

# Explicit Local Class Field Theory à la Lubin and Tate with an Application to Algebraic Topology\*

Hongxiang Zhao

## Abstract

This is part of my senior thesis. The thesis has two goals. Firstly, we state and prove explicit local class field theory à la Lubin and Tate. Secondly, we prove the existence and uniqueness of Ando's norm-coherent coordinates on deformations of formal groups in the context of structured multiplicative orientations in algebraic topology. The first part is almost finished, while the second part is only a sketch proof.

## Contents

<b>1</b>	<b>Brief History of Local Class Field Theory</b>	<b>2</b>
<b>2</b>	<b>Main Theorems of Local Class Field Theory and Proof by Lubin-Tate Formal Group Laws</b>	<b>3</b>
2.1	Statements of the Main Theorems . . . . .	3
2.2	Lubin-Tate Formal Group Laws . . . . .	7
2.3	Construction of $K_\pi$ and the Local Artin Map . . . . .	9
2.4	Local Kronecker-Weber Theorem . . . . .	13
2.5	End of the Proof . . . . .	14
<b>3</b>	<b>Proof of Ando's Criterion via Coleman Norm Operator</b>	<b>16</b>
	<b>Bibliography</b>	<b>20</b>

---

\*Last update: Dec 5th, 2022.

# 1 Brief History of Local Class Field Theory

The motivation of class field theory is to generate all the Galois extensions of a field. In particular, local class field theory wants to generate all the Galois extensions of a local field.

Historically, local class field theory arises from the problem proposed by Emil Artin(1929) that whether one can generalize the norm residue symbol to arbitrary fields that do not contain  $n$ -th roots of unity [4]. Helmut Hasse(1930) solved this problem using the global Artin reciprocity law. For an abelian extension  $L/K$ , where  $K, L$  may not be local fields, and  $\alpha \in K^*$  and  $v$  a place of  $K$ , the new norm residue symbol  $(\alpha, L/K)_v$  is an element in the decomposition group of any  $w \mid v$  [3] (Since  $L/K$  is abelian, all decomposition groups are the same). This led Hasse to the discovery of local class field theory. We first need a lemma to see this.

**Lemma 1.1.** *Suppose  $F/K_v$  is a field extension for some number field  $K$  and a finite place  $v$  of  $K$ . Then there exists a number field  $L/K$  such that  $F = LK_v$ ,  $[L : K] = [F : K_v]$  and  $F = L_w$  for some place  $w$  of  $L$  extending  $v$ .*

*Proof.* Suppose  $F = K_v(\alpha)$  and  $f \in K_v[X]$  is the minimal polynomial of  $\alpha$  over  $K_v$ . By Corollary 3.2.16 in [5], there is a separable and irreducible polynomial  $g \in K[X]$  close enough to  $f$  with  $\deg(g) = \deg(f)$  such that  $K_v(\beta) = K_v(\alpha)$  for some root  $\beta$  of  $g$ . Then  $[F : K_v] = \deg(f) = \deg(g) = [K(\beta) : K]$ . Since  $F$  is a finite extension of a complete field  $K_v$ ,  $F$  is itself complete. Since  $F \supset L$ ,  $F$  is a completion of  $L$  with respect to some valuation  $w$  of  $L$ .  $\square$

Here is how local class field theory shows up: Given an abelian extension  $F/K_v$ , there exists a field extension  $L/K$  such that  $F = LK_v$ ,  $[L : K] = [F : K_v]$  and  $F = L_w$  for some place  $w$  of  $L$  extending  $v$  by the lemma. Thus,  $\text{Gal}(F/K_v) \cong \text{Gal}(L_w/K_v)$ . Note that there is a natural inclusion  $\text{Gal}(L_w/K_v) \rightarrow \text{Gal}(L/K)$  by  $\sigma \mapsto \sigma|_L$ , mapping  $\text{Gal}(L_w/K_v)$  to the decomposition group of  $w \mid v$ . For any  $\alpha \in K^*$ , let  $(\alpha, F/K_v)$  be the image of  $(\alpha, L/K)_v$  in  $\text{Gal}(F/K_v)$ . Therefore, we get a homomorphism

$$K^* \rightarrow \text{Gal}(F/K_v) \quad \alpha \mapsto (\alpha, F/K_v)$$

The definition of  $(\alpha, L/K)_v$  implies that  $(\alpha, L/K)_v = \text{Id}$  when  $v(\alpha)$  is large enough [3]. Thus, the above map can be extended to  $K_v^* \mapsto \text{Gal}(F/K_v)$ , which is now called the local Artin map.

As discussed above, local class field theory is derived from the global class field theory originally and there is no explicit description of the local Artin map. The significance of the

proof by Lubin and Tate is to give an explicit description of the local Artin map.

## 2 Main Theorems of Local Class Field Theory and Proof by Lubin-Tate Formal Group Laws

### 2.1 Statements of the Main Theorems

By a local field, we mean a field  $K$  that is one of the following case:

1.  $K = \mathbb{R}$  or  $K = \mathbb{C}$  with the usual absolute value.
2.  $K$  is complete with respect to a discrete valuation whose valuation ring has finite residue field.

By Proposition 4.1.4 in [5], the latter case is either a finite extension of  $\mathbb{Q}_p$  or a finite extension of  $\mathbb{F}_p((t))$ . The former one is called **archimedean** while the latter case is called **non-archimedean**.

Let  $K$  be a local field,  $K^{al} \supset K^{ab} \supset K^{un}$  be its separable and abelian closure respectively. Let  $\mathcal{O}_K$  be the integer ring of  $K$  and  $\mathfrak{m}$  be the maximal ideal of  $\mathcal{O}_K$  and  $k = \mathcal{O}_K/\mathfrak{m}$  is the residue field with  $q$  elements, where  $q$  is a power of a prime number  $p$ . Suppose  $L/K$  is a finite extension,  $\text{Nm}_{L/K}(x)$  is the norm of  $x \in L$  with respect to  $L/K$ .

Let  $\text{Gal}(K^{ab}/K)$  be the Galois group of  $K^{ab}/K$ . We assign Krull topology to  $\text{Gal}(K^{ab}/K)$ , i.e.,  $\text{Gal}(K^{ab}/E)$  forms a fundamental system of neighborhoods of 1 in  $\text{Gal}(K^{ab}/K)$ , where  $E$  runs through all finite abelian extensions of  $K$ .

The main theorems of the abelian local class field theory are the following:

**Theorem 2.1** (Local Reciprocity Law). *For any non-archimedean local field  $K$ , there exists a unique homomorphism*

$$\phi_K: K^* \rightarrow \text{Gal}(K^{ab}/K)$$

*satisfying:*

- (a) *For any uniformizer  $\pi$  of  $K$ ,  $\phi_K(\pi)$  is the Frobenius element of  $\text{Gal}(K^{un}/K)$  under the restriction  $\text{Gal}(K^{ab}/K) \rightarrow \text{Gal}(K^{un}/K)$ .*

(b) For any finite abelian extension  $L$  of  $K$ , there is an exact sequence:

$$1 \rightarrow \text{Nm}_{L/K}(L^*) \rightarrow K^* \rightarrow \text{Gal}(L/K) \rightarrow 1$$

where the latter map is the composition of  $\phi_K$  and the restriction map. This induces an isomorphism

$$\phi_{L/K}: K^*/\text{Nm}_{L/K}(L^*) \rightarrow \text{Gal}(L/K)$$

In particular,  $(K^* : \text{Nm}_{L/K}(L^*)) = [L : K]$ .

The map  $\phi_{L/K}$  is then called the **local Artin map**.

The following corollary can be deduced from Theorem 2.1.

