mathscr{A}_L \otimes_{\varphi_L, \mathscr{A}_L} M \to M$ is bijective.

Due to Lemma 4.4.8, we know that the map φ_M is continuous, since φ_L is a continuous ring homomorphism of $\mathscr{A}_L$.

Definition. Let M, N be two etale (φ_L, Γ_L)-modules, then a morphism between M and N is an $\mathscr{A}_L$-linear map, such that

$$\alpha \circ \varphi_M = \varphi_N \circ \alpha \text{ and } \alpha \circ \gamma = \gamma \circ \alpha (\forall \gamma \in \Gamma_L)$$

We denote $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$ the category of etale (φ_L, Γ_L)-modules. It can be proved that

Proposition 4.4.9. *$Mod^{et}(\mathscr{A}_L)$ is an abelian category.*

Proof. Let $\alpha : M \to N$ be a morphism between two etale (φ_L, Γ_L)-modules. By the definition, it is easy to see that $\ker\alpha$ and cokerα are (φ_L, Γ_L)-modules. Note that since $\mathscr{A}_L$ is a D.V.R and it is a free $\varphi_L(\mathscr{A}_L)$-module by Lemma 4.1.3, we have $\mathscr{A}_L \otimes_{\varphi_L, \mathscr{A}_L} -$ is an exact functor. From the exact sequence

$$0 \to \ker\alpha \to M \to N \to \mathrm{coker}\alpha \to 0$$

we have

$$0 \to \mathscr{A}_L \otimes_{\varphi_L,\mathscr{A}_L} \ker\alpha \to \mathscr{A}_L \otimes_{\varphi_L,\mathscr{A}_L} M \to \mathscr{A}_L \otimes_{\varphi_L,\mathscr{A}_L} N \to \mathscr{A}_L \otimes_{\varphi_L,\mathscr{A}_L} \mathrm{coker}\alpha \to 0$$

is also exact, and it can be seen that the diagram below

$$\begin{tikzcd}
0 \arrow[r] & \mathscr{A}_L \otimes_{\varphi_L,\mathscr{A}_L} \ker\alpha \arrow[r] \arrow[d, "\varphi^{\mathrm{lin}}_{\ker\alpha}"] & \mathscr{A}_L \otimes_{\varphi_L,\mathscr{A}_L} M \arrow[r] \arrow[d, "\varphi^{\mathrm{lin}}_{M}"] & \mathscr{A}_L \otimes_{\varphi_L,\mathscr{A}_L} N \arrow[r] \arrow[d, "\varphi^{\mathrm{lin}}_{N}"] & \mathscr{A}_L \otimes_{\varphi_L,\mathscr{A}_L} \mathrm{coker}\alpha \arrow[r] \arrow[d, "\varphi^{\mathrm{lin}}_{\mathrm{coker}\alpha}"] & 0 \\
0 \arrow[r] & \ker\alpha \arrow[r] & M \arrow[r] & N \arrow[r] & \mathrm{coker}\alpha \arrow[r] & 0
\end{tikzcd}$$

is commutative, which rows are exact, and the two middle vertical arrows are isomorphism. This yields that the left and right arrows are isomorphisms, too. Hence both $\ker\alpha, \mathrm{coker}\alpha$ are etale (φ_L, Γ_L)-modules. And hence, $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$ is an abelian category. $\square$

Important Remark. The axiom for the continuous action from Γ_L to etale (φ_L, Γ_L)-modules can be deduced from other axioms [Sch17](Theorem 2.2.8).

We finish this chapter by some examples about (φ_L, Γ_L)-modules.

Example 4.4.10. $M := \mathscr{A}_L$ is an etale (φ_L, Γ_L)-modules, with $\varphi_M := \varphi_L$.

Example 4.4.11. Let M be an object in $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$, and $\psi : \Gamma_L \to \mathcal{O}^\times$ is any homomorphism of groups, then we can defined the twists of M, denoted $M(\psi)$, whose underlying $\mathscr{A}_L$-module structure is the same as M, and $\varphi_{M(\psi)} := \varphi_M$. But the action from Γ_L is defined to be

$$\begin{aligned} \Gamma_L \times M(\psi) &\longrightarrow M(\psi) \\ (\gamma, m) &\longmapsto \psi(\gamma)\cdot\gamma(m) \end{aligned}$$

where $\psi(\Gamma)$ acts on M through $\chi_L^{-1} : \mathcal{O}^\times \to \Gamma_L$.

Later, by using the equivalence of categories, we will prove that for the case of rank one module M in $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$, M is isomorphic to $\mathscr{A}_L$ twisted by a character $\psi : \Gamma_L \to \mathcal{O}^\times$.

Example 4.4.12. We will use an explicit method to construct M a free etale (φ_L, Γ_L)-module of rank 1. For $\gamma \in \Gamma_L$, we can assume that $\gamma(e_1) = C_\gamma e_1$, with $C_\gamma \in \mathscr{A}_L \setminus \pi\mathscr{A}_L$, then $\gamma(fe_1) = {}^\gamma f C_\gamma e_1$. For

$$\begin{aligned} \varphi_M : M &\longrightarrow M \\ e_1 &\longmapsto De_1 \end{aligned}$$

it is φ_L linear, i.e. $\varphi_L(fe_1) = \varphi_L(f)\varphi_M(e_1) = \varphi_L(f)De_1$.

The condition ϕ_M commutes with Γ_L actions means $\varphi_M \circ \gamma = \gamma \circ \varphi_M$, where

$$\varphi_M(\gamma(fe_1)) = \varphi_M({}^\gamma f C_\gamma e_1) = \varphi_L({}^\gamma f C_\gamma)e_1 = \varphi_L({}^\gamma f)\varphi_L(C_\gamma)De_1$$

$$\gamma(\varphi_M(fe_1)) = \gamma(\varphi_L(f)De_1) = {}^\gamma\varphi_L(f)({}^\gamma D)C_\gamma e_1$$

And the commutativity implies that $\phi_L(C_\gamma)D = ({}^\gamma D)C_\gamma$, because ϕ_L is Γ_L-equivariant. If we choose further $D \in \mathscr{A}_L \setminus \pi\mathscr{A}_L$, then it is obvious that φ_M^{lin} is an isomorphism. We can reduce the last condition to

$$\varphi_L(C)D = ({}^{\gamma}D)C$$

It is equivalent to say $C([\pi]_\phi(X))D(X) = D([\chi(\gamma]_\phi(X))C(X)$. There is a possible solution for this. We note that

$$[\pi]_\phi([\chi(\gamma)]_\phi(X)) = [\chi(\gamma)]_\phi([\pi]_\phi(X))$$

Taking the derivative both sides, we have

$$[\pi]'_\phi([\chi(\gamma)]_\phi(X)).[\chi(\gamma)]'_\phi(X) = [\chi(\gamma)]'_\phi([\pi]_\phi(X)).[\pi]'_\phi(X)$$

And this yields an obvious solution $C = [\chi(\gamma)]'_\phi(X), D = \frac{[\pi]'_\phi(X)}{\pi}$. Note that we need to divide π in D, since $[\pi]_\phi(X) = \pi X + X^q + ...$, and we need to choose $D \in \mathscr{A}_L \setminus \pi\mathscr{A}_L$. This example shows in fact that the global differential form $\mathscr{A}_L dX = \Omega^1_{\mathscr{A}_L}$ is an etale (φ_L, Γ_L)-module, with the action

$$\gamma(fe_1) = f([\chi(\gamma)]_\phi(X))[\chi(\gamma)]'_\phi(X)dX$$

$$\phi_M(fe_1) = f([\pi]_\phi(X))\frac{[\pi]'_\phi(X)}{\pi}dX$$

It is proved in [SV16] that $\mathscr{A}_L(\chi_L) \cong \Omega^1_{\mathscr{A}_L}$ in $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$.

Chapter 5

An equivalence of categories

In this chapter, we will prove that the categories of Galois representation $\mathrm{Rep}_{\mathcal{O}}(G_L)$ is equivalent to the categories of etale (φ_L, Γ_L)-modules. For the first step, we will construct the ring A, which contains both $\mathcal{O}$ and A_L as subrings. Later, we will describe functors between the two categories, and begin the proof from the case π-torsion modules, and by devissage, deduce the equivalence of categories for the case π^m-torsion modules, and finally, move to the general case by a simple limit argument. We finish this chapter by two applications of the equivalence of categories

- The classification of rank one Galois representations and rank one etale (φ_L, Γ_L)-modules.
- The p-cohomological dimension of $G_{\mathbb{Q}_p}$.

5.1 The ring A

Because $A_L \cong \mathscr{A}_L$ as topological ring, and Fr on the left is compatible with φ_L on the right, we have for all $f \in \mathscr{A}_L$ $\varphi_L(f) \equiv f^q \mod \pi\mathscr{A}_L$ implies that $Fr(a) \equiv a^q \mod \pi A_L$ for all $a \in A_L$. Let us denote B_L the fraction field of A_L. We can see that B_L is a complete, non-archimedean field with its ring of integer A_L, and its residue field E_L.

Let C be an unramified extension of B_L of degree d with its ring of integer $\mathcal{O}_C$ we want to construct the extension σ of Fr on $\mathcal{O}_C$ such that σ is an $\mathcal{O}$-algebra and $\sigma(c) \equiv c^q \mod \pi\mathcal{O}_C$, for all $c \in \mathcal{O}_C$. If such extension exists, then we can use Proposition 2.5.1, to embed $\mathcal{O}_C$ into $W(E_L^{\text{sep}})$.

