

# LOCAL CLASS FIELD THEORY VIA LUBIN-TATE THEORY

TERUYOSHI YOSHIDA

ABSTRACT. We give a self-contained proof of local class field theory, via Lubin-Tate theory and the Hasse-Arf theorem, refining the arguments of Iwasawa [4].

## 1. INTRODUCTION

We prove local class field theory via Lubin-Tate theory and the Hasse-Arf theorem. The only prerequisites are Galois theory (including cyclotomic extensions, finite fields and infinite extensions) and some basic commutative algebra summarized in §7. Our argument is close to Iwasawa [4], but the main innovation here is to use the relative Lubin-Tate groups of de Shalit [2] to prove the base change property (Theorem 5.9) directly, without proving the local Kronecker-Weber theorem first. The author thanks his fellow students at Harvard University, especially Jay Pottharst, who read the draft and gave valuable comments.

**Theorem A (Local Class Field Theory).** (i) *For any local field  $K$ , there is a unique homomorphism  $\text{Art}_K : K^\times \longrightarrow \text{Gal}(K^{\text{ab}}/K)$ , characterized by the two properties:*

- (a) *If  $\pi$  is a uniformizer of  $K$ , then  $\text{Art}_K(\pi)|_{K^{\text{ur}}} = \text{Frob}_K$ .*
- (b) *If  $K'/K$  is a finite abelian extension, then  $\text{Art}_K(N_{K'/K}(K'^{\times}))|_{K'} = \text{id}$ .*

*Moreover,  $\text{Art}_K$  is an isomorphism onto  $W_K^{\text{ab}} := \{\sigma \mid \sigma|_{K^{\text{ur}}} \in \text{Frob}_K^{\mathbb{Z}}\} \subset \text{Gal}(K^{\text{ab}}/K)$ .*

(ii) *If  $K'/K$  is a finite extension, then  $\text{Art}_{K'}(x)|_{K^{\text{ab}}} = \text{Art}_K(N_{K'/K}(x))$  for all  $x \in K'^{\times}$ , and  $\text{Art}_K$  induces an isomorphism  $K^\times/N_{K'/K}(K'^{\times}) \xrightarrow{\cong} \text{Gal}((K' \cap K^{\text{ab}})/K)$ .*

**Notation.** The cardinality of a finite set  $X$  is denoted by  $|X|$ . A *ring* means a commutative ring with a unit, unless stated otherwise. For a ring  $A$ , we write  $A^\times$  for its group of units. For a field  $F$ , we usually (implicitly) fix its algebraic closure  $\overline{F}$  and regard any algebraic extension of  $F$  as a subfield of  $\overline{F}$ . For a finite extension  $F'/F$ , we denote the norm map by  $N_{F'/F} : F'^{\times} \rightarrow F^\times$ . We denote the maximal abelian extension of  $F$  in  $\overline{F}$  by  $F^{\text{ab}}$ . For a positive integer  $n$  not divisible by  $\text{char } F$ , the splitting field of  $X^n - 1$  over  $F$  is denoted by  $F(\boldsymbol{\mu}_n)$  (*cyclotomic extension*), which is an abelian extension such that its Galois group naturally injects into  $(\mathbb{Z}/(n))^\times$ . We denote the set of roots of  $X^n - 1$  by  $\boldsymbol{\mu}_n$ . For  $x \in F^\times$ , we write  $\langle x \rangle$  for the subgroup  $x^{\mathbb{Z}} := \{x^a \mid a \in \mathbb{Z}\}$  of  $F^\times$  generated by  $x$ .

---

*Date:* June 5, 2006.

This work was partially supported by the EPSRC grant on Zeta Functions from the University of Nottingham.

## 2. LOCAL FIELDS AND FORMAL GROUP LAWS

We denote the finite field consisting of  $q$  elements by  $\mathbb{F}_q$ . For each  $n \geq 1$ , we have  $\mathbb{F}_{q^n} = \mathbb{F}_q(\boldsymbol{\mu}_{q^n-1})$ . The Galois group  $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$  is isomorphic to  $\widehat{\mathbb{Z}} := \varprojlim^n \mathbb{Z}/(n)$ , the *profinite completion* of  $\mathbb{Z}$ , by sending the  $q$ -th power *Frobenius map*  $x \mapsto x^q$  to 1.