**Corollary 2.2.** *Let  $K$  be a non-archimedean local field. Assume that Theorem 2.1 is true. Then*

- (a) *The map  $L \mapsto \text{Nm}(L^*)$  is an order-reversing bijection between abelian extensions of  $K$  and norm groups in  $K^*$ .*
- (b)  $\text{Nm}((L \cdot L')^*) = \text{Nm}(L^*) \cap \text{Nm}(L'^*)$ .
- (c)  $\text{Nm}((L \cap L')^*) = \text{Nm}(L^*) \cdot \text{Nm}(L'^*)$
- (d) *Every subgroup of  $K^*$  containing a norm group is a norm group itself.*

*Proof.* See [7] Corollary 1.2. □

**Theorem 2.3** (Local Existence Theorem). *The norm groups in  $K^*$  are exactly the open subgroups of finite index.*

Thus, the remaining of this section is to prove Theorem 2.1 and Theorem 2.3.

The following remarks of the main theorems are essential to the proof. Recall in the finite case, if  $L/K$  is a totally ramified extension of degree  $n$  and  $F/K$  is an unramified extension of degree  $m$ , then  $LF/K$  is of degree  $mn$  (Here we do not require  $K, L, F$  to be local fields). Actually  $K^{ab}$  can also be decomposed into the composition of a maximal unramified extension and a maximal totally ramified extension as follows.

Given the isomorphisms

$$\phi_{L/K}: K^*/\text{Nm}(L^*) \rightarrow \text{Gal}(L/K) \cong \text{Gal}(K^{ab}/K)/\text{Gal}(K^{ab}/L)$$

for each finite abelian extension  $L$  of  $K$ , by passing to the limit we get an isomorphism:

$$\hat{\phi}_K: \widehat{K^*} \rightarrow \text{Gal}(K^{ab}/K)$$

where  $\widehat{K^*}$  is the profinite completion of  $K^*$  since  $\text{Nm}(L^*)$  are all open subgroups of finite index in  $K^*$  by Theorem 2.3.

Now choose an uniformizer  $\pi$  of  $K$ . We have

$$K^* \cong U_K \times \pi^{\mathbb{Z}} \cong U_K \times \mathbb{Z}$$

**Lemma 2.4.** *Under the decomposition above,  $\lim_{n \in \mathbb{N}^*, m \in \mathbb{N}^*} K^*/((1 + \mathfrak{m}^n) \times m\mathbb{Z}) \cong \widehat{K^*}$ .*

*Proof.* It suffices to show that for any open subgroup of finite index  $H$  in  $K^*$ ,  $H$  contains some  $(1 + \mathfrak{m}^n) \times m\mathbb{Z}$ . Since  $H$  is open and  $(1 + \mathfrak{m}^n) \times \{0\}$  forms a fundamental system of neighborhoods of 1 in  $K^*$ ,  $H \supset (1 + \mathfrak{m}^n) \times \{0\}$  for some  $n$ . Moreover,  $H$  contains a  $u\pi^r$  for some integer  $r$  and  $u \in U_K$ . Since  $U_K/(1 + \mathfrak{m}^n)$  is a finite group,  $u^s \in (1 + \mathfrak{m}^n)$  for some integer  $s$ . Therefore,  $H \supset (1 + \mathfrak{m}^n) \times rs\mathbb{Z}$ .  $\square$

Then we have

$$\widehat{K^*} \cong U_K \times \pi^{\hat{\mathbb{Z}}} \cong U_K \times \hat{\mathbb{Z}}$$

It is well-known that profinite topological groups are equivalent to compact Hausdorff totally disconnected topological groups. Since  $U_K, \hat{\mathbb{Z}}$  are profinite, they are compact. Because  $\widehat{K^*}$  is Hausdorff, both  $U_K, \hat{\mathbb{Z}}$  are closed subgroups in  $\widehat{K^*}$ . Since  $\mathbb{Z}$  is dense in  $\hat{\mathbb{Z}}$ ,  $\hat{\mathbb{Z}} = \overline{\mathbb{Z}}$  in  $\widehat{K^*}$ . Let  $K_\pi = (K^{ab})^{\hat{\phi}_K(\pi)}$  and  $K^{un} = (K^{ab})^{\hat{\phi}_K(U_K)}$ . Then by infinite Galois theory,  $\text{Gal}(K^{ab}/K_\pi) = \hat{\mathbb{Z}}$  and  $\text{Gal}(K^{ab}/K^{un}) = U_K$ . Thus,  $K_\pi$  is the union of finite abelian extensions  $L$  such that  $\pi \in \text{Nm}(L^*)$ , which are totally ramified, and  $K^{un}$  is the union of finite abelian extensions  $L$  such that  $\text{Nm}(L^*) \supset U_K$ , which are unramified. We deduce that  $K^{un}$  is the maximal unramified extension of  $K$  in  $K^{ab}$  and  $K^{un} \cap K_\pi = K$ . Thus,  $\text{Gal}(K_\pi K^{un}/K) = \text{Gal}(K_\pi/K) \times \text{Gal}(K^{un}/K) = U_K \times \hat{\mathbb{Z}}$ . Hence,  $K^{ab} = K_\pi K^{un}$ .

Under such view of point, we can show the uniqueness of  $\phi_K$ .

**Lemma 2.5.** *Assume that Theorem 2.3 is true. Then there exists at most one homomorphism  $\phi: K^* \rightarrow \text{Gal}(K^{ab}/K)$  satisfying the conditions in Theorem 2.1.*

*Proof.* We know that  $K^{ab} = K^{un} K_\pi$ . If there is a  $\phi$  satisfies the conditions in Theorem 2.1,

then  $\phi(\pi)|_{K^{un}}$  is the Frobenius element for any uniformizer  $\pi$  of  $K$ . Since  $K_\pi$  is fixed by  $\phi(\pi)$  from above discussion. The value of  $\phi(\pi)$  is determined for all uniformizer  $\pi$ . Since  $K^*$  is generated by uniformizers  $\pi$  of  $\mathcal{O}_K$ , the value of  $\phi$  is uniquely determined.  $\square$

Since we know the restriction of the local Artin map on  $K^{un}$  is the Frobenius element, we may prove the existence by constructing the fields  $K^{un}$ ,  $K_\pi$  and the restriction of local Artin map  $U_K \rightarrow \text{Gal}(K_\pi/K)$ . Then we need to show that the composition  $K_\pi K^{un}$  and the associated map  $\phi_\pi$  are independent of the choice of  $\pi$ . Next, we show that  $K_\pi K^{un} = K^{ab}$ . Finally, we have to show that  $\phi_\pi$  satisfies the condition (b) of Theorem 2.1.

**Example 2.6.** Suppose  $K = \mathbb{Q}_p$  for some prime number  $p$  and pick the uniformizer  $\pi = p$ . By Kummer-Dedekind Theorem, for each positive integer  $n$ ,  $\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p$  is unramified if  $(n, p) = 1$  and is totally ramified if  $n = p^i$  for some positive integer  $i$ . Moreover, the Galois group  $\text{Gal}(\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p)$  is  $(\mathbb{Z}/n\mathbb{Z})^*$ . By taking the colimit, we see that the Galois groups of  $\left(\bigcup_{(n,p)=1} \mathbb{Q}_p(\mu_n)\right)/\mathbb{Q}_p$  and  $\left(\bigcup_{i=1}^{\infty} \mathbb{Q}_p(\mu_{p^i})\right)/\mathbb{Q}_p$  are  $\hat{\mathbb{Z}}$  and  $(\mathbb{Z}_p)^*$  respectively. Thus, we have

$$(\mathbb{Q}_p)_p = \bigcup_{i=1}^{\infty} \mathbb{Q}_p(\mu_{p^i}) \quad Q_p^{un} = \left( \bigcup_{(n,p)=1} \mathbb{Q}_p(\mu_n) \right)$$