Let $b \in \mathcal{O}_C$, so that $\mathcal{O}_C = A_L \oplus A_L b \oplus ... \oplus A_L b^{d-1}$, and b has its minimal polynomial $P(X)$ over B_L, such that $\overline{P}(X) := P(X) \mod E_L[X]$ is separable. Hence, to determine σ, we have $\sigma(a_0 + a_1 b + ... + a_{d-1} b_{d-1}) = \varphi_L(a_0) + \varphi_L(a_0)\sigma(b) + ... + \varphi_L(a_{d-1})\sigma(b^{d-1})$. So, it is sufficient to determine $\sigma(b)$. But then, since $\mathcal{O}_C \cong \mathscr{A}_L[X]/P\mathscr{A}_L[X]$, where b is sent to X, we need a compatible condition between b and $\sigma(b)$, so that σ is a ring homomorphism. Say another words, if $P(X) = a_0 + a_1 X + ... + a_{d-1} X^{d-1} + X^d$, then $\sigma(b)$ is a root of $Q(X) := \varphi_L(a_0) + \varphi_L(a_1)X + ... + \varphi_L(a_{d-1})X^{d-1} + X^d$. Because $\varphi_L(a) \equiv a^q \mod \pi A_L$, we have $\overline{Q}(X^q) = Q(X) \mod \pi = \overline{P}(X)$. This yields if α is a root of $\overline{P}(X)$, then α^q is a root of $\overline{Q}(X)$. So, in particular, $\overline{Q}(X)$ has d distinct roots, and it is separable, since $\overline{P}(X)$ is. Now, $\overline{b}^q$ is a root of $\overline{Q}(X)$, and by Hensel's lifting lemma, we can lift $\overline{b}^q$ to a unique $c \in \mathcal{O}_C$, such that $Q(c) = 0$, and $c \equiv b^q \mod \pi\mathcal{O}_C$. So, due to the uniqueness of root lifting, we need to have $\sigma(b) = c$. From this, we obtain the existence and the uniqueness of the extension of Fr on $\mathcal{O}_C$.

We can now embed $\mathcal{O}_C$ into $W(E_L^{\text{sep}})$ as follows. If we begin with F/E_L a finite extension in E_L^{sep}, then there exists a unique C/B_L a finite unramified extension such that $\mathcal{O}_C/\pi\mathcal{O}_C \cong F$. And by the existence of σ in $\mathcal{O}_C$, by Proposition 2.5.1, there exists an $\mathcal{O}$-algebra homomorphism $s : \mathcal{O}_C \to W(\mathcal{O}_C)$ such that s is uniquely determined by the two commutative diagrams below.

$$\begin{tikzcd} \mathcal{O}_C \arrow[r, "s"] \arrow[dr, "id"'] & W(\mathcal{O}_C) \arrow[d, "\Phi_0"] \\ & \mathcal{O}_C \end{tikzcd} \tag{5.1}$$

$$\begin{tikzcd} \mathcal{O}_C \arrow[r, "s"] \arrow[d, "\sigma"] & W(\mathcal{O}_C) \arrow[d, "Fr"] \\ \mathcal{O}_C \arrow[r, "s"] & W(\mathcal{O}_C) \end{tikzcd} \tag{5.2}$$

From 5.1, we obtain the following comutative diagram.

$$\begin{tikzcd} \mathcal{O}_C \arrow[r, "s"] \arrow[dr, "id"] & W(\mathcal{O}_C) \arrow[r, "W(\mathrm{pr})"] \arrow[d, "\Phi_0"] & W(\mathcal{O}_C/\pi\mathcal{O}_C) \arrow[r, "\sim"] \arrow[d, "\Phi_0"] & W(F) \arrow[r] \arrow[d, "\Phi_0"] & W(E_L^{\mathrm{sep}}) \arrow[d, "\Phi_0"] \\ & \mathcal{O}_C \arrow[r, "pr"] & \mathcal{O}_C/\pi\mathcal{O}_C \arrow[r, "\sim"] & F \arrow[r] & E_L^{\mathrm{sep}} \end{tikzcd}$$

The composition map $\mathcal{O}_C \to W(E_L^{\mathrm{sep}})$ is hence, injective, since otherwise, $\pi^m \mapsto 0$ for some m, but it is absurd, since π is not a zero divisor in $W(E_L^{\mathrm{sep}})$ (Proposition 2.4.5) . We denote this image as $A(F)$, then $A(F) \cong \mathcal{O}_C$ via an $\mathcal{O}$-algebra isomorphism. This follows that

(1") $A(F)$ is a D.V.R with prime element π. This is clear via the isomorphism.

(2") $A(F)/\pi A(F) \cong F$ via Φ_0. It is also clear from the commutative diagram

$$\begin{tikzcd} \mathcal{O}_C \arrow[r, "\sim"] \arrow[d, "pr"] & A(F) \arrow[d, "\Phi_0"] \\ F \arrow[r] & F. \end{tikzcd}$$

We prove that such $A(F)$ satisfying $A_L \subseteq A(F) \subseteq W(E_L^{\mathrm{sep}})$, and (1"), (2") as above is unique, for fixed F/E: finite, separable extension. In fact, if we fix an algebraic closure of the fraction field of $W(E_L^{\mathrm{sep}})$, then it contains a algebaic closure $\overline{B_L}$ of B_L, and because of conditions (1") and (2"), the fraction field of $A(F)$ is the unique finite unramified extension of B_L in $\overline{B_L}$, with residue field F. We can also see that the field $A(F)$ satisfies

(3") The fraction field of $A(F)$ is a finite unramified extension of B_L. This is clear.

(4") The Frobenius Fr on $W(E_L^{\mathrm{sep}})$ preserves $A(F)$.

For (4"), it follows from 5.5 that the diagram

$$\begin{tikzcd} \mathcal{O}_C \arrow[r, "s"] \arrow[d, "\sigma"] & W(\mathcal{O}_C) \arrow[r, "W(\mathrm{pr})"] \arrow[d, "Fr"] & W(\mathcal{O}_C/\pi\mathcal{O}_C) \arrow[r, "\sim"] \arrow[d, "Fr"] & W(F) \arrow[r] \arrow[d, "Fr"] & W(E_L^{\mathrm{sep}}) \arrow[d, "Fr"] \\ \mathcal{O}_C \arrow[r, "s"] & W(\mathcal{O}_C) \arrow[r, "W(\mathrm{pr})"] & W(\mathcal{O}_C/\pi\mathcal{O}_C) \arrow[r, "\sim"] & W(F) \arrow[r] & W(E_L^{\mathrm{sep}}) \end{tikzcd} \tag{5.3}$$

is commutative. Hence, we get the diagram

$$\begin{tikzcd} \mathcal{O}_C \arrow[r, "s"] \arrow[d, "\sigma"] & A_L \arrow[d, "Fr"] \\ \mathcal{O}_C \arrow[r, "s"] & A_L \end{tikzcd} \tag{5.4}$$

is also commutative, so that Fr fixes $A(F)$. We now denote

$$A^{\mathrm{nr}} := \bigcup_{F/E:\text{fin. sep.}} A(F)$$

then it can be seen that

(1') A^{nr} is a D.V.R with prime element π, and $A^{\mathrm{nr}}/\pi A^{\mathrm{nr}} \cong E_L^{\mathrm{sep}}$.

(2') Frobenius on $W(E_L^{\mathrm{sep}})$ preserves A^{nr}.

(3') The action from G_L to $W(\mathcal{O}_{\mathbb{C}_p^\flat})$ preserves A^{nr}.

For (3'), we recall that the action from Γ_L and hence, G_L preserves E_L, because H_L fixes $\widehat{L_\infty}$ and hence $\widehat{L_\infty}^\flat$, and $E_L \subseteq \widehat{L_\infty}^\flat$. This yields G_L preserves E_L^{sep}. Also, the isomorphism $\mathscr{A}_L \cong A_L$ is Γ_L-equivariant Proposition 4.3.3, so G_L also preserves A_L. Hence, for any $\gamma \in G_L$, we have $A_L \subseteq {}^\gamma A(F) \subseteq W(E_L^{\mathrm{sep}})$. And it is clear that ${}^\gamma A(F)$ also satisfies the conditions (1") and (2"), because γ acts as $\mathcal{O}$-algebra automorphism. Due to the uniqueness of $A(F)$, we have ${}^\gamma A(F) = A(F)$. This yields G_L perserves A^{nr}.

We denote A the completion of A^{nr}, w.r.t the π-adic topology. We will prove that $A \subseteq W(E_L^{\mathrm{sep}})$. But this follows easily, since $W(E_L^{\mathrm{sep}})$ is π-adically complete by Corollary 2.4.4, and $\pi^m W(E_L^{\mathrm{sep}}) \cap A^{\mathrm{nr}} = \pi^m A^{\mathrm{nr}}$, so the π-adic topology on A^{nr} is induced from the π-adic topology on $W(E_L^{\mathrm{sep}})$. So we get

(1) A is complete D.V.R with prime element π, and $A/\pi A \cong E_L^{\mathrm{sep}}$.

Also, any $\mathcal{O}$-algebra homomorphism $W(\mathbb{C}_p^\flat) \to W(\mathbb{C}_p^\flat)$ is continuous w.r.t the π-adic topology, because $\mathcal{O}_{\mathbb{C}_p^\flat}$ is perfect extension of k, and hence $W(\mathbb{C}_p^\flat)$ is a D.V.R with prime element π. And in particular, Fr and the action from G_L is continuous on $W(E_L^{\mathrm{sep}})$ w.r.t the π-adic topology. So by continuity and (2'), (3'), we get

(2) Frobenius Fr preserves A.

(3) G_L preserves A, with H_L fixes A_L. This is because H_L fixes $W(\widehat{L_\infty}^\flat) \supseteq W(E_L)$.

5.2 A description for the functors

Definition. We denote $\mathrm{Rep}_{\mathcal{O}}(G_L)$ the category consisting of finitely generated $\mathcal{O}$-module V, where G_L acts continuously as $\mathcal{O}$-linear endomorphisms, with respect to the π-adic topology on V.