**2.1. Local fields (see §7).** Let  $p$  be a prime, fixed throughout the article. The *ring of  $p$ -adic integers* is defined as  $\mathbb{Z}_p := \varprojlim^m \mathbb{Z}/(p^m)$ . This is a CDVR (complete discrete valuation ring) with  $(p)$  as its maximal ideal. The fraction field  $\mathbb{Q}_p$  of  $\mathbb{Z}_p$  is the  *$p$ -adic field*. In this article, *local field* means a finite extension of  $\mathbb{Q}_p$ . For a local field  $K$ , the integral closure of  $\mathbb{Z}_p$  in  $K$  is denoted by  $\mathcal{O}_K$ , which is called the *ring of integers* of  $K$ . This is again a CDVR (Proposition 7.1(i)), and its maximal ideal is denoted by  $\mathfrak{p} := \mathfrak{p}_K$ . The field  $k := \mathcal{O}_K/\mathfrak{p}$  is called the *residue field* of  $K$ . As  $k$  is a finite extension of the residue field  $\mathbb{F}_p$  of  $\mathbb{Q}_p$ , it is equal to  $\mathbb{F}_q$  for a certain power  $q$  of  $p$ . A generator of  $\mathfrak{p}$  is called a *uniformizer* of  $K$ . We denote its *valuation* by  $v_K : K^\times \rightarrow \mathbb{Z}$ .

Let  $K'/K$  be a finite extension of local fields. Then  $\mathcal{O}_{K'}$  is the integral closure of  $\mathcal{O}_K$  in  $K'$ , and the residue field  $k'$  of  $K'$  is a finite extension of  $k$ . The *ramification index*  $e = e(K'/K)$  and the *residue degree*  $f = f(K'/K)$  of  $K'/K$  are defined by  $\mathfrak{p}\mathcal{O}_{K'} = \mathfrak{p}_{K'}^e$  and  $[k' : k] = f$ . Then the following hold:

$$[K' : K] = ef, \quad v_{K'}(x) = ev_K(x) \ (\forall x \in K), \quad v_K(N_{K'/K}(x)) = fv_{K'}(x) \ (\forall x \in K'^\times).$$

We say  $K'/K$  is *unramified* if  $e = 1$ , and *totally ramified* if  $f = 1$ . If  $K''/K'$  is another finite extension, we have  $e(K''/K) = e(K''/K')e(K'/K)$  and  $f(K''/K) = f(K''/K')f(K'/K)$ . Therefore, if  $K'/K$  is unramified and  $K''/K'$  is totally ramified, then  $K' \cap K''/K$  is unramified and totally ramified, hence  $K' \cap K'' = K$ .

Unramified extensions are classified using the following lemma (see §7 for its proof):

**Lemma 2.1.** (Hensel's lemma) *Let  $n \geq 1$  with  $(p, n) = 1$ . Then  $\boldsymbol{\mu}_n \subset k \iff \boldsymbol{\mu}_n \subset K$ .*

For  $f \geq 1$ , let  $K_f := K(\boldsymbol{\mu}_{q^f-1})$  and  $k_f$  be its residue field. Then  $K_f/K$  is unramified (Proposition 7.2), and  $\mathbb{F}_{q^f} \subset k_f$  by the above lemma. As  $\text{Gal}(K_f/K) \cong \text{Gal}(k_f/\mathbb{F}_q)$  shows that an element of  $\text{Gal}(k_f/\mathbb{F}_q)$  is determined by its action on  $\boldsymbol{\mu}_{q^f-1}$ , we have  $k_f = \mathbb{F}_{q^f}$  and  $[K_f : K] = f$ . Conversely, if  $K'/K$  is unramified of degree  $f$ , then the residue field of  $K'$  is  $\mathbb{F}_{q^f}$ , hence  $\boldsymbol{\mu}_{q^f-1} \subset K'$  by the above lemma, and we see  $K' = K_f$  by comparing the degrees. As  $K_f \subset K_{f'}$  for  $f \mid f'$ , the union  $K^{\text{ur}} := \bigcup_{f \geq 1} K_f$  is an infinite Galois extension of  $K$  (the *maximal unramified extension* of  $K$ ), and by the above isomorphism:

$$\text{Gal}(K^{\text{ur}}/K) \xrightarrow{\cong} \varprojlim_f \text{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q) \cong \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \xrightarrow{\cong} \widehat{\mathbb{Z}}.$$

As the element of  $\text{Gal}(K^{\text{ur}}/K)$  mapped to  $1 \in \widehat{\mathbb{Z}}$ , we can take the  $\varphi$  (*arithmetic Frobenius*), which is mapped to the Frobenius map of  $\overline{\mathbb{F}}_q$ , or its inverse  $\text{Frob}_K$  (*geometric Frobenius*). For any finite extension  $K'/K$ , we see that  $K'$  is totally ramified over  $K' \cap K^{\text{ur}}$ .