By above discussion,

$$\mathbb{Q}_p^{ab} = \left( \bigcup_{(n,p)=1} \mathbb{Q}_p(\mu_n) \right) \cdot \left( \bigcup_{i=1}^{\infty} \mathbb{Q}_p(\mu_{p^i}) \right)$$

The above method of construction  $Q_p^{un}$  applies to arbitrary local field  $K$ . Suppose  $p \nmid n$ ,  $\mu_n$  is the primitive  $n$ -th root of unity over  $K$  and  $L = K(\mu_n)$ . Suppose  $\Phi_n(t)$  is the minimal polynomial of  $\mu_n$  over  $K$  and  $\overline{\Phi}_n(t)$  is the reduction of  $\Phi_n(t)$  to the residue field  $k$ . Thus,  $\overline{\Phi}_n(t) \mid (t^n - 1)$ , so it is separable. By Hensel's Lemma,  $\overline{\Phi}_n(t)$  is also irreducible. Thus,  $\overline{\Phi}_n(t)$  is the minimal polynomial of  $\bar{\mu}_n$  over  $k$ . Therefore,

$$[L : K] = \deg \Phi_n(t) = \deg \overline{\Phi}_n(t) = [k(\bar{\mu}_n) : k] \leq [l : k] \leq [L : K]$$

where  $l$  is the residue field of  $L$ . Hence,  $[L : K] = [l : k]$  implying that  $L/K$  is unramified. By field theory, we know that  $l = k(\bar{\mu}_n)$  is the splitting field of  $t^{q^f} - t$ , where  $f$  is the smallest number such that  $n \mid (q^f - 1)$ . Therefore,  $\left(\bigcup_{(n,p)=1} K(\mu_n)\right)/K$  is an unramified extension and has the residue field  $\bar{k}$ , implying that  $K^{un} = \bigcup_{(n,p)=1} K(\mu_n)$ .

However, we cannot simply add of roots of unity to  $K$  to construct  $K_\pi$ . Indeed, if  $K =$

$\mathbb{F}_p((t))$ , then  $K$  itself contains  $p^i$ -th roots of unity. Lubin-Tate theory generalizes this method to arbitrary local field via Lubin-Tate formal group laws. If we let  $\mathbb{G}_m$  to be the multiplication formal group law on  $\mathbb{Z}_p$ ,  $\mathbb{G}_m(X, Y) = X + Y + XY$ , then there exists a natural map  $\mathbb{Z}_p \rightarrow \text{End}(\mathbb{G}_m)$  given by the following: for any  $n \in \mathbb{Z}$ ,  $((1 + T)^n - 1) \in \text{End}(\mathbb{G}_m)$ . This can be extended to  $\mathbb{Z}_p$ . For any  $a \in \mathbb{Z}_p$ ,

$$(1 + T)^a = \sum_{m \geq 0} \binom{a}{m} T^m \quad \binom{a}{m} = \frac{a(a-1) \cdots (a-m+1)}{m(m-1) \cdots 1}$$

By continuity,  $\binom{a}{m} \in \mathbb{Z}_p$  and  $((1 + T)^a - 1) \in \text{End}(\mathbb{G}_m)$ . Then we see that  $(\mu_{p^i} - 1)$  is a  $p^n$ -torsion point. Thus,  $\mathbb{Q}_p(\mu_{p^i}) = \mathbb{Q}_p(\mu_{p^i} - 1)$  can be viewed as adding  $p^n$ -torsion points in  $\mathbb{Q}_p^{al}$ .

## 2.2 Lubin-Tate Formal Group Laws

Note that for power series  $f, g, h$ ,  $f \circ (g + h) \neq f \circ g + f \circ h$  in general. In order to make the distribution law possible, we need to rewrite the addition. Suppose  $F$  is the new addition. Then we need  $f \circ F(g, h) = F(f \circ g, f \circ h)$ . We use the formal group law to capture this.

**Definition 2.7** (One-Parameter Commutative Formal Group Law). Let  $R$  be a commutative ring. A **one-parameter commutative formal group law** is a power series  $F \in R[[X, Y]]$  such that

- (a)  $F(X, Y) \equiv X + Y \pmod{(X, Y)^2}$ .
- (b) (Associativity)  $F(X, F(Y, Z)) = F(F(X, Y), Z)$ .
- (c) (Commutativity)  $F(X, Y) = F(Y, X)$ .

We can prove that with the conditions (a)(b), there exists a unique  $i_F(T) \in R[[T]]$  such that  $F(X, i_F(X)) = 0$ .

We denote  $\text{End}(F)$  by the set of  $f \in R[[X]]$  such that  $f \circ F(X, Y) = F(f(X), f(Y))$  and  $f +_F g = F(f, g)$ . Then we see from the beginning of this subsection that  $\text{End}(F)$  admits a ring structure with the addition  $+_F$  and the multiplication  $\circ$ .

**Definition 2.8.** Let  $\mathcal{F}_\pi$  be the set of  $f(X) \in \mathcal{O}_K[[X]]$  such that

- (a)  $f \equiv \pi X \pmod{X^2}$ .

$$(b) f \equiv X^q \pmod{\pi}.$$

**Example 2.9.** Let  $K = \mathbb{Q}_p$ ,  $\pi = p$ . Then  $f(X) = (1 + X)^p - 1$  lies in  $\mathcal{F}_p$ .

**Lemma 2.10.** Let  $f, g \in \mathcal{F}_\pi$  and  $\phi_1(X_1, \dots, X_n) \in \mathcal{O}_K[X_1, \dots, X_n]$  is a linear form. Then there exists a unique  $\phi \in \mathcal{O}_K[[X_1, \dots, X_n]]$  such that

$$(a) \phi \equiv \phi_1 \pmod{(X_1, \dots, X_n)^2}.$$

$$(b) f(\phi(X_1, \dots, X_n)) = \phi(g(X_1), \dots, g(X_n)).$$

*Proof.* See [7], Lemma 2.11.

The idea is doing induction on the degree of  $\phi$  and taking the limit, i.e., show that there exists a unique polynomial  $\phi_r(X_1, \dots, X_n)$  of degree  $r$  such that  $\phi_r \equiv \phi_1 \pmod{(X_1, \dots, X_n)^2}$  and  $f(\phi_r(X_1, \dots, X_n)) \equiv \phi_r(g(X_1), \dots, g(X_n)) \pmod{(X_1, \dots, X_n)^{r+1}}$ .  $\square$

The following three propositions can be deduced by repeatedly applying the above lemma.

**Proposition 2.11.** For every  $f \in \mathcal{F}_\pi$ , there is a unique formal group law  $F_f \in \mathcal{O}_K[[X, Y]]$  admitting  $f$  as an endomorphism.

**Proposition 2.12.** For  $f, g \in \mathcal{F}_\pi$  and  $a \in \mathcal{O}_K$ , let  $[a]_{g,f}$  be the unique element of  $\mathcal{O}_K[[T]]$  such that

$$(a) [a]_{g,f} \equiv aT \pmod{T^2}.$$

$$(b) g \circ [a]_{g,f} = [a]_{g,f} \circ f.$$

Then  $[a]_{g,f}$  is a homomorphism  $F_f \rightarrow F_g$ .

**Proposition 2.13.** For any  $a, b \in \mathcal{O}_K$ ,  $[a + b]_{g,f} = [a]_{g,f} +_{F_g} [b]_{g,f}$  and  $[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}$ .

This proposition has two direct corollaries.

**Corollary 2.14.** For any  $f, g \in \mathcal{F}_\pi$ ,  $F_f \cong F_g$ .

*Proof.* Given every  $u \in \mathcal{O}_K^*$ ,  $[u]_{f,g}$  and  $[u^{-1}]_{g,f}$  are inverse to each other.  $\square$

**Corollary 2.15.** For each  $a \in \mathcal{O}_K$ , there is a unique endomorphism  $[a]_f: F_f \rightarrow F_f$  such that  $[a]_f \equiv aT \pmod{T^2}$  and  $[a]_f$  commutes with  $f$ . The map

$$\mathcal{O}_K \rightarrow \text{End}(F_f): a \mapsto [a]_f$$

is an injective ring homomorphism. In particular,  $[\pi]_f = f$ .