In this section, we will describe the functors between $\mathrm{Rep}_{\mathcal{O}}(G_L)$ and $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$. For the first functor, we have to use the second tilting correspondence for absolute Galois groups. Recall that $\mathrm{Gal}(\overline{\mathbb{Q}_p}/L_\infty) = H_L \cong H_{E_L} = \mathrm{Gal}(E_L^{\mathrm{sep}}/E_L)$.

Lemma 5.2.1. $A^{H_L} = A_L$.

Proof. We have $(A/\pi A)^{H_L} = (E_L^{\mathrm{sep}})^{H_L} = E_L = A_L/\pi A_L$. Consider the following diagram, where rows are exact

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_L/\pi^m A_L & \longrightarrow & A_L/\pi^{m+1} A_L & \longrightarrow & A_L/\pi A_L & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & (A/\pi^m A)^{H_L} & \longrightarrow & (A/\pi^{m+1} A)^{H_L} & \longrightarrow & (A/\pi A)^{H_L} & \longrightarrow & 0. \end{array} \tag{5.5}$$

By induction, the left and right arrows are isomorphism. This yields the middle arrow is an isomorphism, too. And we get $(A/\pi^m A)^{H_L} = A_L/\pi^m A_L$ for all m. From this, we get

$$A^{H_L} = (\varprojlim_m A/\pi^m A)^{H_L} = \varprojlim_m (A/\pi^m A)^{H_L} = \varprojlim_m (A_L/\pi^m A_L) = A_L.$$

□

Now, let V be any object in $\mathrm{Rep}_{\mathcal{O}}(G_L)$, we have $A \otimes_{\mathcal{O}} V$ is an A-module, with the action from G_L

$$\begin{aligned} G_L \times (A \otimes_{\mathcal{O}} V) &\longrightarrow A \otimes_{\mathcal{O}} V \\ (\sigma, a \otimes v) &\longmapsto \sigma(a) \otimes \sigma(v) \end{aligned}$$

Let us denote $\varphi := Fr \otimes id : A \otimes_{\mathcal{O}} V \to A \otimes_{\mathcal{O}} V$ a linear map of A-module, and $\mathscr{D}(V) := (A \otimes_{\mathcal{O}} V)^{H_L}$. As in Lemma 5.2.1, because $A^{H_L} = A$, we have $\mathscr{D}(V)$ is an $\mathscr{A}_L$-module. The action from Γ_L on $\mathscr{D}(V)$ is induced from the action from G_L on $A \otimes_{\mathcal{O}} V$ defined above, which is semi-linear, since if we take any $\sigma \in G_L, a \in A_L$, then

$$\sigma(ab \otimes v) = \sigma(a)\sigma(b) \otimes \sigma(v) = \sigma(a)\sigma(b \otimes v)$$

Furthermore, let us define $\varphi_{\mathscr{D}(V)} := \varphi|_{\mathscr{D}(V)}$, then it can be seen that $\varphi_{\mathscr{D}(V)}$ is φ_L-linear, where $\varphi_L = Fr$ in A_L, since

$$\varphi_{\mathscr{D}(V)}(ab \otimes v) = Fr(ab) \otimes v = Fr(a)Fr(b) \otimes v = \varphi_L(a)(Fr(b) \otimes v) = \varphi_L(a)\varphi_{\mathscr{D}(V)}(b \otimes v)$$

Also, since Fr acts on $W(E_L^{\mathrm{sep}})$ is just bt taking q-th power of coordinates, it is obvious commutative with the action from G_L. Hence, we have a candidate for our first functor

$$\begin{aligned} \mathscr{D} : \mathrm{Rep}_{\mathcal{O}}(G_L) &\longrightarrow \mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L) \\ V &\longmapsto \mathscr{D}(V) = (A \otimes_{\mathcal{O}} V)^{H_L} \end{aligned}$$

Later, we will show that $\mathscr{D}$ is actually well-defined. To do this, we will prove two things:
(D1) $\mathscr{D}(V)$ is a finitely generated $\mathcal{O}$-module.
(D2) The action from Γ_L to $\mathscr{D}(V)$ is continuous.
We also obtain a map

$$\begin{aligned} ad_V : A \otimes_{A_L} \mathscr{D}(V) &\longrightarrow A \otimes_{\mathcal{O}} V \\ a \otimes (a' \otimes v) &\longmapsto aa' \otimes v \end{aligned}$$

. And it is easy to check that $ad_V \circ (Fr \otimes \varphi_{\mathscr{D}(V)}) = \varphi \circ ad_V$, and ad_V is G_L-equivariant.
And we obtain an additional property (that we will need to check)
(D3) ad_V is bijective.
And it can be deduced that (D1) and (D3) imply (D2) [Sch17](Proposition 3.1.12 (i)). Furthermore, we have

Proposition 5.2.2. *Let $V \in Rep_{\mathcal{O}}(G_L)$ such that $(D1)$ and $(D3)$ holds for V, then V and $\mathscr{D}(V)$ have the same elementary divisors.*

Proof. Because $A, \mathcal{O}, A_L$ are DVRs, as $\mathcal{O}$-module, we can write $V = \bigoplus_{i=1}^r \mathcal{O}/\pi^{n_i}\mathcal{O}$. And as A_L-module, due to $(D1)$, we can $\mathscr{D}(V) = \bigoplus_{i=1}^s A_L/\pi^{m_i}A_L$. We can write

$$A \otimes_{\mathcal{O}} V = A \otimes_{\mathcal{O}} \Big(\bigoplus_{i=1}^r \mathcal{O}/\pi^{n_i}\mathcal{O} \Big) = \bigoplus_{i=1}^r A/\pi^{n_i}A$$

And similarly

$$A \otimes_{A_L} \mathscr{D}(V) = \bigoplus_{i=1}^s A/\pi^{m_i}A$$

Due to (D3), we then $r = s$, and $n_i = m_i$ up to some permutation. □

We now come to the second cadidate.

Lemma 5.2.3. $(W(E_L^{sep}))^{Fr=1} = W(k) = \mathcal{O}$.

Proof. We have $(W(E_L^{\mathrm{sep}}))^{Fr=1} = \{(a_0, a_1, ...) \in W(E_L^{\mathrm{sep}}), a_i^q = a_i, \forall i\}$. And this yields $a_i \in k$ for all i. □

Now, let M be an object in $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$, we have $A \otimes_{A_L} M$ is an A-module. We can define $\varphi := Fr \otimes \varphi_M : A \otimes_{A_L} M \to A \otimes_{A_L} M$, and the action from G_L is defined as

$$\begin{aligned} G_L \times A \otimes_{A_L} M &\longrightarrow A \otimes_{A_L} M \\ (\sigma, a \otimes m) &\longmapsto \sigma(a) \otimes \sigma(m) \end{aligned}$$

where σ acts on M by the reduction from G_L to Γ_L. We can see, by Lemma 5.2.3, that $\mathscr{V}(M) := (A \otimes_{A_L} M)^{\varphi=1}$ is actually an $\mathcal{O}$-module. And the action from G_L is obvious $\mathcal{O}$-linear, since G_L fixes L. And we then obtain a candidate for the second functor

$$\begin{aligned} \mathscr{V} : \mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L) &\longrightarrow \mathrm{Rep}_{\mathcal{O}}(G_L) \\ M &\longmapsto (A \otimes_{A_L} M)^{\varphi=1} \end{aligned}$$

To prove that $\mathscr{V}(M)$ is well-defined, we have to prove that

(V1) $\mathscr{V}(M)$ is finitely generated.

(V2) G_L acts continuously on $\mathscr{V}(M)$.

And we also have a map

$$\begin{aligned} ad_M : A \otimes_{\mathcal{O}} \mathscr{V}(M) &\longrightarrow A \otimes_{A_L} M \\ a' \otimes a \otimes m &\longmapsto a'a \otimes m \end{aligned}$$

It is easy to check that ad_M is G_L-equivariant, and $(Fr \otimes \varphi_M) \circ ad_M = ad_M \circ (Fr \otimes id)$. We have an additional property of ad_M, that we need to check

(V3) ad_M is bijective.

Similarly, (V1) and (V3) imply (V2) [Sch17](Proposition 3.1.13 (i)), and similar to Propositition5.2.2, we obtain

Proposition 5.2.4. *If M in $Mod^{et}(\mathscr{A}_L)$ satisfying (D1) and (D3), then M and $\mathscr{V}(M)$ has the same elementary divisors.*

We also have

Lemma 5.2.5. *Under the assumptions (D1), (D3), (V1) and (V3), we have $\mathscr{D}$ and $\mathscr{V}$ are quasi-inverse of each other.*

Proof. First, under the assuptions of (D1), (D3) and (V1), V(3), $\mathscr{D}, \mathscr{V}$ are well-defined. We have

$$\mathscr{V}(\mathscr{D}(V)) = (A \otimes_{A_L} \mathscr{D}(V))^{Fr \otimes \varphi_{\mathscr{D}(V)}=1} \xrightarrow{\sim} (A \otimes_{\mathcal{O}} V)^{Fr \otimes id=1} = A^{Fr=1} \otimes_{\mathcal{O}} V = V$$

where the second isomorphism follows from (D3). And similarly,

$$\mathscr{D}(\mathscr{V}(M)) = (A \otimes_{\mathcal{O}} \mathscr{V}(M))^{H_L} \xrightarrow{\sim} (A \otimes_{A_L} M)^{H_L} = A^{H_L} \otimes_{A_L} M = M$$

where the second isomorphism follows from (V3), and the third identity is obtained from the fact that M i fixed under the action of H_L. ☐

We are now ready to state the main theorem

Theorem 5.2.6. *The functors $\mathscr{D}$ and $\mathscr{V}$ are well-defined functors between $Rep_{\mathcal{O}}(G_L)$ and $Mod^{et}(\mathscr{A}_L)$, and are quasi-inverse of each other.*

Via our above arguments, it is now sufficient to check the conditions (D1), (D3) for $\mathscr{D}$, and (V1), (V3) for $\mathscr{V}$. In the next section, we will first begin with the case of π-torsion modules.