**2.2. Formal group laws.** Let  $A$  be a ring, not a zero ring. In the formal power series ring of one variable  $A[[X]] := \varprojlim_m A[X]/(X^m)$  over  $A$ , the ideal  $(X) \subset A[[X]]$ , consisting of all the elements with constant term equal to 0, is a monoid under the composition  $f \circ g := f(g(X))$  with  $X$  as the identity. For  $f \in (X)$ , there exists an  $f^{-1}$  satisfying  $f \circ f^{-1} = f^{-1} \circ f = X$  if and only if the coefficient of  $X$  in  $f$  belongs to  $A^\times$ . Also, we use similar notation for  $f \in (X) \subset A[[X]]$  and a power series of several variables  $F \in A[[X_1, \dots, X_n]]$ :

$$f \circ F := f(F(X_1, \dots, X_n)), \quad F \circ f := F(f(X_1), \dots, f(X_n)) \in A[[X_1, \dots, X_n]].$$

**Definition 2.2.** A *formal group law over  $A$*  is a formal power series of two variables  $F(X, Y) \in A[[X, Y]]$  which satisfies the following<sup>1</sup>:

- (i)  $F(X, Y) \equiv X + Y \pmod{\deg 2}$ .
- (ii)  $F(F(X, Y), Z) = F(X, F(Y, Z))$ .
- (iii)  $F(X, Y) = F(Y, X)$ .

The basic examples are the *additive group*  $\widehat{\mathbb{G}}_a(X, Y) := X + Y$  and the *multiplicative group*  $\widehat{\mathbb{G}}_m(X, Y) := X + Y + XY$ .

Let  $F$  be a formal group law over a ring  $A$ . If we let  $f(X) := F(X, 0)$ , we have  $f(X) \equiv X \pmod{\deg 2}$  by (i), hence  $f^{-1}$  exists. By (ii), we have  $f \circ f = f$ , hence we get  $f(X) = X$  by composing  $f^{-1}$ . Similarly we have  $F(0, Y) = Y$ , hence  $F$  does not have a term containing only  $X$  or  $Y$ , apart from the linear terms  $X + Y$ . Therefore we can solve  $F(X, Y) = 0$  with respect to  $Y$  and get a unique  $i_F(X) \in A[[X]]$  satisfying  $F(X, i_F(X)) = 0$ . If we define the addition  $+_F$  on the ideal  $(X) \subset A[[X]]$  by

$$f +_F g := F(f(X), g(X)),$$

then  $(X)$  becomes an abelian group with 0 as the identity and  $i_F \circ f$  as the inverse of  $f$ .

**Definition 2.3.** Let  $F, G$  be formal group laws over  $A$ . A power series  $f(X) \in (X) \subset A[[X]]$  is called a *homomorphism* from  $F$  to  $G$  if it satisfies

$$f \circ F = G \circ f, \quad \text{i.e. } f(F(X, Y)) = G(f(X), f(Y)),$$

and we write  $f : F \rightarrow G$ . Two homomorphisms compose via the composition of power series, with  $f(X) = X$  as the identity  $\text{id} : F \rightarrow F$ . If  $f^{-1}$  exists, it defines  $f^{-1} : G \rightarrow F$  and  $f \circ f^{-1} = f^{-1} \circ f = \text{id}$ . In this case  $f$  is called an *isomorphism* and we write  $f : F \xrightarrow{\cong} G$ .

The set  $\text{Hom}_A(F, G)$  of all homomorphisms from  $F$  to  $G$  is an abelian group under  $+_G$ . Moreover,  $\text{End}_A(F) := \text{Hom}_A(F, F)$  is a (not necessarily commutative) ring with  $+_F$  as the addition and  $\circ$  as the multiplication.

If  $A$  is a CDVR with the maximal ideal  $P$ , then for a formal group  $F$  over  $A$  and for all  $x, y \in P$ , we have  $x +_F y := F(x, y) \in P$  (see §7).

<sup>1</sup>Precisely speaking, this is called a *commutative formal group law of dimension 1*. It is called a ‘‘formal group’’ in [4], but this term usually stands for an isomorphism class of formal group laws (i.e. formal group scheme). We mostly deal with the group law itself (a power series) in this article.