The formal group law  $F_f$  associated to an uniformizer  $\pi$  is called the **Lubin-Tate formal group law**.

**Example 2.16.** When  $K = \mathbb{Q}_p$ ,  $\pi = p$ ,  $f(X) = (1 + X)^p - 1$ ,  $F_f = \mathbb{G}_m$  is the multiplication group law. The power series  $[a]_f = (1 + X)^a - 1$  is the one we defined before.

### 2.3 Construction of $K_\pi$ and the Local Artin Map

For any  $f \in \mathcal{F}_\pi$ , let  $\Lambda_f = \{\alpha \in K^{al} : |\alpha| < 1\}$ . Define a  $\mathcal{O}_K$ -module structure on  $\Lambda_f$  by  $\alpha + \beta = \alpha +_{F_f} \beta = F_f(\alpha, \beta)$  and  $a \cdot \alpha = [a]_f(\alpha)$ . Let  $\Lambda_{f,n}$  be the submodule of  $\Lambda_f$  consisting of elements killed by  $[\pi]_f^n$ .

**Remark.** The canonical isomorphism  $[1]_{g,f} : F_f \rightarrow F_g$  induces isomorphisms  $\Lambda_f \rightarrow \Lambda_g$  and  $\Lambda_{f,n} \rightarrow \Lambda_{g,n}$  for each  $n$ .

**Proposition 2.17.** For each  $n$ ,  $\Lambda_{f,n} = \mathcal{O}_K/(\pi^n)$  as  $\mathcal{O}_K$ -modules. Thus,  $\text{End}(\Lambda_{f,n}) \cong \mathcal{O}_K/(\pi^n)$  and  $\text{Aut}(\Lambda_{f,n}) \cong (\mathcal{O}_K/(\pi^n))^*$ .

*Proof.* By the above remark, it suffices to take  $f = \pi X + X^q$ . Thus,  $[\pi^n]_f = \pi^n X + \dots + X^{q^n}$ . From the Newton polygon of  $[\pi^n]_f$ , we see that all the roots of  $[\pi^n]_f$  lie in  $\Lambda_{f,n}$ .

Since  $f = \pi X + X^q$  is an Eisenstein polynomial,  $f$  is irreducible and has  $q$  distinct roots. Thus,  $\Lambda_{f,1}$  has exactly  $q$  elements. By the structure theorem of modules over PID,  $\Lambda_{f,1} \cong \mathcal{O}_K/(\pi)$  since  $\mathcal{O}_K/(\pi^n)$  contains  $q^n$  elements.

For each  $\alpha \in K^{al}$  with  $|\alpha| < 1$ ,  $f(X) - \alpha = X^q + \dots + \pi X - \alpha$ . From the Newton polygon of  $f(X) - \alpha$ , we see that all roots of  $f(X) - \alpha$  lie in  $\Lambda_f$ . Therefore,  $[\pi]_f$  is surjective.

Suppose  $\Lambda_{f,n} \cong \mathcal{O}_K/(\pi^n)$  for some  $n$ . Since  $[\pi]_f$  is surjective, we have the following exact sequence:

$$0 \rightarrow \Lambda_{f,1} \rightarrow \Lambda_{f,n+1} \xrightarrow{[\pi]_f} \Lambda_{f,n} \rightarrow 0$$

Thus,  $\Lambda_{f,n+1}$  has  $q^{n+1}$  elements. Suppose  $\Lambda_{f,n+1} \cong \mathcal{O}_K/(\pi^{n_1}) \oplus \dots \oplus \mathcal{O}_K/(\pi^{n_r})$  by the structure theorem of modules over PID. Then the exact sequence implies that  $\Lambda_{f,1} \cong (\pi^{n_1-1})/(\pi^{n_1}) \oplus \dots \oplus (\pi^{n_r-1})/(\pi^{n_r})$ . Therefore,  $r = 1$  and  $\Lambda_{f,n+1} \subset \mathcal{O}_K/(\pi^{n+1})$ .  $\square$

**Lemma 2.18.** Every subfield  $E$  in  $K^{al}$  containing  $K$  is closed in the topological sense.

*Proof.* Let  $G = \text{Gal}(K^{al}/E)$ . By the uniqueness of the extension of the absolute valuation,  $G$  fixes the closure of  $E$ . Thus,  $\overline{E} = (K^{al})^G = E$ .  $\square$

**Theorem 2.19.** *Let  $K_{\pi,n} = K(\Lambda_{f,n})$ . Then we have*

- (a)  $K_{\pi,n}$  is independent of the choice of  $f$ .
- (b) For each  $n$ ,  $K_{\pi,n}/K$  is a totally ramified extension of degree  $(q-1)q^{n-1}$ .
- (c) The action of  $\mathcal{O}_K$  on  $\Lambda_n$  induces an isomorphism

$$(\mathcal{O}_K/\mathfrak{m}^n)^* \rightarrow \text{Gal}(K_{\pi,n}/K)$$

Thus,  $K_{\pi,n}/K$  is an abelian extension.

- (d) For each  $n$ ,  $Nm(K_{\pi,n}^*) \ni \pi$ .

*Proof.* (a) Via the isomorphisms  $[1]_{g,f}: \Lambda_{f,n} \rightarrow \Lambda_{g,n}$ , we have that

$$\widehat{K(\Lambda_{g,n})} = K(\widehat{[1]_{g,f}(\Lambda_{f,n})}) \subset \widehat{K(\Lambda_{f,n})} = K(\widehat{[1]_{f,g}(\Lambda_{g,n})}) \subset \widehat{K(\Lambda_{g,n})}$$

Thus,  $\widehat{K(\Lambda_{g,n})} = \widehat{K(\Lambda_{f,n})}$ . By the above lemma,

$$K(\Lambda_{g,n}) = \widehat{K(\Lambda_{g,n})} \cap K^{al} = \widehat{K(\Lambda_{f,n})} \cap K^{al} = K(\Lambda_{f,n})$$

- (b)(c) Since  $K_{\pi,n}$  is independent on the choice of  $f$ , we may assume again that  $f = [\pi]_f = \pi X + \cdots + X^q$ .

Choose a nonzero root  $\pi_1$  of  $f$  and  $\pi_{s+1}$  of  $f(X) - \pi_s$  for each  $s = 1, 2, \dots, n-1$ . Then there is a sequence of field extensions:

$$K(\pi_n) \supset K(\pi_{n-1}) \supset \cdots \supset K(\pi_1) \supset K$$

Note that each extension is Eisenstein, so is totally ramified. The degree of  $K(\pi_1)/K$  is  $q-1$  and the degree of  $K(\pi_{s+1})/K(\pi_s)$  is  $q$  for each  $s$ . Therefore,  $K(\pi_n)/K$  is a totally ramified extension of degree  $q^{n-1}(q-1)$ . Since  $[\pi^n]_f(\pi_n) = 0$ ,  $K(\Lambda_{f,n}) \supset K(\pi_n)$ .