5.3 The equivalence of categories in the case π-torsion modules

If V in $\mathrm{Rep}_{\mathcal{O}}(G_L)$, and $\pi V = 0$, we can consider V as a finite dimensional k-vector space, and the action of G_L is continuous w.r.t the discrete topology on V. And in this case, $\mathscr{D}(V) = (E_L^{\mathrm{sep}} \otimes_k V)^{H_L}$. And for M in $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$, with $\pi M = 0$, we can regard M as a finite dimensional E_L-vector space. And in this case $\mathscr{V}(M) = (E_L^{\mathrm{sep}} \otimes_{E_L} M)^{\varphi=1}$. We will prove first that $\mathscr{D}$ is well-defined.

Lemma 5.3.1. *Let F/E be finite Galois extension of fields with Galois group G, and V a finite dimensional E-vector space, with a linear action from G, then there exists an F-basis of $F \otimes_E V$ such that this basis is fixed by G.*

Proof. We recall that if F/E is a finite Galois extension with Galois group G, then there exists $b \in F$, such that $(g(b))_{g\in G}$ forms an E-basis for F. Let us denote $d := \dim_E V$, and V^{tri} be V as E-vector space, with the trivial action from G. We can define a map

$$\alpha : F \otimes_E V^{\text{tri}} \longrightarrow F \otimes_E V$$
$$\Big(\sum_{g\in G} a_g g(b)\Big) \otimes v \longmapsto \Big(\sum_{g\in G} a_g g(b)\Big) \otimes g(v)$$

where $a_g \in E$ for all $g \in G$. It can be seen that α is an isomorphism of E-vector spaces, and G-modules. Hence,

$$(F \otimes_E V) \cong (F \otimes_E V^{\text{tri}})^G = V^{\text{tri}}$$

Hence, there exists $(u_1, ..., u_d)$ in $F \otimes_E V$ such that $u_1, ..., u_d$ is linearly independent over E, and they are fixed under the action of G. We will prove that they are linearly independent over F. Assume that there exists $c_1, ..., c_d \in F$ such that $\sum_i c_i u_i = 0$, with $c_1 \neq 0$. By multiplying c_1 with $c_1^{-1}b$, we can assume that $c_1 = b$. Taking the action for all $g \in G$ to the sum above, and summing them up, we obtain

$$\Big(\sum_{g\in G} g(b)\Big)u_1 + ... + \Big(\sum_{g\in G} g(c_d)\Big)u_d = 0$$

But it is a contradiction, since $\sum_{g\in G} g(c_i) \in E$, and $\sum_{g\in G} g(b) \neq 0$. Hence $(u_1, ..., u_d)$ is an F-basis for $F \otimes_E V$. □

Lemma 5.3.2. *Let E be a field, and E^{sep} a seperable closure of E with Galois group H, and V a finite dimensional E-vector space, and an H-module, with $\dim_E V = d$. Assume that $(u_1, ..., u_d)$ in $E^{sep} \otimes_E V$ is E-linearly independent, and they are fixed by the action of H, then $(u_1, ..., u_d)$ is an E^{sep}-basis for $E^{sep} \otimes_E V$.*

Proof. Assume that there exists $c_i \in E^{\text{sep}}$, such that $\sum_i c_i u_i = 0$, with $c_1 \neq 0$. Let F be the normal closure of $E(c_1, ..., c_d)$, then F/E is a finite Galois extension with Galois group G, where G is a quotient of H. And H fixes u_i implies that G fixes u_i, and hence, if we take actions of all $g \in G$, and sum them up, we can apply the same trick as in the proof of the previous lemma, and obtain a contradiction. □

Lemma 5.3.3. *Let V be in $Rep_{\mathcal{O}}(G_L)$, with $\pi V = 0$, there exists an E_L^{sep}-basis of $E_L^{sep} \otimes_k V$ that is fixed by H_L.*

Proof. Because G_L acts continuously on V, so does H_L, and because the topology on V is discrete, any $\{v_i\} \subset V$ is open, and hence, there exists an open normal subgroup N of H_L such that N fixes V. Because $H_L \cong \mathrm{Gal}(E_L^{\text{sep}}/E_L)$ topologically, we have N is an open normal subgroup of $\mathrm{Gal}(E_L^{\text{sep}}/E_L)$, and therefore, is of finite index. Let $F := (E_L^{\text{sep}})^N$, then F/E_L is a finite Galois extension with Galois group $G := H_L/N$. And we have

$$(E_L^{\text{sep}} \otimes_k V)^N = F \otimes_k V$$

And hence,

$$(E_L^{\text{sep}} \otimes_k V)^{H_L} = (F \otimes_k V)^G \tag{5.6}$$

Let $W_1 := E_L \otimes_k V$, then the action of G on W_1 is E_L-linear, and by Lemma 5.3.3, there exists an F-basis $(u_1, ..., u_d)$ of $F \otimes_{E_L} W_1 = F \otimes_k V$ that is fixed by G. And due to 5.6, $(u_1, ..., u_d)$ is fixed by H_L. Let $W_2 := F \otimes_k V$, then $(u_1, ..., u_d)$ are F-linearly independent in $E_L^{\text{sep}} \otimes_F W_2 = E_L^{\text{sep}} \otimes_k V$ fixed by H_L. Therefore, by Lemma 5.3.2, $(u_1, ...u_d)$ is an E_L^{sep}-basis of $E_L^{\text{sep}} \otimes_F W_2 = E_L^{\text{sep}} \otimes_k V$. □

We are now ready for one of the main results of this section

Proposition 5.3.4. *For any V in $Rep_{\mathcal{O}}(G_L)$, with $\pi V = 0$, then $\mathscr{D}(V)$ satisfies (D1) and (D3).*

Proof. We recall that we can write $\mathscr{D}(V) = (E_L^{\text{sep}} \otimes_k V)^{H_L}$. Let $(u_1, ..., u_d)$ be a basis in Lemma 5.3.3 above, where $d := \dim_k V$, then

$$(E_L^{\text{sep}} \otimes_k V)^{H_L} = (E_L^{\text{sep}} u_1 \oplus ... \oplus E_L^{\text{sep}} u_d)^{H_L} = E_L u_1 \oplus ... \oplus E_L u_d$$

Hence, $\mathscr{D}(V)$ is a finite dimensional E_L-vector space, and it satisfies (D1). And

$$E_L^{\text{sep}} \otimes_{E_L} \mathscr{D}(V) = E_L^{\text{sep}} \otimes_{E_L} \Big(E_L u_1 \oplus ... \oplus E_L u_d \Big) = E_L^{\text{sep}} \otimes_k V$$

And this yields $\mathscr{D}(V)$ also satisfies (D3). □

Now, via Proposition 5.3.4, we can see that the functor $\mathscr{D}$ is well-defined. We now turn to the case of the functor $\mathscr{V}$.

Let F be any separable closed field over k, and W is a finite dimensional F-vector space, with a map $f : W \to W$, such that f is ϕ_q-endomorphism, where ϕ_q is the Frobenius map, and the map

$$\begin{aligned} f^{\text{lin}} : F \otimes_{\phi_q, F} W &\longrightarrow W \\ a \otimes w &\longmapsto af(w) \end{aligned}$$

is bijective. We will prove that $\dim_k W^{f=1} = \dim_F W$, via several steps.

Note that since $F^{\phi_q = 1} = k$, for any $w \in W^{f=1}$, and $a \in k$, we have

$$f(aw) = a^q f(w) = af(w) = aw$$

So, $aw \in W^{f=1}$, and $W^{f=1}$ is a k-vector space. In the latter, we assume that $W \neq 0$.

Lemma 5.3.5. $W^{f=1} \neq 0$.

Proof. Let us choose $w_0 \neq 0$ in W, and $r \geq 1$ be the smallest integer such that $w_0, w_1 = f(w_0), ..., w_r := f(w_{r-1})$ are linearly dependent. And there exists $c_0, ..., c_r$ in F such that $c_0 w_0 + ... + c_r w_r = 0$, where $c_r \neq 0$.

Assume that there exists $d_1, ..., d_r$ in F such that $d_1 w_1 + ... + d_r w_r = 0$, then since $w_i = f(w_{i-1})$, we have $d_1 f(w_0) + ... + d_r f(w_{r-1}) = 0$. Since f^{lin} is bijective, $f^{\text{lin}}(d_1 \otimes w_0 + ... + d_r \otimes w_{r-1}) = 0$ implies that $d_1 \otimes w_0 + ... + d_r \otimes w_{r-1} = 0$, but this yields $d_1 = ... = d_r = 0$, since $w_0, ..., w_{r-1}$ are linearly independent over F. Hence $w_1, ..., w_r$ are also linearly independent. And we get $c_0 \neq 0$.

We consider now a linear combination $w = x_0 w_0 + ... + x_{r-1} w^{r-1}$, then $f(w) = x_0^q w_1 + ... + x_{r-1}^q w_r$. We will find x_i such that $f(w) = w$. This happen iff $f(w) - w = 0$, or equivalently

$$x_0 w_0 + (x_1^q - x_0^q) w_1 + ... + (x_{r-1} - x_{r-2}^q) w_{r-1} - x_{r-1}^q w_r = 0$$

And this occurs iff there exists $x \in F$, such that

$$x_0 = c_0 x$$

$$x_1 - x_0^q = c_1 x \Leftrightarrow x_1 = c_0^q x^q + c_1 x$$

$$x_{r-1} - x_{r-2}^q = c_{r-1} x \Leftrightarrow x_{r-1} = c_0^{q^{r-1}} x^{q^{r-1}} + ... + c_{r-1} x$$

$$x_{r-1}^q + c_r x = 0 \Leftrightarrow c_0^{q^r} x^{q^r} + ... + c_{r-1}^q x^q + c_r x = 0$$

i.e. x is a root of the last equation. Because $c_0, c_r \neq 0$, the polynomial in the last equation is separable, and hence, it has a root x in F. And have constructed $w \neq 0$ such that $w \in W^{f=1}$. □

Lemma 5.3.6. $\dim_k W_1 \leq \dim_F W$, *where* $W_1 := W^{f=1}$.