## 3. LUBIN-TATE GROUPS AND LUBIN-TATE EXTENSIONS

We return to the notation of §2.1:  $K$  is a local field,  $\mathcal{O}_K$  is its ring of integers, whose maximal ideal is  $\mathfrak{p} = \mathfrak{p}_K$ , and the residue field has characteristic  $p = \text{char}(\mathcal{O}_K/\mathfrak{p})$  and order  $q = |\mathcal{O}_K/\mathfrak{p}|$ . We start from the following general remark. Let  $E/K$  be an algebraic extension (not necessarily finite). We denote the integral closure of  $\mathcal{O}_K$  in  $E$  by  $\mathcal{O}_E$ . If  $E = \bigcup_{K'} K'$  where  $K'/K$  are finite extensions, then  $\mathcal{O}_E = \bigcup_{K'} \mathcal{O}_{K'}$  and  $E = \mathcal{O}_E \otimes_{\mathcal{O}_K} K$ , in particular  $E = \text{Frac}(\mathcal{O}_E)$ . As all inclusion maps between  $\mathcal{O}_{K'}$  are local homomorphisms<sup>2</sup>,  $\mathcal{O}_E$  is a local ring with the maximal ideal  $\mathfrak{p}_E := \bigcup_{K'} \mathfrak{p}_{K'}$ . We call  $E/K$  *unramified* (resp. *totally ramified*) if it is a union of unramified (resp. totally ramified) finite extensions of  $K$ . If  $E/K$  is unramified, then  $\mathfrak{p}_{K'} = \mathfrak{p}_K \mathcal{O}_{K'}$  for all  $K'$ , hence  $\mathfrak{p}_E = \mathfrak{p}_K \mathcal{O}_E$  and  $\mathcal{O}_E$  is a DVR<sup>3</sup>.

Now let  $E/K$  be an unramified extension, and  $L$  be its completion (see §7), i.e.  $\mathcal{O}_L := \widehat{\mathcal{O}_E}$  and  $L := \text{Frac}(\mathcal{O}_L)$  (if  $E/K$  is finite, then  $E = L$ ). We call such  $L$  a *complete unramified extension* of  $K$ . Then  $\mathcal{O}_L$  is a CDVR with the maximal ideal  $\mathfrak{p}_L := \widehat{\mathfrak{p}_E}$ . Any uniformizer of  $K$  is also a uniformizer of  $E$ , hence of  $L$ , but not vice versa. Any automorphism of  $E/K$ , for example the arithmetic Frobenius  $\varphi = \text{Frob}_K^{-1} \in \text{Gal}(K^{\text{ur}}/K)$ , induces automorphisms of  $\mathcal{O}_E$  and  $\mathcal{O}_E/\mathfrak{p}_E^m$ , hence extends to an automorphism of  $\mathcal{O}_L$  and  $L$ . For an element  $\alpha \in \mathcal{O}_L$  and  $n \in \mathbb{Z}$ , we write  $\alpha^{\varphi^n} := \varphi^n(\alpha)$ , and for a power series  $F \in \mathcal{O}_L[[X]]$ , we define  $F^{\varphi^n}$  by applying  $\varphi^n$  to all coefficients of  $F$ . If  $F$  is a formal group law over  $\mathcal{O}_L$ , so is  $F^{\varphi^n}$ .

**3.1. Lubin-Tate group laws.** In the rest of §3, we fix a complete unramified extension  $L/K$ . As  $\mathfrak{p}_L = \mathfrak{p} \mathcal{O}_L$ , we write  $\text{mod } \mathfrak{p}$  for  $\text{mod } \mathfrak{p} \mathcal{O}_L$ .

**Proposition 3.1.** *Let  $\pi$  be a uniformizer of  $L$ , and let  $f \in \mathcal{O}_L[[X]]$  satisfy the following:*

$$(1) \quad f(X) \equiv \pi X \pmod{\text{deg } 2}, \quad f(X) \equiv X^q \pmod{\mathfrak{p}}.$$

*Then there exists a unique formal group law  $F_f$  over  $\mathcal{O}_L$  such that  $f \in \text{Hom}_{\mathcal{O}_L}(F_f, F_f^\varphi)$ .*

**Lemma 3.2.** *Let  $\pi, \pi'$  be uniformizers of  $L$  and let  $f, f' \in \mathcal{O}_L[[X]]$  satisfy (1) for  $\pi, \pi'$ , respectively. Assume that  $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$  satisfy  $\pi' \alpha_i = \pi \alpha_i^\varphi$  for  $1 \leq i \leq n$ . Then there is a unique  $F \in \mathcal{O}_L[[X_1, \dots, X_n]]$  satisfying the following:*

$$F \equiv \alpha_1 X_1 + \dots + \alpha_n X_n \pmod{\text{deg } 2}, \quad f' \circ F = F^\varphi \circ f.$$