Note that  $K(\Lambda_{f,n})$  is the splitting field of  $[\pi^n]_f$  over  $K$ . Thus,  $\text{Gal}(K(\Lambda_{f,n})/K)$  can be identified as a subgroup of permutations on  $\Lambda_{f,n}$ . By passing to limit of the power series, we can prove that the action of  $\text{Gal}(K(\Lambda_{f,n})/K)$  on  $\Lambda_{f,n}$  is compatible with the  $A$ -module

structure on  $\Lambda_{f,n}$ . Thus,  $\text{Gal}(K(\Lambda_{f,n})/K) < \text{Aut}(\Lambda_{f,n}) = (\mathcal{O}_K/(\pi^n))^*$ . Therefore,

$$(q-1)q^{n-1} = |(\mathcal{O}_K/(\pi^n))^*| \geq [K(\Lambda_{f,n})/K] \geq [K(\pi_n)/K] = (q-1)q^{n-1}$$

Hence,  $K(\Lambda_{f,n}) = K(\pi_n)$  is a totally ramified extension of degree  $(q-1)q^{n-1}$  over  $K$  and  $\text{Gal}(K_{\pi,n}/K) \cong (\mathcal{O}_K/\mathfrak{m}^n)^*$  and  $u \in \mathcal{O}_K^*$  acts on  $\Lambda_{f,n}$  by  $[u]_f$ .

- (d) Since the degree of  $[\pi^n]_f/X = \pi + \dots + X^{(q-1)q^{n-1}}$  is  $(q-1)q^n$ , it is the minimal polynomial of  $\pi_n$  over  $K$ . Hence,  $\text{Nm}_{K_{\pi,n}/K}(\pi_n) = (-1)^{(q-1)q^{n-1}}\pi$ , so  $\pi \in \text{Nm}(K_{\pi,n}^*)$ .  $\square$

Let  $K_\pi = \bigcup_{n=1}^\infty K_{\pi,n}$ . By passing to the limit, we have that  $\tilde{\phi}_f: U_K \cong \text{Gal}(K_\pi/K)$  given by  $u \mapsto [u^{-1}]_f$ . The inverse here will make the formula elegant in the future.

Let  $\phi_f: K^* \rightarrow \text{Gal}(K_\pi K^{un}/K)$  given as follows: for each  $a = u\pi^m \in K^*$ ,  $\phi_f(a)|_{K^{un}}$  is the  $m$ -th power of the Frobenius element and  $\phi_f(a)(\lambda) = \tilde{\phi}_f(u)(\lambda) = [u^{-1}]_f(\lambda)$  for all  $\lambda \in \bigcup_{n=1}^\infty \Lambda_{f,n}$ .

Next, we want to show that  $K_\pi K^{un}$  and  $\phi_f$  are independent of the choice of  $\pi, f$ . Note that in the proof of the part (a) of Theorem 2.19, the essential part is the  $\mathcal{O}_K$ -isomorphisms  $[1]_{g,f}: \Lambda_{f,n} \rightarrow \Lambda_{g,n}$ , where  $[1]_{g,f}$  is a power series with coefficients in  $\mathcal{O}_K$ . Now suppose  $\pi, \omega$  are two uniformizers of  $\mathcal{O}_K$  and  $\omega = u\pi$  for some  $u \in U_K$ . Let  $B, \hat{B}$  be the integer ring of  $K^{un}, \hat{K}^{un}$  respectively. Suppose we have such  $\mathcal{O}_K$ -isomorphisms  $\theta: \Lambda_{f,n} \rightarrow \Lambda_{g,n}$ , where  $f \in \mathcal{F}_\pi, g \in \mathcal{F}_\omega$  and  $\theta$  is a power series with coefficients in  $\hat{B}$  (Since we took completion in the proof of the part (a) of Theorem 2.19, the coefficients of  $\theta$  can be taken in  $\hat{B}$  and the proof of part (a) of Theorem 2.19 still work). We need to explore properties  $\theta$  need for proving that  $\phi_f$  is independent of  $\pi, f$ .

In order to show that  $\phi_f = \phi_g$ , it suffices to show that they agree on every uniformizer of  $\mathcal{O}_K$ . Given any uniformizer  $\pi'$  of  $\mathcal{O}_K$ ,  $\phi_f(\pi')|_{K^{un}} = \phi_g(\pi')|_{K^{un}}$  is the Frobenius element. Suppose  $\pi' = v\pi = vu^{-1}\omega$ . Let  $\theta^\sigma$  be the power series obtained by acting  $\sigma$  on each coefficient of  $\theta$ . Then for each  $\lambda \in \Lambda_{f,n}$ ,

$$\phi_f(\pi')(\theta(\lambda)) = \theta^\sigma(\phi_f(v)(\lambda)) = \theta^\sigma \circ [v^{-1}]_f(\lambda)$$

We want that the right-hand side is equal to  $\phi_g(\pi')(\theta(\lambda)) = [uv^{-1}]_g \circ \theta(\lambda) = \theta \circ [uv^{-1}]_f(\lambda)$  since  $\theta$  is a  $\mathcal{O}_K$ -homomorphism. Therefore, we need that  $\theta^\sigma = \theta \circ [u]_f$ . Note that  $\theta^\sigma = \theta \circ [u]_f$

implies that  $\theta$  induces isomorphisms  $\Lambda_{f,n} \rightarrow \Lambda_{g,n}$  because  $(\sigma \circ f)^\sigma = \theta \circ [u\pi]_f = [\omega]_g \circ \theta = g \circ \theta$ .

Suppose  $\theta(X) = \epsilon X + \dots$  for some  $\epsilon \in \hat{B}$ . Then  $\sigma(\epsilon) = \epsilon u$ . We claim that  $\sigma(\cdot)/\cdot: \hat{B} \rightarrow \hat{B}$  is surjective while it is not true that  $\sigma(\cdot)/\cdot: B \rightarrow B$  is surjective. That is why we require the coefficients of  $\theta$  to be in  $\hat{B}$ .

**Lemma 2.20.** *The homomorphism  $\sigma(\cdot)/\cdot: \hat{B}^* \rightarrow \hat{B}^*$  is surjective with kernel  $\mathcal{O}_K^*$ .*

*Proof.* Let  $\mathfrak{n}$  be the maximal ideal in  $B$ . It suffices to show that the sequence

$$1 \rightarrow (\mathcal{O}_K/\mathfrak{m}^n)^* \rightarrow (B/\mathfrak{n}^n)^* \xrightarrow{\sigma(\cdot)/\cdot} (B/\mathfrak{n}^n)^* \rightarrow 1$$

is exact for each  $n$  and then pass to the limit.

For  $n = 1$ ,  $B/\mathfrak{n} = \bar{k}$  and the result follows easily. Assume that the sequence is exact for  $n - 1$ . Then we have the following diagram:

$$\begin{array}{ccccccc} & & 1 & & 1 & & \\ & & \downarrow & & \downarrow & & \\ & & (\mathcal{O}_K/\mathfrak{m})^* & & (\mathcal{O}_K/\mathfrak{m}^{n-1})^* & & \\ & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & (B/\mathfrak{n})^* & \longrightarrow & (B/\mathfrak{n}^n)^* & \longrightarrow & (B/\mathfrak{n}^{n-1})^* \longrightarrow 1 \\ & & \downarrow \sigma(\cdot)/\cdot & & \downarrow \sigma(\cdot)/\cdot & & \downarrow \sigma(\cdot)/\cdot \\ 1 & \longrightarrow & (B/\mathfrak{n})^* & \longrightarrow & (B/\mathfrak{n}^n)^* & \longrightarrow & (B/\mathfrak{n}^{n-1})^* \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \\ & & 1 & & 1 & & \end{array}$$

By the snake lemma,  $\sigma(\cdot)/\cdot: (B/\mathfrak{n}^n)^* \rightarrow (B/\mathfrak{n}^n)^*$  is surjective with kernel of  $q^n$  elements. Since  $(\mathcal{O}_K/\mathfrak{m}^n)^*$  contains  $q^n$  elements and is contained in the kernel, the kernel is  $(\mathcal{O}_K/\mathfrak{m}^n)^*$ .  $\square$

The following proposition says that there exists the required  $\theta \in \hat{B}[[X]]$ , so it finishes the proof that  $K_\pi K^{un}$  and  $\phi_f$  are independent on the choice of  $\pi, f$ .