Proof. Assume that $\dim_k W_1 > \dim_F W$, then since $W \neq 0$, we have $\dim_k W_1 \geq 2$. And we can choose a smallest integer $r \geq 2$ such that $u_1, ..., u_r$ in W_1, linearly independent over k, but linearly dependent over F. Assume that $w := c_1u_1 + ... + c_ru_r = 0$, where $c_i \in F, c_r \neq 0$, then we must have $c_i \in F^\times$, since otherwise, it will contradict to the minimality of r. We can assume that $c_r = 1$, and

$$f(w) = u_1 + c_1^q u_2 + ... + c_r^q u_r = 0$$

And this yields $(c_2^q - c_2)u_2 + ... + (c_r^q - c_r)u_r = 0$, and this yields all $c_i^q - c_i = 0$, i.e. $c_i \in k$. and this leads to a contradiction. □

Lemma 5.3.7. *We have*

1. $\dim_k W_1 = \dim_k W$.
2. *The F-linear map*
$$\begin{aligned} F \otimes_k W_1 &\longrightarrow W \\ a \otimes w &\longmapsto aw \end{aligned}$$
is bijective.
3. *The k-linear map $f - \mathrm{id} : W \to W$ is surjective.*

Proof. We will prove that there exists a k-basis of W_1 such that it is also an F-basis of W by induction on $d := \dim_F W$. Assume that $d = 1$, then by Lemma 5.3.5, $W_1 \neq 0$, and $\dim_k W_1 \geq 1$. By Lemma 5.3.6, $\dim_k W_1 = 1$, and hence, there exists $w_1 \in W_1$ such that w_1 is both k-basis for W_1 and F-basis for W.

Now, let $d \geq 2$, we can choose $w_1 \in W_1$ such that $w_1 \neq 0$. Let $\tilde{W} := W/Fw_1$, and

$$\begin{aligned} \tilde{f} : \tilde{W} &\longrightarrow \tilde{W} \\ w + Fw_1 &\longmapsto f(w) + Fw_1 \end{aligned}$$

This map is well-defined since $f(w_1) = w_1$. And the map $\tilde{f}^{\mathrm{lin}}$ is bijective. In fact, the surjectivity follows directly from the surjectivity of f^{lin}. Moreover

$$\begin{aligned} f^{\mathrm{lin}}|_{Fw_1} : F \otimes_{\phi_q, F} Fw_1 &\longrightarrow Fw_1 \\ a \otimes bw_1 &\longmapsto ab^q w_1 \end{aligned}$$

is well-defined, and hence bijective, since they have both dimension 1 over F. From this, we have $f(a \otimes w) \in Fw_1$ iff $w \in Fw_1$. And this yields $\tilde{f}^{\mathrm{lin}}$ is also injective.

We next have the pair $(W/Fw_1, \tilde{f}^{\mathrm{lin}})$ satisfies the same condition as (W, f). Hence, by induction, there exists $w_2', ..., w_d'$ a k-basis of $(W/Fw_1)^{\tilde{f}=1}$ such that $w_2', ..., w_d'$ is also an F-basis of W/Fw_1. And we have $\tilde{f}(w_i') = w_i'$ implies that $f(w_i') = w_i' + a_iw_1$, for some $a_i \in F$, and $2 \leq i \leq d$. Take $w_i = w_i' + x_iw_1$, we will find x_i such that $f(w_i) = w_i$, i.e.

$$w_i' + x_iw_1 = w_i = f(w_i) = f(w_i' + x_iw_1) = f(w_i') + x_i^q f(w_1) = w_i' + a_iw_1 + x_i^q w_1$$

And it is sufficient to have x_i is a root of $f_i(x) := x^q - x + a_i$. These polynomiasl are clearly separable, so they have roots in F. And via the construction, we obtain $(w_1, ..., w_d) \in W_1$ is a desired basis.

From this construction, we easily obtain the second statement. For the third statement, it can be seen that the map $f - id$ on W corresponds to the map $(\phi_q - id) \otimes id$ on $F \otimes_k W_1$. But for any $c \in F$, the equation $x^q - x = c$ is seperable and hence, has solutions in F. This yields $f - id$ is surjective. □

We are now going to apply the first two parts of this lemma to the functor $\mathscr{V}$, where $F := E_L^{\mathrm{sep}}, W := E_L^{\mathrm{sep}} \otimes_{E_L} M$, and $f := \phi_q \otimes \varphi_M$, then we will get

(V1) $\mathscr{V}(M)$ is a finite dimensional k-vector space.

(V3) $E_L^{\mathrm{sep}} \otimes_k \mathscr{V}(M) \cong E_L^{\mathrm{sep}} \otimes_{E_L} M$.

Hence, we obtain

Proposition 5.3.8. *Let M be in $Mod^{et}(\mathscr{A}_L)$, such that $\pi M = 0$, then $\mathscr{V}(M)$ satisfies $(V1)$ and $(V3)$.*

Via Proposition 5.3.8, Proposition 5.3.4, and Lemma 5.2.5 we obtain in the case of π-torsion modules, $\mathscr{D}$, $\mathscr{V}$ are well-defined functors, and they are quasi-inverse of each other.

5.4 The case of π^m-torsion modules

We will begin this section with applications of Hilbert's 90 theorem.

Lemma 5.4.1. *Let F/E be a finite Galois extension of fields, with Galois group G, and V/E is a finite dimensional E-vector space, with a linear action from G, then $H^1(G, F \otimes_E V) = 0$.*

Proof. We recall the result of Lemma 5.3.1 that there exists an F-basis $(u_1, ..., u_d)$ of $F \otimes_E V$ such that it is fixed by G. Let $c : G \to F \otimes_E V$ be a 1-st cocycle, we can represent

$$c(g) = \sum_{i=1}^{d} c_i(g) u_i$$

where $c_i(g) : G \to F$. Because u_i is fixed under the action of G, due to Hilbert's 90 theorem, we can represent $c_i(g) = g(x_i) - x_i$ where $x_i \in F$. Then

$$c(g) = \sum_{i=1}^{d} (g(x_i) - x_i) u_i = \sum_{i=1}^{d} (g(x_i) u_i - x_i u_i) = \sum_{i=1}^{d} (g(x_i u_i) - x_i u_i)$$

So, if we denote $x := \sum_{i=1}^{d} x_i u_i$, then $c(g) = g(x) - x$, i.e. $H^1(G, F \otimes_E V) = 0$. □

We now come back to the case $E_L^{\mathrm{sep}} \otimes_k V$, where V is in $\mathrm{Rep}_{\mathcal{O}}(G_L)$, such that $\pi V = 0$. One can see that $H_L := \mathrm{Gal}(E_L^{\mathrm{sep}}/E_L)$ and hence, for any $a \in E_L^{\mathrm{sep}}$, there exists an open subgroup U of H_L that fixes f. Because the topology on V is discrete, for any $v \in V$, there exists an open subgroup U' of H_L that fixes v. And this yields $E_L^{\mathrm{sep}} \otimes_k V$ is a discrete H_L-module, since $U \cap U'$ fixes $a \otimes v$. And one obtains from this that

$$H^1(H_L, E_L^{\mathrm{sep}} \otimes_k V) = \varinjlim H^1(H_L/N, (E_L^{\mathrm{sep}} \otimes_k V)^N)$$

where N runs over all open normal subgroup of H_L. Again, due to V is discrete, for any open normal subgroup U of H_L, there exists an open normal subgroup $N \subseteq H_L$ such that $N \subset U$. And with such N, we have

$$(E_L^{\mathrm{sep}} \otimes_k V)^N = (E_L^{\mathrm{sep}})^N \otimes_k V$$

Let $F := (E_L^{\mathrm{sep}})^N$, and $G = \mathrm{Gal}(F/E) = H_L/N$, we have

$$H^1(H_L/N, (E_L^{\mathrm{sep}} \otimes_k V)^N) = H^1(G, F \otimes_k V) = H^1(G, F \otimes_{E_L} (E_L \otimes_k V)) = H^1(G, F \otimes_{E_L} W) = 0$$

where $W := (E_L \otimes_k V)$ is a finite dimensional E_L-vector space with a linear action from G, and the last equality follows from the lemma above. We obtain from this that

Proposition 5.4.2. *Let V be in $Rep_{\mathcal{O}}(G_L)$, such that $\pi V = 0$, then $H^1(H_L, E_L^{sep} \otimes_k V) = 0$.*

Let V be in $\mathrm{Rep}_{\mathcal{O}}(G_L)$, such that $\pi^m V = 0$. We note that the topology on V is discrete. If we begin with a short exact sequence in $\mathrm{Rep}_{\mathcal{O}}(G_L)$

$$0 \to V_0 \to V \to V_1 \to 0$$

then since π is not a zero divisor in A, we have

$$0 \to A \otimes_{\mathcal{O}} V_0 \to A \otimes_{\mathcal{O}} V \to A \otimes_{\mathcal{O}} V_1 \to 0$$

is still exact. And one can see that both V_0, V_1 are also π^m-torsion, and the topology on them are also discrete. In the case $\pi V_0 = 0$, we have $A \otimes_{\mathcal{O}} V_0 = E_L^{\text{sep}} \otimes_k V_0$, and by Proposition 5.4.2, we have $H^1(H_L, A \otimes_{\mathcal{O}} V_0) = 0$, and this yields by a long exact sequence of H_L-modules induced from the short exact sequence above that

$$0 \to (A \otimes_{\mathcal{O}} V_0)^{H_L} \to (A \otimes_{\mathcal{O}} V)^{H_L} \to (A \otimes_{\mathcal{O}} V_1)^{H_L} \to 0$$

is exact.