*Proof.* It suffices to show that for each  $m \geq 1$ , there is a unique polynomial  $F_m$  of degree  $\leq m$  that satisfies the conditions  $\text{mod } \text{deg}(m+1)$ . The case  $m = 1$  is assumed, and suppose we have  $F_m$ , and let  $G_{m+1} := f' \circ F_m - F_m^\varphi \circ f$ . Then as  $G_{m+1} \equiv F_m^q - F_m^\varphi(X_1^q, \dots, X_n^q) \equiv 0 \pmod{\mathfrak{p}}$ , its coefficients are divisible by  $\pi'$ . Now we show that a homogeneous polynomial  $H_{m+1} := F_{m+1} - F_m$  of degree  $m+1$  is uniquely determined. We need  $f' \circ F_{m+1} - F_{m+1}^\varphi \circ f = G_{m+1} + (f' \circ H_{m+1} - H_{m+1}^\varphi \circ f) \equiv G_{m+1} + (\pi' H_{m+1} - \pi^{m+1} H_{m+1}^\varphi) = 0 \pmod{\text{deg}(m+2)}$ . For any monomial of degree  $m+1$ , if we let  $\pi' \beta$  be its coefficient in  $G_{m+1}$ , and  $\alpha$  its coefficient in  $H_{m+1}$ , then  $\pi' \beta + \pi' \alpha - \pi^{m+1} \alpha^\varphi = 0$ , hence  $\alpha = -\beta - \sum_{i=1}^{\infty} (\pi^{m+1}/\pi')^{1+\varphi+\dots+\varphi^{i-1}} \beta^{\varphi^i}$ .  $\square$

<sup>2</sup>For  $\phi: \mathcal{O}_{K'} \rightarrow \mathcal{O}_{K''}$ , we have  $\phi(\mathfrak{p}_{K'}) \subset \mathfrak{p}_{K''}$ .

<sup>3</sup>This is true if  $E$  is finite over  $E \cap K^{\text{ur}}$ . When  $E/K$  is totally ramified of infinite degree,  $\mathcal{O}_E$  is not noetherian, as finite extensions  $K'_1 \subset K'_2 \subset \dots$  inside  $E$  give a sequence  $\mathfrak{p}_{K'_1} \mathcal{O}_E \subsetneq \mathfrak{p}_{K'_2} \mathcal{O}_E \subsetneq \dots$  of ideals.

*Proof.* (of Proposition 3.1) Applying the lemma for  $\pi = \pi'$ ,  $f = f'$ ,  $n = 2$ ,  $\alpha_1 = \alpha_2 = 1$ , we get a unique  $F_f \in \mathcal{O}_L[[X, Y]]$  with  $F_f \equiv X + Y \pmod{\deg 2}$  and  $f \circ F_f = F_f^\varphi \circ f$ . As  $F_f(Y, X)$  enjoys the same property,  $F_f(X, Y) = F_f(Y, X)$ . Similarly,  $F_f(F_f(X, Y), Z)$  and  $F_f(X, F_f(Y, Z))$  both satisfy the conditions of the lemma for  $n = 3$ ,  $\alpha_1 = \alpha_2 = \alpha_3 = 1$ , hence they are equal. Thus  $F_f$  is a formal group law and  $f \in \text{Hom}_{\mathcal{O}_L}(F_f, F_f^\varphi)$ .  $\square$

**Definition 3.3.** Let  $\pi, \pi'$  be uniformizers of  $L$  and set  $A_{\pi, \pi'}^L := \{\theta \in \mathcal{O}_L \mid \pi' \theta = \pi \theta^\varphi\}$ . It is an additive group, the multiplication gives  $A_{\pi, \pi'}^L \times A_{\pi', \pi''}^L \rightarrow A_{\pi, \pi''}^L$ , and  $A_{\pi, \pi}^L = \mathcal{O}_K$ . Let  $f, f' \in \mathcal{O}_L[[X]]$  satisfy (1) for  $\pi, \pi'$ , respectively. For every  $\theta \in A_{\pi, \pi'}^L$ , Lemma 3.2 gives a unique  $[\theta]_{f, f'} \in \mathcal{O}_L[[X]]$  such that  $[\theta]_{f, f'}(X) \equiv \theta X \pmod{\deg 2}$  and  $f' \circ [\theta]_{f, f'} = [\theta]_{f, f'}^\varphi \circ f$ .