**Proposition 2.21.** *Let  $F_f$  and  $F_g$  be the Lubin-Tate formal group law defined by  $f \in \mathcal{F}_\pi$  and  $g \in \mathcal{F}_\omega$ , where  $\omega = u\pi$  are two uniformizers of  $\mathcal{O}_K$ . Then there exists an  $\epsilon \in \hat{B}^*$  such that  $\sigma(\epsilon) = \epsilon u$  and a power series  $\theta \in \hat{B}[[X]]$  such that*

(a)  $\theta(X) \equiv \epsilon X \pmod{X^2}$ .

(b)  $\theta^\sigma = \theta \circ [u]_f$ .

$$(c) \theta(F_f(X, Y)) = F_g(\theta(X), \theta(Y)).$$

$$(d) \theta \circ [a]_f = [a]_g \circ \theta.$$

*Proof.* The proof has four steps:

1. Show that there exists a  $\theta \in \hat{B}[[X]]$  satisfying (a)(b). This can be shown by induction on the degree of  $\theta$  as Lemma 2.10.
2. Show that the  $\theta$  in the first step can be chosen so that  $g = \sigma \circ f \circ \theta^{-1}$ . Let  $h = \theta^\sigma \circ f \circ \theta^{-1}$ . Then show that  $h \in \mathcal{O}_K[[X]]$ . Let  $\theta' = [1]_{g,h} \circ \theta$ . Then  $\theta'$  satisfies (a)(b) and  $(\theta')^\sigma \circ f \circ (\theta')^{-1} = [1]_{g,h} \circ h \circ [1]_{h,g} = g$ .
3. Show that  $\theta \left( F_f(\theta^{-1}(X), \theta^{-1}(Y)) \right) = F_g(X, Y)$ .
4. Show that  $\theta \circ [a]_f \circ \theta^{-1} = [a]_g$ .

Both the third and the fourth steps can be shown by directly Lemma 2.10. For details, see [7] Proposition 3.10. □

## 2.4 Local Kronecker-Weber Theorem

The main propose of this section is to prove the following theorem:

**Theorem 2.22.** (*Local Kronecker-Weber Theorem*)  $K_\pi K^{un} = K^{ab}$ .

**Lemma 2.23.** *Let  $L$  be a finite abelian extension of  $K_\pi$  of degree  $m$ . Let  $K_m$  be the unramified extension of  $K_\pi$  of degree  $m$ . Then there exists a totally ramified extension  $L_t/K_\pi$  such that  $L \subset L_t K_m = LK_m$ .*

*Proof.* Note that  $\text{Gal}(LK_m/K_\pi)$  is a subgroup of  $\text{Gal}(L/K_\pi) \times \text{Gal}(K_m/K_\pi)$ , so every element in  $\text{Gal}(LK_m/K_\pi)$  has torsion  $m$ . Pick a  $\tau \in \text{Gal}(LK_m/K_\pi)$  such that  $\tau|_{K_m}$  is the Frobenius element. Then  $\tau$  has order  $m$  in  $\text{Gal}(LK_m/K_\pi)$ . By the structure theorem of finite abelian groups, we have that  $\text{Gal}(LK_m/K_\pi)$  can be decomposed into  $\langle \tau \rangle \times H$  for some subgroup  $H < \text{Gal}(LK_m/K_\pi)$ . Let  $L_t = L^{\langle \tau \rangle}$ . Then  $L_t \cap K_m = K_\pi$  since  $\text{Gal}(K_m/K_\pi) = \langle \tau|_{K_m} \rangle$ , so  $L_t/K_\pi$  is totally ramified and  $\text{Gal}(L_t/K_\pi) = H$ . Therefore,  $L_t K_m = LK_m \supset L$ . □

**Remark.** *The above proof actually works for all henselian valuation field with finite residue field  $K$  and finite abelian extension  $L/K$ .*

**Lemma 2.24.** *Let  $L$  be a totally ramified extension of  $K$  and  $L \supset K_\pi$ . Then  $L = K_\pi$ .*

*Proof.* See [7] Lemma 4.9.

The idea is that  $\text{Gal}(L/K_\pi) = \bigcap_{n=1}^{\infty} \text{Gal}(L/K_{\pi,n})$ . In fact,  $\text{Gal}(L/K_{\pi,n})$  is some ramification group of  $\text{Gal}(L/K)$ , so their intersection is trivial.  $\square$

**Lemma 2.25.** *Every finite unramified extension of  $K_\pi$  is contained in  $K_\pi K^{un}$*

*Proof.* Suppose  $L/K_\pi$  is a finite unramified extension. Then  $L = K_\pi(\alpha)$  for some  $\alpha \in K^{al}$ . Suppose  $f \in K_\pi[X]$  is the minimal polynomial of  $\alpha$  over  $K_\pi$ . Then  $f \in K_{\pi,n}[X]$  for some  $n$ . Since  $L/K_\pi$  is unramified,  $f$  is irreducible in the residue field of  $K_\pi$ , which is the same with the residue field of  $K_{\pi,n}$ . Thus,  $K_{\pi,n}(\alpha)/K_{\pi,n}$  is unramified. Suppose  $T/K$  is the maximal unramified extension of  $K_{\pi,n}(\alpha)/K$ , so the residue field of  $T$  equals the residue field of  $K_{\pi,n}(\alpha)$ . Then  $[T : K]$  equals the inertia index of  $K_{\pi,n}(\alpha)/K$ . Thus,  $K_{\pi,n}(\alpha) = TK_{\pi,n}$ . Hence,  $L = K_\pi T \subset K_\pi K^{un}$ .  $\square$

*Proof.* (of Theorem 2.22): Suppose  $L/K$  is a finite abelian extension. Then  $LK_\pi/K_\pi$  is also a finite abelian extension. Thus, there exists a totally ramified extension  $L_t/K_\pi$  and an unramified extension  $K_m/K_\pi$  such that  $LK_\pi \subset L_t K_m$ . By the two lemmas above,  $L_t = K_\pi$  and  $K_m \subset K_\pi K^{un}$ . Therefore,  $L \subset LK_\pi \subset K_\pi K^{un}$ . Hence,  $K_\pi K^{un} = K^{ab}$ .  $\square$

## 2.5 End of the Proof

Now we finish the proof of the main theorems of local class field theory by showing that the  $\phi_K$  we constructed satisfies the Theorem 2.1 and that Theorem 2.3 is true.

By construction, we know that  $\phi_K(\pi)|_{K^{un}}$  is the Frobenius element for each uniformizer  $\pi$  of  $K$ .

To prove the part (b) of the Theorem 2.1, take a finite abelian extension  $L/K$ .

**Lemma 2.26.** *The following diagram is commutative*

$$\begin{array}{ccc} L^* & \xrightarrow{\phi_L} & \text{Gal}(K^{ab}/L) \\ Nm \downarrow & & \downarrow \\ K^* & \xrightarrow{\phi_K} & \text{Gal}(K^{ab}/K) \end{array}$$

*Proof.* Since  $L^*$  is generated by all uniformizers, it suffices to show that  $\phi_L(\Pi) = \phi_K(\text{Nm}(\Pi))$  for all uniformizers  $\Pi$  of  $L$ . By taking the maximal unramified extension of  $K$  in  $L$ , it suffices to show the cases when  $L/K$  is totally ramified and unramified respectively.

For detail, see [6] Theorem 6.9. □

Thus,  $\phi_K$  induces a homomorphism  $\phi_{L/K}: K^*/\text{Nm}(L^*) \rightarrow \text{Gal}(L/K)$ .

From the construction of  $\phi_K$ , it is easy to see that

**Lemma 2.27.** *The homomorphism  $\phi_K$  is injective and continuous. Moreover,  $\phi_K(K^*)$  is dense in  $\text{Gal}(K^{ab}/K)$ , consisting of all elements  $\tau$  such that  $\tau|_{K^{un}}$  is a power of the Frobenius element.*

The following proposition finishes the proof of the part (b) of Theorem 2.1.