One can choose $V_0 := \pi^{m-1}V$, and $V_1 = V/V_0 = V/\pi^{m-1}V$, we can see that V_0 is π-torsion, and V_1 is π^{m-1}-torsion. By Proposition 5.3.4, we have $\mathscr{D}(V_0)$ is finitely generated $\mathscr{A}_L$-module, and by induction, so is $\mathscr{D}(V_1)$. This yields $\mathscr{D}(V)$ is also a finitely generated $\mathscr{A}_L$-module. And hence, $\mathscr{D}(V)$ satisfies (D1). For (D3), we begin from the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A \otimes_{A_L} \mathscr{D}(V_0) \arrow[r] \arrow[d, "ad_{V_0}"] & A \otimes_{A_L} \mathscr{D}(V) \arrow[r] \arrow[d, "ad_V"] & A \otimes_{A_L} \mathscr{D}(V_1) \arrow[r] \arrow[d, "ad_{V_1}"] & 0 \\
0 \arrow[r] & A \otimes_{\mathcal{O}} V_0 \arrow[r] & A \otimes_{\mathcal{O}} V \arrow[r] & A \otimes_{\mathcal{O}} V_1 \arrow[r] & 0
\end{tikzcd} \tag{5.7}$$

where rows are exact. Again, by induction, we obtain that the arrows on the left and the right are isomorphisms, so is the middle arrows. Hence, $\mathscr{D}(V)$ satisfies (D3). This yields

Proposition 5.4.3. *For any V in $Rep_{\mathcal{O}}(G_L)$ such that $\pi^m V$, for $m \geq 1$, then V satisfies (D1) and (D3). Moreover, in the sub-category of π^m-torsion modules, $\mathscr{D}$ is an exact functor.*

Proof. It is sufficient to prove the second statement. If we begin with a short exact sequence

$$0 \to V_0 \to V \to V_1 \to 0$$

where $\pi^m = 0$, then we have short exact sequences

$$0 \to \pi^{m-1}V_0 \to V \to V/\pi^{m-1}V_0 \to 0$$

$$0 \to \pi^{m-2}V_0/\pi^{m-1}V_0 \to V/\pi^{m-1}V_0 \to V/\pi^{m-2}V_0 \to 0$$

$$...$$

$$0 \to V_0/\pi V_0 \to V/\pi V_0 \to V/V_0 \cong V_1 \to 0$$

So we get

$$(A \otimes_{\mathcal{O}} V)^{H_L} \twoheadrightarrow (A \otimes_{\mathcal{O}} V/\pi^{m-1}V_0)^{H_L} \twoheadrightarrow ... \twoheadrightarrow (A \otimes_{\mathcal{O}} V/\pi V_0)^{H_L} \twoheadrightarrow (A \otimes_{\mathcal{O}} V_1)^{H_L}$$

where all surjective maps obtained from Proposition 5.4.2. Now, this yields

$$0 \to \mathscr{D}(V_0) \to \mathscr{D}(V) \to \mathscr{D}(V_1) \to 0$$

is also exact. $\square$

We now move to the functor $\mathscr{V}$. Let

$$0 \to M_0 \to M \to M_1 \to 0$$

be an exact sequence in $\text{Mod}^{\text{et}}(\mathscr{A}_L)$, we then have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A \otimes_{A_L} M_0 \arrow[r] \arrow[d, "\varphi-1"] & A \otimes_{A_L} M \arrow[r] \arrow[d, "\varphi-1"] & A \otimes_{A_L} M_1 \arrow[r] \arrow[d, "\varphi-1"] & 0 \\
0 \arrow[r] & A \otimes_{A_L} M_0 \arrow[r] & A \otimes_{A_L} M \arrow[r] & A \otimes_{A_L} M_1 \arrow[r] & 0
\end{tikzcd} \tag{5.8}$$

where rows are exact. We will prove that

Lemma 5.4.4. *If $\pi^m M = 0$, then $\varphi - 1$ is surjective, and*

$$0 \to \mathscr{V}(M_0) \to \mathscr{V}(M) \to \mathscr{V}(M_1) \to 0$$

is exact.

Proof. For the first statement, when $m = 1$, this follows from Lemma 5.3.7. So by 5.8, we can use induction with $M_0 := \pi^{m-1}M$. For the second statement, we can see that $\mathscr{V}(M)$ is a kernel of the map $\varphi - 1$, and hence, the exact sequence follows from the snake lemma. □

Proposition 5.4.5. *If $\pi^m M = 0$, then $\mathscr{V}(M)$ satisfies (V1) and (V3), and the functor $\mathscr{V}$ restricted on the sub-category of π^m-torsion modules are exact.*

Proof. The exactness of $\mathscr{V}$ follows directly from the lemma above. For (V1), we can apply the previous lemma with $M_0 := \pi^{m-1}M$, and induction. For (V3), from the exact sequence

$$0 \to \mathscr{V}(M_0) \to \mathscr{V}(M) \to \mathscr{V}(M_1) \to 0$$

and the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A \otimes_{\mathcal{O}} \mathscr{V}(M_0) & \longrightarrow & A \otimes_{\mathcal{O}} \mathscr{V}(M) & \longrightarrow & A \otimes_{\mathcal{O}} \mathscr{V}(M_1) & \longrightarrow & 0 \\ & & \big\downarrow{\scriptstyle ad_{M_0}} & & \big\downarrow{\scriptstyle ad_M} & & \big\downarrow{\scriptstyle ad_{M_1}} & & \\ 0 & \longrightarrow & A \otimes_{A_L} M_0 & \longrightarrow & A \otimes_{A_L} M & \longrightarrow & A \otimes_{A_L} M_1 & \longrightarrow & 0 \end{array} \tag{5.9}$$

where rows are exact. If we again apply this to the case $M_0 := \pi^{m-1}M$, then by induction, the arrows on the left and the right are exact, and so is the arrow in the middle. □

Via Proposition 5.4.5, Proposition 5.4.3, Proposition 5.2.2, and Proposition 5.2.4, we obtain that if we restrict on the case of π^m-torsion modules, then the two sub-categories of $\mathrm{Rep}_{\mathcal{O}}(G_L)$ and $\mathrm{Mod}^{\mathrm{et}}(\mathscr{A}_L)$ are equivalent, and the functors $\mathscr{D}$ and $\mathscr{V}$ are exact and quasi-inverse of each other.

5.5 The general case

In order to pass to the general case, we will use the inverse limit argument, and apply the result of the previous section, for π^m-torsion modules. In order to do this, we need the following

Lemma 5.5.1. *Let $D_0 \subseteq D$ be DVRs with the same prime element π, and D is complete. If N is a finitely generated D_0-module, then*

$$D \otimes_{D_0} N = \varprojlim_m D \otimes_{D_0} (N/\pi^m N)$$

Proof. Since we can write $N = \bigoplus_{i=1}^{j} D_0/\pi^{n_i} D_0$, and both $\otimes$ and $\varprojlim_m$ are additive, it is sufficient to prove for the case $N = D_0/\pi^n D_0$. If $n \neq \infty$, then for $m \geq n$, $\pi^m N = 0$, and this yields directly that the statement holds. When $n = \infty$, i.e. $N \cong D_0$ as D_0-modules, we have $D \otimes_{D_0} N = D$, and $\varprojlim_m D \otimes_{D_0} (N/\pi^m N) = \varprojlim_m D/\pi^m D$. Since D is complete, we have $D = \varprojlim_m D/\pi^m D$. □

Using this, we can now deduce facts about the functor $\mathscr{D}$.

Lemma 5.5.2. *For any V in $Rep_{\mathcal{O}}(G_L)$, we have*

1. *$\mathscr{D}(V) = \varprojlim_m \mathscr{D}(V/\pi^m V)$*
2. *The natural map $\mathscr{D}(V/\pi^{m+1}V)$ to $\mathscr{D}(V/\pi^m V)$ is surjective,*
3. *If $0 \to V_0 \to V \to V_1 \to 0$ is exact, then $0 \to \mathscr{D}(V_0) \to \mathscr{D}(V) \to \mathscr{D}(V_1) \to 0$ is also exact.*

Proof. 1. We have

$$\mathscr{D}(V) = (A \otimes V)^{H_L} = (\varprojlim_m A \otimes_{\mathcal{O}} V/\pi^m V)^{H_L} = \varprojlim_m (A \otimes_{\mathcal{O}} V/\pi^m V)^{H_L} = \varprojlim_m \mathscr{D}(V/\pi^m V)$$

where the second identity follows from Lemma 5.5.1, the third identity follows from the fact that $\varprojlim_m$ is commutative with $(.)^{H_L}$.

2. This follows from the short exact sequence

$$0 \to \pi^m V/\pi^{m+1} V \to V/\pi^{m+1} V \to V/\pi^m V \to 0$$

and the case of π^m-torsion modules.