**Proposition 3.4.** For  $\pi, \pi'$  and  $f, f'$  as above,  $[\theta]_{f, f'} \in \text{Hom}_{\mathcal{O}_L}(F_f, F_{f'})$  for all  $\theta \in A_{\pi, \pi'}^L$ . The map  $[\cdot]_{f, f'} : A_{\pi, \pi'}^L \rightarrow \text{Hom}_{\mathcal{O}_L}(F_f, F_{f'})$  is injective and satisfies

$$[\theta]_{f, f'} +_{F_{f'}} [\theta']_{f, f'} = [\theta + \theta']_{f, f'}, \quad [\theta']_{f', f''} \circ [\theta]_{f, f'} = [\theta \theta']_{f, f''}.$$

In particular,  $[\cdot]_f := [\cdot]_{f, f} : \mathcal{O}_K \rightarrow \text{End}_{\mathcal{O}_L}(F_f)$  is an injective ring homomorphism<sup>4</sup>.

*Proof.* For  $[\theta] := [\theta]_{f, f'}$ , we have  $[\theta] \circ F_f = F_{f'} \circ [\theta]$ , because the equalities:

$$\begin{aligned} f' \circ ([\theta] \circ F_f) &= [\theta]^\varphi \circ f \circ F_f = ([\theta]^\varphi \circ F_f^\varphi) \circ f = ([\theta] \circ F_f)^\varphi \circ f, \\ f' \circ (F_{f'} \circ [\theta]) &= F_{f'}^\varphi \circ f' \circ [\theta] = (F_{f'}^\varphi \circ [\theta]^\varphi) \circ f = (F_{f'} \circ [\theta])^\varphi \circ f, \end{aligned}$$

show that both sides satisfy the conditions of Lemma 3.2 for  $\pi = \pi'$ ,  $n = 2$ ,  $\alpha_1 = \alpha_2 = \theta$ . As  $[\theta]_{f, f'} +_{F_{f'}} [\theta']_{f, f'}$  (resp.  $[\theta']_{f', f''} \circ [\theta]_{f, f'}$ ) has the property that characterizes  $[\theta + \theta']_{f, f'}$  (resp.  $[\theta \theta']_{f, f''}$ ), they coincide. Injectivity of  $[\cdot]_{f, f'}$  follows from  $[\theta]_{f, f'}(X) \equiv \theta X \pmod{\deg 2}$ .  $\square$

**3.2. Lubin-Tate extensions.** As  $\mathcal{O}_L$  is a CDVR, for any finite extension  $L'/L$ , the integral closure  $\mathcal{O}_{L'}$  of  $\mathcal{O}_L$  in  $L'$  is a CDVR by Proposition 7.1, and let  $\mathfrak{p}_{L'}$  be its maximal ideal.

**Proposition 3.5.** Let  $\pi$  be a uniformizer  $\pi$  of  $L$ , and let  $f \in \mathcal{O}_L[X]$  be a monic polynomial satisfying (1), e.g.  $f(X) = \pi X + X^q$ . For each  $m \geq 1$ , define a polynomial  $f_m$  by  $f_m := f^{\varphi^{m-1}} \circ \dots \circ f^\varphi \circ f$ , and let  $L(\boldsymbol{\mu}_{f, m})$  be its splitting field over  $L$ . Let

$$\boldsymbol{\mu}_{f, m} := \{\alpha \in L(\boldsymbol{\mu}_{f, m}) \mid f_m(\alpha) = 0\},$$

then  $\boldsymbol{\mu}_{f, m} \subset \mathcal{O}_{L(\boldsymbol{\mu}_{f, m})}$  because  $f_m(X) \in \mathcal{O}_L[X]$ .

- (i) The set  $\boldsymbol{\mu}_{f, m}$  is an  $\mathcal{O}_K$ -module by  $+_{F_f}$  and  $[\cdot]_f$ . Choose any  $\alpha \in \boldsymbol{\mu}_{f, m} \setminus \boldsymbol{\mu}_{f, m-1}$ . Then the following is an isomorphism of  $\mathcal{O}_K$ -modules:

$$\mathcal{O}_K/\mathfrak{p}^m \ni a \mapsto [a]_f(\alpha) \in \boldsymbol{\mu}_{f, m}.$$

- (ii)  $L(\boldsymbol{\mu}_{f, m})/L$  is totally ramified and  $-\alpha$  is a uniformizer of  $L(\boldsymbol{\mu}_{f, m})$ . Also,  $\boldsymbol{\mu}_{f, m} \setminus \boldsymbol{\mu}_{f, m-1}$  is the set of all conjugates of  $\alpha$  over  $L$ , and  $N_{L(\boldsymbol{\mu}_{f, m})/L}(-\alpha) = \pi^{\varphi^{m-1}}$ .