**Proposition 2.28.** *As notations above,  $\phi_{L/K}: K^*/\text{Nm}(L^*) \rightarrow \text{Gal}(L/K)$  is an isomorphism.*

*Proof.* If  $\phi_K(x)|_L = \text{Id}$  for some  $x \in K^*$ , then there is  $\tau = \phi_K(x)|_L \in \text{Gal}(K^{ab}/L)$ . Let  $T = L \cap K^{un}$ . Suppose  $[T : K] = m$ . Then  $\phi_K(x)|_T = \text{Id}$  implies that  $\phi_K(x)|_{K^{un}}$  is a power of  $\sigma^m$  by the above lemma. Note that  $\text{Gal}(K^{un}/T) \cong \text{Gal}(LK^{un}/L) = \text{Gal}(L^{un}/L)$  and  $\sigma^m$  corresponds to the Frobenius element of  $L$  under this isomorphism. Therefore,  $\phi_K(x)|_L^{un}$  is a power of the Frobenius element of  $L$ . By the above lemma again, there is  $y \in L$  such that  $\phi_L(y) = \phi_K(x)$ . Since  $\phi_L(y) = \phi_K(\text{Nm}(y))$  and  $\phi_K$  is injective,  $x = \text{Nm}(y)$ . Thus,  $\phi_{L/K}$  is injective.

In order to prove the surjectivity, identify  $\text{Gal}(L/K)$  as  $\text{Gal}(K^{ab}/K)/\text{Gal}(K^{ab}/L)$ . For each  $[\tau] \in \text{Gal}(L/K)$ ,  $\tau\text{Gal}(K^{ab}/L)$  is an open subset of  $\text{Gal}(K^{ab}/K)$ . Since  $\phi_K(K^*)$  is dense in  $\text{Gal}(K^{ab}/K)$ , there is  $x \in K^*$  such that  $\phi_K(x) \in \tau\text{Gal}(K^{ab}/L)$ . Therefore,  $\phi_{L/K}(x) = [\tau]$ . □

Finally, we should prove Theorem 2.3.

**Lemma 2.29.** *Let  $K$  be a non-archimedean local field and  $L/K$  is a field extension. If  $\text{Nm}(L^*)$  is of finite index in  $K^*$ , then it is open.*

*Proof.* Since  $U_L$  is profinite,  $U_L$  is compact. Thus,  $\text{Nm}(U_L)$  is compact in  $K^*$ , which is Hausdorff. Therefore,  $\text{Nm}(U_L)$  is closed in  $K^*$ . Since  $\text{Nm}(U_L) = \text{Nm}(L^*) \cap U_K$ ,  $U_L$  is a closed subgroup with finite index in  $U_K$ , so is open in  $U_K$ . Note that  $U_K$  is open in  $K^*$ . Hence,  $\text{Nm}(L^*)$  contains an open subgroup of  $K^*$ , so is open. □

*Proof.* (of Theorem 2.3): By the part (b) of Theorem 2.1, we see that every norm group in  $K^*$  is of finite index. Thus, by the lemma above, they are open. Conversely, by the part (d) of the Corollary 2.2, it suffices to show that each open subgroup of finite index  $H$  in  $K^*$  contains a norm group. Since  $H$  is open,  $H \supset (1 + \mathfrak{m}^n)$  for some  $n$ . Since  $H$  is of finite index, there is

an integer  $s$  such that  $H \supset (1 + \mathfrak{m}^n) \times s\mathbb{Z}$  by the same proof as in Lemma 2.4. Let  $K_s$  be the unramified extension of  $K$  of degree  $s$  and  $L = K_{\pi,n}K_s$ . Therefore,  $\phi_{L/K}((1 + \mathfrak{m}^n) \times s\mathbb{Z}) = 1$ . It follows that  $(1 + \mathfrak{m}^n) \times s\mathbb{Z} \subset \text{Nm}(L^*)$ . Since they have the same index in  $K^*$ ,  $(1 + \mathfrak{m}^n) \times s\mathbb{Z} = \text{Nm}(L^*)$ .  $\square$

### 3 Proof of Ando's Criterion via Coleman Norm Operator

In this section, we suppose that  $\pi = p$ . Suppose  $\Phi$  is a Honda formal group law over  $k = F_q$ , i.e.  $[p]_\Phi = T^q$ , where  $[p]_\Phi$  is the  $p$ -th composition of  $\Phi$  with itself. Then every lifting  $F$  of  $\Phi$  to  $\mathcal{O}_K$  is a Lubin-Tate formal group law. Let  $f \in \mathcal{F}_\pi$  be the element associated to  $F$ . Then  $f = [p]_f = [p]_F$ .

By [1, Theorem 4],

**Definition 3.1** (Ando's criterion). We say a formal group law  $F$  over  $\mathcal{O}_K$  that is a lifting of a Honda formal group law over  $k$  satisfies Ando's criterion if

$$[p]_F(T) = \prod_{\lambda \in \Lambda_1} (T +_F \lambda)$$

Suppose  $\mathcal{O}_K((T))$  is the ring of Laurent series with coefficients in  $\mathcal{O}_K$ . We assign the “compact-open” topology to  $\mathcal{O}_K((T))$ , i.e. a sequence  $\{g_n\}$  converges to  $g$  if and only if for any closed annulus  $A$  around zero in  $\mathfrak{m}$ , and for each  $\epsilon > 0$ , there exists a positive integer  $N = N(A, \epsilon)$  such that  $|g_n(a) - g(a)| < \epsilon$  for all  $a \in A$  and  $n \geq N$ . Then the Coleman Norm Operator is given by:

**Theorem 3.2.** *There exists a unique  $\mathcal{N}_f: \mathcal{O}_K((T)) \rightarrow \mathcal{O}_K((T))$  satisfying*

$$\mathcal{N}_f(g) \circ [\pi]_f = \prod_{\lambda \in \Lambda_1} g(T +_F \lambda)$$

*for every  $g \in \mathcal{O}_K((T))$ . Moreover,  $\mathcal{N}_f$  is continuous and multiplicative.*

*Proof.* See [2, Theorem 11, Corollary 12].  $\square$

Therefore, we see that a Lubin-Tate formal group law satisfies Ando's criterion if and only if

$$[p]_F(T) = \mathcal{N}_f(T) \circ [p]_F$$



Since  $[p]_F$  has a composition inverse in  $K[[T]]$ , we can cancel the  $[p]_F$  on both sides, so that Ando's criterion is equivalent to

$$\mathcal{N}_f(T) = T$$

Let  $\mathcal{M}_\infty = \{g \in \mathcal{O}_K((T)) : \mathcal{N}_f(g) = g\}$  and  $\varprojlim \Lambda_{f,n}$  be the inverse limit taken with respect to  $[\pi]_f$ . Suppose  $v_f = (v_{f,n}) \in \varprojlim \Lambda_{f,n}$  is a generator, i.e.  $v_{f,n}$  is a generator of  $\Lambda_{f,n}$  as a  $\mathcal{O}_K$ -module for each  $n$ . Let  $X_\infty = \varprojlim K_n^*$ , where the inverse limit is taken with respect to norm maps  $N_{n+1,n} : K_{n+1}^* \rightarrow K_n^*$ . According to [2, Corollary 17],  $T \in \mathcal{M}_\infty$  if and only if  $v \in X_\infty$ , i.e.

$$N_{n+1,n}(v_{f,n+1}) = v_{f,n}$$

for each  $n$ .