3. By 1, the statement is equivalent to prove that

$$0 \to \varprojlim_m \mathscr{D}(V_0/\pi^m V_0) \to \varprojlim_m \mathscr{D}(V/\pi^m V) \to \varprojlim_m \mathscr{D}(V_1/\pi^m V_1) \to 0$$

is exact. But it follows from the fact that

$$0 \to \mathscr{D}(V_0/\pi^m V_0) \to \mathscr{D}(V/\pi^m V) \to \mathscr{D}(V_1/\pi^m V_1) \to 0$$

is exact, for any m, due to the case π^m-torsion modules. □

With this lemma at hand, we have

Proposition 5.5.3. *For all V in $Rep_{\mathcal{O}}(G_L)$, then $\mathscr{D}(V)$ satisfies (D1) and (D3) and $\mathscr{D}$ is an exact functor.*

Proof. For (D1), there exists an exact sequence

$$0 \to V^{\mathrm{tor}} \to V \to V/V^{\mathrm{tor}} \to 0$$

in $\mathrm{Rep}_{\mathcal{O}}(G_L)$, where V^{tor} is the torsion part of V. We can see that V^{tor} is π^m-torsion, for some $m \geq 1$. Hence, $\mathscr{D}(V^{\mathrm{tor}})$ is a finitely generated A_L-module, due to the case π^m-torsion. And V/V^{tor} is free finitely generated $\mathcal{O}$-module. And since $\mathscr{D}$ is exact by the lemma above, it is sufficient to have (D1) for the case V is free, finitely generated $\mathcal{O}$-module.

One has $\mathscr{D}(V) = \varprojlim_m \mathscr{D}(V/\pi^m V)$, and from the exact sequence $\pi^m V \to V \to V/\pi^m V \to 0$, we have $\mathscr{D}(V/\pi^m V) = \mathscr{D}(V)/\pi^m \mathscr{D}(V)$. Let $e_1, ..., e_d$ be an E_L-basis for $\mathscr{D}(V)/\pi\mathscr{D}(V) = \mathscr{D}(V/\pi V)$. By Nakayama's lemma, $e_1, ..., e_d$ is also a basis for the free $A_L/\pi^m A_L$-module $\mathscr{D}(V)/\pi^m \mathscr{D}(V)$ (note that the freeness follows since for $\mathscr{D}(V/\pi^m V)$, $\mathscr{D}$ preserves elementary divisors). And this yields $e_1, ..., e_d$ is also a basis for the free A_L-module $\mathscr{D}(V) = \varprojlim_m \mathscr{D}(V)/\pi^m \mathscr{D}(V)$. And this yields $\mathscr{D}(V)$ satisfies (D1).

From the finite generation of $\mathscr{D}(V)$, we can now apply Lemma 5.5.1, to obtain

$$A \otimes_{A_L} \mathscr{D}(V) = \varprojlim_m A \otimes_{A_L} (\mathscr{D}(V)/\pi^m \mathscr{D}(V)) = \varprojlim_m A \otimes_{A_L} \mathscr{D}(V/\pi^m V) = \varprojlim_m A \otimes_{\mathcal{O}} V/\pi^m V = A \otimes_{\mathcal{O}} V$$

where the third identity follows from (D3) for the case of π^m-torsion modules, and the last equality follows from Lemma 5.5.1 again.

The exactness of $\mathscr{D}$ follows from Lemma 5.5.2 above. □

By the similar argument, we also obtain that $\mathscr{V}$ satifies (V1) and (V3), and it is also an exact functor. We conclude this section by the main theorem

Theorem 5.5.4. *The functors $\mathscr{D} : Rep_{\mathcal{O}}(G_L) \to Mod^{et}(\mathscr{A}_L)$ and $\mathscr{V} : Mod^{et}(\mathscr{A}_L) \to Rep_{\mathcal{O}}(G_L)$ are well-defined exact functors and quasi-inverse of each other. Moreover, they preserve elementary divisors.*

Proof. By the arguments above, $\mathscr{D}$ satifies (D1), and (D3), and hence $\mathscr{D}$ is well-defined, and is exact. Similarly, $\mathscr{V}$ satisfies (V1), (V3) and $\mathscr{V}$ is also well-defined, and exact. Applying Lemma 5.2.5 that they are inverse of each other. □

5.6 Application II: The case of rank 1 representations

We are now interested in the case of free modules of rank 1. Due to Lemma 5.2.5, $\mathscr{D}$ and $\mathscr{V}$ preserve elementary divisors, and hence, they send free modules of rank 1 to free modules of rank 1. We will prove in this section that all rank 1 Galois representations and rank 1 (φ_L, Γ_L)-modules come from the twist of characters.

Let V in $\mathrm{Rep}_{\mathcal{O}}(G_L)$ be such a module, then because $V \cong \mathcal{O}$ as $\mathcal{O}$-modules, so to understand the action from G_L to V, it is sufficient to look at how G_L acts on $\mathcal{O}$. Let us denote $\psi(\gamma) := \gamma(1)$, for $\gamma \in G_L$, then it can be seen that $\gamma(1) \in \mathcal{O}^\times$, and this yields a continuous homomorphism $\psi : G_L \to \mathcal{O}^\times$.

Conversely, let $\psi : G_L \to \mathcal{O}^\times$ be any continuous character, then there exists an open subset N_m of G_L such that $\psi(N_m) \subseteq 1 + p^m\mathcal{O}$. We can then twist $\mathcal{O}$ as follows. Let $\mathcal{O}(\psi)$ be an $\mathcal{O}$-module, identical with $\mathcal{O}$ as $\mathcal{O}$-module, but the action from G_L is defined as

$$\begin{aligned} G_L \times \mathcal{O}(\psi) &\longrightarrow \mathcal{O}(\psi) \\ (\gamma, c) &\longmapsto \psi(\gamma)c \end{aligned}$$

then

Lemma 5.6.1. *$\mathcal{O}(\psi)$ with the G_L actions defined as above is in $Rep_{\mathcal{O}}(G_L)$.*

Proof. We can see easily that G_L acts linearly on $\mathcal{O}(\psi)$. It is sufficient to prove that the action from G_L is continuous on $\mathcal{O}(\psi)$. Let $\psi(\gamma)c + p^m\mathcal{O}$ be an open neighborhood of $\psi(\gamma)c$ in $\mathcal{O}$. By using N_m defined as above, we have

$$(\gamma N_m, c + p^m\mathcal{O}) \subseteq \psi(\gamma)(1 + p^m\mathcal{O})(c + p^m\mathcal{O}) \subseteq \psi(\gamma)c + p^m\mathcal{O}$$

It then follows that the action is continuous. □

Lemma 5.6.2. *If $\psi : G_L \to \mathcal{O}^\times$ is not a trivial character, then $\mathcal{O}$ is not isomorphic to $\mathcal{O}(\psi)$ in $Rep_{\mathcal{O}}(G_L)$.*

Proof. Assume that

$$\begin{aligned} \alpha : \mathcal{O} &\longrightarrow \mathcal{O}(\psi) \\ f &\longmapsto fe \end{aligned}$$

is an isomorphism between the two modules in $\mathrm{Rep}_{\mathcal{O}}(G_L)$, where $e \in \mathcal{O}^\times$ is a generator of $\mathcal{O}(\psi)$ as $\mathcal{O}$-module. Then for all $f \in \mathcal{O}, \gamma \in G_L$, we have

$$\alpha({}^\gamma f) = fe = {}^\gamma\alpha(f) = {}^\gamma(fe) = f{}^\gamma e$$

It then follows that $e = \psi(\gamma)e$, and hence $\psi(\gamma) = 1$, i.e. γ is the trivial character. □

And this yields

Proposition 5.6.3. *Any free module of rank 1 in $Rep_{\mathcal{O}}(G_L)$ comes from twist of $\mathcal{O}$ by a continuous character.*

We can now take a look what happens in the side of etale (φ_L, Γ_L)-modules of rank 1. It can be seen from the definition that $\mathscr{A}_L$ is an etale module of rank 1. Then for any character $\chi : \Gamma_L \to \mathcal{O}^\times$, we can define the twist module $\mathscr{A}_L(\chi)$ with the $\mathscr{A}_L$ module structure is identical with $\mathscr{A}_L$, and the action from Γ_L is defined as

$${}^\gamma f := \chi(\gamma)\chi_L(\gamma) \cdot f = (\chi\chi_L)(\gamma) \cdot f$$

Then $\mathscr{A}_L(\chi)$ also an etale free module of rank 1.

Lemma 5.6.4. *If χ is not a trivial character, then $\mathscr{A}_L$ is not isomorphic to $\mathscr{A}_L(\chi)$ in $Mod^{et}(\mathscr{A}_L)$.*

Proof. Assume that

$$\begin{aligned} \alpha : \mathscr{A}_L &\longrightarrow \mathscr{A}_L(\chi) \\ f &\longmapsto fe \end{aligned}$$

is an isomorphism between two etale modules, then for all $f \in \mathscr{A}_L, \gamma \in \Gamma_L$, we have

$$\alpha({}^\gamma f) = {}^\gamma\alpha(f) = {}^\gamma(fe)$$

We have $\alpha({}^\gamma f) = (\chi_L(\gamma)\cdot f)e$, and ${}^\gamma(fe) = (\chi\chi_L)(\gamma)\cdot(fe)$. Then $(\chi_L(\gamma)\cdot f)e = (\chi\chi_L)(\gamma)\cdot(fe)$ if and only if

$$f(\chi_L^{-1}(\gamma)\cdot e) = \chi(\gamma)\cdot(fe) = (\chi(\gamma)\cdot f)(\chi(\gamma)\cdot e) \tag{5.10}$$

If e is a constant, we have $\chi_L^{-1}\cdot e = \chi(\gamma)\cdot e = e$, and this yields by (5.10) that $f = \chi(\gamma)\cdot f$ for all $f \in \mathscr{A}_L, \gamma \in \Gamma_L$, and hence χ is the trivial character.