<sup>4</sup>This means that  $(F_f, [\cdot]_f)$  is a formal  $\mathcal{O}_K$ -module law, and  $[\theta]_{f, f'} : (F_f, [\cdot]_f) \rightarrow (F_{f'}, [\cdot]_{f'})$  is a homomorphism of formal  $\mathcal{O}_K$ -module laws. Also, when  $\pi \in K$ , we have  $f = [\pi]_f$ .

(iii) *The following is an isomorphism of abelian groups, independent of the choice of  $\alpha$ :*

$$\begin{aligned} \rho_{f,m} : \text{Gal}(L(\boldsymbol{\mu}_{f,m})/L) &\xrightarrow{\cong} (\mathcal{O}_K/\mathfrak{p}^m)^\times \\ (\alpha \mapsto [u]_f(\alpha)) &\longmapsto u \bmod \mathfrak{p}^m \end{aligned}$$

*Proof.* In the proof, we omit the suffix  $f$  in  $+_{F_f}, [\cdot]_f$ , and write  $L' = L(\boldsymbol{\mu}_{f,m})$ .

(i):  $\boldsymbol{\mu}_{f,m} \setminus \boldsymbol{\mu}_{f,m-1}$  is the set of all roots of  $h(X) := f_m(X)/f_{m-1}(X)$ , and we have  $h(X) \equiv \pi^{\varphi^{m-1}} \pmod{X}$  and  $h(X) \equiv X^{(q-1)q^{m-1}} \pmod{\mathfrak{p}}$ , because  $h(X) = j(f_{m-1}(X))$  for  $j(X) := f^{\varphi^{m-1}}(X)/X$ , with  $j(X) \equiv \pi^{\varphi^{m-1}} \pmod{X}$  and  $j(X) \equiv X^{q-1} \pmod{\mathfrak{p}}$ . Hence for all  $\alpha \in \boldsymbol{\mu}_{f,m} \setminus \boldsymbol{\mu}_{f,m-1}$ , we have  $0 = h(\alpha) \equiv \alpha^{(q-1)q^{m-1}} \pmod{\mathfrak{p}\mathcal{O}_{L'}}$ , therefore  $\alpha \in \mathfrak{p}_{L'}$ . Now as  $m$  was arbitrary,  $\boldsymbol{\mu}_{f,m} \subset \mathfrak{p}_{L'}$ , and we can substitute its elements into  $+_F, [\cdot]$ . As  $f \circ F_f = F_f^\varphi \circ f$  and  $f \circ [a] = [a]^\varphi \circ f$  by definition, we have  $f_m \circ F_f = F_f^{\varphi^m} \circ f_m$  and  $f_m \circ [a] = [a]^{\varphi^m} \circ f_m$ , hence  $\boldsymbol{\mu}_{f,m}$  is closed under  $+_F$  and  $[\cdot]$  and is an  $\mathcal{O}_K$ -module. As  $|\boldsymbol{\mu}_{f,m}| \leq \deg f_m = q^m$ , the annihilator<sup>5</sup> of any  $\alpha \in \boldsymbol{\mu}_{f,m}$  contains  $\mathfrak{p}^m$ , i.e. if  $\pi_0$  is a uniformizer of  $K$ , we have  $[\pi_0^m](\alpha) = 0$  for all  $\alpha \in \boldsymbol{\mu}_{f,m}$ . On the other hand:

**Lemma 3.6.** *Let  $g \in \mathcal{O}_L[[X]]$ . If  $g(\alpha) = 0$  for all  $\alpha \in \boldsymbol{\mu}_{f,m}$ , then  $f_m(X) \mid g(X)$  in  $\mathcal{O}_L[[X]]$ .*

*Proof.* For  $\alpha \in \boldsymbol{\mu}_{f,m}$ , if  $g(X) = \sum_{i=0}^{\infty} a_i X^i$ ,  $g(\alpha) = 0$  then if we let  $b_i := \sum_{j=0}^{\infty} a_{i+j+1} \alpha^j \in \mathcal{O}_{L'}$  for each  $i \geq 0$ , then  $g(X) = (X - \alpha) \cdot \sum_{i=0}^{\infty} b_i X^i$  in  $\mathcal{O}_{L'}[[X]]$ . Repeating, we get  $g(X) = f_m(X) \cdot g'(X)$ , and as  $g, f_m \in \mathcal{O}_L[[X]]$ , also  $g'$  has coefficients in  $L \cap \mathcal{O}_{L'} = \mathcal{O}_L$ .  $\square$