**Proposition 3.3.** *If  $[p]_f = \sum_{i=0}^q a_i T^i$  where  $a_0 = \pi, a_q = 1$ , then  $F$  satisfies Ando's criterion.*

*Proof.* By the above discussion, it suffices to show that  $N_{n+1,n}(v_{f,n+1}) = v_{f,n}$  for each  $n$ . Since  $v_{f,n} = [p]_f(v_{f,n+1})$  and  $[p]_f$  is an Eisenstein polynomial,  $[p]_f(T) - v_{f,n}$  is the minimal polynomial of  $v_{f,n+1}$  over  $K_n$ . Hence,  $N_{n+1,n}(v_{f,n+1}) = (-1)^q(-v_{f,n}) = v_{f,n}$ .  $\square$

We say two liftings  $F, \tilde{F}$  of  $\Phi$  are  $\star$ -isomorphic if the isomorphism  $\psi \in T\mathcal{O}_K[[T]]$  between  $F, \tilde{F}$  satisfies  $\psi \equiv T \pmod{\pi}$ .

We have the following description for Ando's criterion ([1, Theorem 4]):

**Theorem 3.4 (Ando).** *In each  $\star$ -isomorphism class of lifting of  $\Phi$  to a complete local ring with residue field  $k$ , there is a unique formal group law  $F$  satisfying Ando's criterion.*

The goal of this section is to prove Theorem 3.4 via Coleman Norm Operator.

First we need some notations. Some of them follow the notations in [2].

$$\begin{aligned} I &:= \mathcal{O}_K[[T]] \\ I^0 &:= 1 + \pi I \\ J &:= TI = T\mathcal{O}_K[[T]] \\ J^0 &:= TI^0 = T + \pi TI \end{aligned}$$

**Proposition 3.5.** *Suppose  $g, h \in \mathcal{F}_\pi$ . Then  $F_g, F_h$  are  $\star$ -isomorphic if and only if there is  $u \in J^0$  such that  $h = u \circ g \circ u^{-1}$ .*

*Proof.* If  $F_g, F_h$  are  $\star$ -isomorphic with isomorphism  $u$ . Then  $u \in J^0$  and  $u \circ g = h \circ u$ .

Conversely, if there is a  $u \in J^0$  such that  $u \circ g = h \circ u$ ,  $u = [u'(0)]_{h,g}$  by Proposition 2.12.

Thus,  $u \in \text{Hom}(F_g, F_h)$  is an isomorphism and  $u \equiv t \pmod{\pi}$ .  $\square$

Fix  $f \in \mathcal{F}_\pi$  and  $u \in J^0$ . Let  $f_u := u \circ f \circ u^{-1}$ . By above discussion,  $F_{f_u}$  satisfies the Ando's criterion if and only if  $N_{n+1,n}(v_{f_u,n+1}) = v_{f_u,n}$  for all  $n$ . Note that  $u$  induces isomorphisms between  $\Lambda_{f,n} \rightarrow \Lambda_{f_u,n}$  for all  $n$ . Let  $v_{f,n} = u^{-1}(v_{f_u,n})$ . Since  $f_u(v_{f_u,n+1}) = v_{f_u,n}$  for each  $n$ ,  $f(v_{f,n+1}) = v_{f,n}$  for each  $n$ . Thus,  $v_f = (v_{f,n}) \in \varprojlim \Lambda_{f,n}$  is a generator. Then by [2, Corollary 12(ii)],

$$N_{n+1,n}(v_{f_u,n+1}) = v_{f_u,n} \Leftrightarrow u(v_{f,n}) = N_{n+1,n}(u(v_{f,n+1})) = \mathcal{N}_f(u)(v_{f,n})$$

For any  $\lambda \in \Lambda_{f,n} - \Lambda_{f,n-1}$ ,  $\lambda = \tau(v_{f,n})$  for some  $\tau \in \text{Gal}(K_{\pi,n}/K)$ . Since  $u, \mathcal{N}_f(u) \in \mathcal{O}_K[[T]]$ ,

$$u(\lambda) = \tau(u(v_{f,n})) = \tau(\mathcal{N}_f(u)(v_{f,n})) = \mathcal{N}_f(\lambda)$$

Thus,  $\mathcal{N}_f(u), u$  agree on  $v_{f,n}$  for all  $n$  if and only if they agree on  $\Lambda_{f,n} - \{0\}$  for all  $n$ . By [2, Uniqueness Principle], the latter condition is equivalent to say that  $\mathcal{N}_f(u) = u$ . Thus, we are left to prove

**Proposition 3.6.** *For an  $f \in \mathcal{F}_\pi$ , there is a unique  $u \in J^0$ , such that  $\mathcal{N}_f(u) = u$ .*

We first need the following lemma from [2].

**Lemma 3.7.** *Let  $i \geq 1$ ,  $g \in 1 + \pi^i I$  and  $h \in I$ . Then*

$$(a) \quad \mathcal{N}_f(g) \in 1 + \pi^{i+1} I.$$

$$(b) \quad \mathcal{N}_f^i(h) / \mathcal{N}_f^{i-1}(h) \in 1 + \pi^i I.$$

*Proof.* See [2, Lemma 13].  $\square$

Then we see that  $\mathcal{N}_f^\infty(h) := \lim_{i \rightarrow \infty} \mathcal{N}_f^i(h)$  exists. By Lemma 3.7(a),  $\mathcal{N}_f^\infty$  vanishes on  $I^0$ . Since  $\mathcal{N}_f$  is continuous,

$$\mathcal{N}_f(\mathcal{N}_f^\infty(h)) = \mathcal{N}_f(\lim_{i \rightarrow \infty} \mathcal{N}_f^i(h)) = \lim_{i \rightarrow \infty} \mathcal{N}_f(\mathcal{N}_f^i(h)) = \mathcal{N}_f^\infty(h)$$

Moreover,  $\mathcal{N}_f^\infty$  is multiplicative since  $\mathcal{N}_f$  is.

*Proof of Proposition 3.6.* If  $\mathcal{N}_f(u) = u$ , then  $\mathcal{N}_f^i(u) = u$  for each  $i$ . Thus,  $\mathcal{N}_f^\infty(u) = u$  after taking the limit. Since  $u \in J^0$ , there is  $\tilde{u} \in I^0$  such that  $u = t\tilde{u}$ . Then

$$u = \mathcal{N}_f^\infty(u) = \mathcal{N}_f^\infty(t)\mathcal{N}_f^\infty(\tilde{u}) = \mathcal{N}_f^\infty(t)$$

It suffices to show that  $\mathcal{N}_f^\infty(t) \in J^0$ . Suppose  $g_i := \mathcal{N}_f^i(t)/\mathcal{N}_f^{i-1}(t) \in 1 + \pi^i I$ . Then  $\mathcal{N}_f^\infty(t) = tg_1g_2\cdots$ . Calculating each coefficient we see that  $\mathcal{N}_f^\infty(t) \in J^0$ .  $\square$

## References

- [1] Matthew Ando. Isogenies of formal group laws and power operations in the cohomology theories en. *Duke mathematical journal*, 79(2), 1995. 3, 3
- [2] Robert F. Coleman. Division values in local fields. *Inventiones mathematicae*, 53(2):91–116, 1979. 3.2, 3, 3, 3, 3, 3.7
- [3] Keith Conrad. History of class field theory. <https://kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf>. 1, 1
- [4] Günther Frei, Franz Lemmermeyer, and Peter J Roquette. *Emil Artin and Helmut Hasse: The Correspondence 1923-1958*, volume 5 of *Contributions in mathematical and computational sciences*. Springer Basel AG, Basel, 2014. 1
- [5] Yong Hu. Topics in algebra and number theory. SUSTech lecture notes, Not Published, 2021. 1.1, 2.1
- [6] Kenkichi Iwasawa. *Local class field theory*. Oxford Science Publications, 1986. 2.26
- [7] James Milne. Class field theory. <https://www.jmilne.org/math/CourseNotes/CFT.pdf>, 2020. 2.2, 2.10, 2.21, 2.24