If e is not a constant, then for any $a \neq b$ in $\mathcal{O}^\times$, we have

$$e([a]_\phi(X)) \neq e([b]_\phi(X))$$

since $[a]_\phi(X) = aX + ...$, and when $f = 1$, by (5.10), we have

$$\chi_L^{-1}(\gamma)\cdot e = \chi(\gamma)\cdot e$$

for all $\gamma \in \Gamma_L$, and this follows that $\chi = \chi_L^{-1}$. And from (5.10) again, we have for all $f \in \mathscr{A}_L, \gamma \in \Gamma_L$

$$f = \chi_L^{-1}(\gamma)\cdot f$$

And this yields χ_L^{-1} is the trivial character, a contradiction. □

We are now able to see that all free etale modules of rank one, in the case $L := \mathbb{Q}_p$ with cyclotomic extension, come from twist, too. If we begin with $\psi : G_L \to \mathcal{O}^\times$ is any continuous character, then for any $N \subseteq \mathcal{O}^\times$: an open subgroup, then $\psi^{-1}(N)$ is also an open normal subgroup of G_L of finite index (since N is of finite in $\mathcal{O}^\times$), and $G_L/\psi^{-1}(N)$ is a finite abelian group, which is a Galois group of an abelian extension of L. It means that this quotient group is a quotient group of $G_L^{\mathrm{ab}} = \mathrm{Gal}(L^{\mathrm{ab}}/L)$. Moreover, via ψ, $G_L/\psi^{-1}(N)$ maps to $\mathcal{O}^\times/N$. Taking the limit when N runs through all open subgroups of $\mathcal{O}^\times$, we obtain a map from $H := \varprojlim G_L/\psi^{-1}(N)$ to $\varprojlim \mathcal{O}^\times/N \cong \mathcal{O}^\times$. It can be seen that H is a quotient group of $G_L^{\mathrm{ab}} \cong \Gamma_L \times \mathrm{Gal}(L^{\mathrm{ur}}/L)$. And by using the embedding map $\Gamma_L \hookrightarrow G_L^{\mathrm{ab}}$, we then obtain an induced character $\chi : \Gamma_L \to \mathcal{O}^\times$. Since for the case $L = \mathbb{Q}_p$, we can factor $\psi = \chi_L^a\psi_0$, for some $a \in \mathbb{Z}_p$ and ψ_0 is an unramified character. And in this case, via the functors of the two categories, we can see that $\mathscr{D}(\mathcal{O}(\psi)) \cong \mathscr{A}_L(\chi)$.

Conversely, if we begin with $\chi : \Gamma_L \to \mathcal{O}^\times$ is any character, then because $\mathcal{O}^\times$ is a profinite group, and so is Γ_L, by the universal property of profinite group, we can lift χ to $\chi^c : \Gamma_L \to \mathcal{O}^\times$, where χ^c is continuous. And we then obtain from this a continuous character $\psi : G_L \to \mathcal{O}^\times$ as the composition of the two continuous maps

$$G_L \to \Gamma_L \xrightarrow{\chi^c} \mathcal{O}^\times$$

And via the functors again, we obtain $\mathscr{V}(\mathscr{A}_L(\chi)) \cong \mathcal{O}(\psi)$. We hence obtain

Proposition 5.6.5. *In the case $L = \mathbb{Q}_p$ with cyclotomic extension, all free rank one modules in $Mod^{et}(\mathscr{A}_L)$ comes from a twist of $\mathscr{A}_L$ by a character from Γ_L to $\mathcal{O}^\times$.*

5.7 Application III: Another proof for the p-cohomological dimension of $G_{\mathbb{Q}_p}$

In this section, we will sketch another the proof about p-cohomological dimension of $G_{\mathbb{Q}_p}$ is not larger than 2, by [Her98]. We restrict ourselves to the case $L := \mathbb{Q}_p, \pi := p$, and L_∞ in this case is $\mathbb{Q}_p^\infty$, the field obtained from $\mathbb{Q}_p$ by adjoining all p^n-th root of unity. We denote $\mathbb{F}_p((X)) = E_L =: E, \Gamma := \Gamma_L \cong \mathbb{Z}_p^\times, G := G_{\mathbb{Q}_p}$. Note that in this case Γ is a procyclic group with a (topological) generator γ. We also denote $\mathrm{Rep}_{p-tor}(G_{\mathbb{Q}_p})$ the subcategory of $\mathrm{Rep}_{\mathbb{Z}_p}(G_{\mathbb{Q}_p})$ containing p-torsion modules, and similarly for $\mathrm{Mod}^{\mathrm{et}}_{p-tor}(\mathscr{A}_{\mathbb{Q}_p})$. By results from Section 3 of this chapter, $\mathrm{Rep}_{p-tor}(G_{\mathbb{Q}_p})$ and $\mathrm{Mod}^{\mathrm{et}}_{p-tor}(\mathscr{A}_{\mathbb{Q}_p})$ are equivalent via functors $\mathscr{D}$ and $\mathscr{V}$.

We recall a theorem of Grothendieck: Assume that $\mathscr{C}$, $\mathscr{D}$ are abelian categories such that $\mathscr{C}$ has enough injectives, and $(T_n)_{n\geq 0}$ is a δ-functor from $\mathscr{C}$ to $\mathscr{D}$. If $(T_n)_{n>0}$ is effaceable, then T^0 is left exact and T^n is isomorphic to the n-th derived functors R^nT^0.

Let us consider the category $\mathscr{C} := \varinjlim \mathrm{Mod}^{\mathrm{et}}_{p-tor}(\mathscr{A}_{\mathbb{Q}_p})$, whose objects are injective limits of objects in $\mathrm{Mod}^{\mathrm{et}}_{p-tor}(\mathscr{A}_{\mathbb{Q}_p})$, then $\mathscr{C}$ is abelian with enough injectives. And $\mathrm{Mod}^{\mathrm{et}}_{p-tor}(\mathscr{A}_{\mathbb{Q}_p})$ is a subcategory of $\mathscr{C}$ is an obvious way.

For any object M in $\mathscr{C}$, we define the **Herr's complex**

$$C(M) : 0 \to M \xrightarrow{\alpha} M \oplus M \xrightarrow{\beta} M \to 0 \to 0 \to ...$$

where $\alpha(x) = ((\varphi_M - 1)x, (\gamma - 1)x)$, and $\beta(y, z) = (\gamma - 1)y - (\varphi_M - 1)z$. And one can define a functor

$$\begin{aligned} \mathfrak{H}^n : \mathscr{C} &\longrightarrow \mathrm{Ab} \\ M &\longmapsto H^n(C(M)) \end{aligned}$$

And the key result of Herr [Her98] is that $\mathfrak{h}^n$ is effaceable for $n > 0$, and hence, $\mathfrak{h}^n$ is just the n-th right derived functors of $\mathfrak{h}^0$, where $\mathfrak{h}^0(M) = M^{\varphi_M=1,\gamma=1}$. Using this, we can prove that

Theorem 5.7.1. *Let V be an object in $\mathrm{Rep}_{p-tor}(G_{\mathbb{Q}_p})$, then $H^n(G, V) = 0$, for all $n \geq 3$.*

Proof. The functor

$$\begin{aligned} (.)^G : \mathrm{Rep}_{p-tor}(G_{\mathbb{Q}_p}) &\longrightarrow \mathrm{Ab} \\ V &\longmapsto V^G \end{aligned}$$

has its n-th derived functor $H^n(G, -)$. And

$$V^G = \mathscr{V}(\mathscr{D}(V))^G = ((E^{\mathrm{sep}} \otimes_E \mathscr{D}(V))^{\phi_p \otimes \varphi_{\mathscr{D}(V)}=1})^G = ((E^{\mathrm{sep}} \otimes_E \mathscr{D}(V))^G)^{\phi_p \otimes \varphi_{\mathscr{D}(V)}=1}) =$$

$$= \mathscr{D}(V)^{\varphi_{\mathscr{D}(V)}=1,\gamma=1} = \mathfrak{h}^0(\mathscr{D}(V))$$

This yields the derived functors $H^n(G, -)$ and $\mathfrak{h}^n(\mathscr{D}(-))$ are just the same. And it follows easily from the Herr's complex that $H^n(G, V) = 0$, for $n \geq 3$. $\square$

Bibliography

[Fon90] J.-M. Fontaine. Representations p-adiques des corps locaux. *The Grothendieck Festschrift*, pages 249–309, 1990.

[FV02] I.B. Fesenko and S.V. Vostokov. Local fields and their extensions. *Translations of mathematical monographs, volume 121*, 2002.

[FW79] J.-M. Fontaine and J.-P. Wintenberger. Extensions algebriques et corps des normes des extensions apf des corps locaux. *C. R. Acad. Sci. Paris Ser. A-B*, 8:A441–A444, 1979.

[Her98] L. Herr. Sur la cohomologie galoisienne des corps p-adiques. *Bull. Soc. Math. France, 126*, pages 563–600, 1998.

[Ked15] K. Kedlaya. *New methods for (phi, Gamma)-modules.* arXiv: 1307.2937v2, 2015.

[KR09] M. Kisin and W. Ren. Galois representations and lubin-tate groups. *Documenta Math.*, pages 441–461, 2009.

[LT65] J. Lubin and J. Tate. Formal complex multiplication in local fields. *Annals of Mathematics, Second Series, 81*, page 380–387, 1965.

[Mil13] J. Milne. *Class Field Theory.* available at http://www.jmilne.org/math/CourseNotes/CFT.pdf, 2013.

[NSW00] J. Neukirch, A. Schmidt, and K. Wingberg. Cohomology of number fields. *A Series of Comprehensive Studies in Mathematics*, 2000.

[Sch12] P. Scholze. Perfectoid spaces. *Publ. Math. IHES*, 116:245–313, 2012.

[Sch17] P. Schineider. *Galois representation and (phi, Gamma)-modules.* Cambridge studies in advanced mathematics, 2017.

[SV16] P. Schneider and O. Venjakob. Coates-wiles homomorphisms and iwasawa cohomology for lubin-tate extensions. *Springer Proc. Math. Stat, Springer*, 2016.

[Win83] J.-P. Wintenberger. Le corps des normes de certaines extensions infinies de corps locaux;application. *Ann. Sci. ENS*, pages 59–89, 1983.

Index