Therefore  $[\pi_0^m](X) = f_m(X)g_m(X)$ , and as the coefficients of  $X$  in  $[\pi_0^m]$  and  $f_m$  both have valuation  $m$  in  $L$ , the constant term of  $g_m(X)$  is in  $\mathcal{O}_L^\times$ . Hence for  $\alpha \in \boldsymbol{\mu}_{f,m} \subset \mathfrak{p}_{L'}$  we have  $g_{m-1}(\alpha) \neq 0$ . Therefore,  $[\pi_0^{m-1}](\alpha) = 0$  implies  $f_{m-1}(\alpha) = 0$ , i.e.  $\alpha \in \boldsymbol{\mu}_{f,m-1}$ . We have shown<sup>6</sup> that the annihilator of  $\alpha \in \boldsymbol{\mu}_{f,m} \setminus \boldsymbol{\mu}_{f,m-1}$  is exactly  $\mathfrak{p}^m$ . Therefore the stated  $\mathcal{O}_K$ -linear map is injective, and as  $|\boldsymbol{\mu}_{f,m}| \leq q^m = |\mathcal{O}_K/\mathfrak{p}^m|$  it is an isomorphism.

(ii): By (i), we have  $\boldsymbol{\mu}_{f,m} = \{[a](\alpha) \mid a \in \mathcal{O}_K\} \subset L(\alpha)$ , therefore  $L' = L(\alpha)$ , and as  $\alpha$  is a root of  $h$ , we get  $[L' : L] \leq \deg h$ . On the other hand, the constant term of  $h(X)$  is  $\pi^{\varphi^{m-1}} = \prod_{\alpha} (-\alpha)$  where  $\alpha$  runs through  $\boldsymbol{\mu}_{f,m} \setminus \boldsymbol{\mu}_{f,m-1}$ , so taking  $v_{L'}$  of both sides, we get  $e(L'/L) \geq \deg h$ . As  $e(L'/L) \leq [L' : L]$ , these are all equalities,  $h$  is irreducible and all the claims follow.

(iii): As  $L' = L(\alpha)$ , an element  $\sigma \in \text{Gal}(L'/L)$  is determined by  $\sigma(\alpha)$ , hence the stated map is injective. As  $[u] \in \mathcal{O}_L[[X]]$  is fixed by any  $\sigma \in \text{Gal}(L'/L)$ , it is a homomorphism, and  $[L' : L] = \deg h = (q-1)q^{m-1} = |(\mathcal{O}_K/\mathfrak{p}^m)^\times|$  shows that it is an isomorphism. If  $\sigma(\alpha) = [u](\alpha)$  then  $\sigma([u](\alpha)) = [u](\sigma(\alpha)) = [u'u](\alpha) = [u]([u](\alpha))$ , hence the map is independent of the choice of  $\alpha$ .  $\square$

<sup>5</sup>Kernel of the  $\mathcal{O}_K$ -linear map  $\mathcal{O}_K \ni a \mapsto [a](\alpha) \in \boldsymbol{\mu}_{f,m}$ .

<sup>6</sup>We have also shown  $\boldsymbol{\mu}_{f,m} = \{\alpha \in \mathfrak{p}_{L'} \mid [a](\alpha) = 0 \ (\forall a \in \mathfrak{p}^m)\}$  for  $\forall m \geq 1$  and  $L(\boldsymbol{\mu}_{f,m}) \subset \forall L' \subset \bar{L}$ .

## 4. UNIQUENESS OF LUBIN-TATE EXTENSIONS AND ARTIN MAPS

4.1. **Isomorphisms of Lubin-Tate group laws.**  $\widehat{K}^{\text{ur}}$  denotes the completion of  $K^{\text{ur}}$ .

**Proposition 4.1.** *Let  $f, f' \in \mathcal{O}_{\widehat{K}^{\text{ur}}}[[X]]$  satisfy (1) for uniformizers  $\pi, \pi'$  of  $\widehat{K}^{\text{ur}}$ , respectively. For  $\theta \in A_{\pi, \pi'}^{\widehat{K}^{\text{ur}}} \cap \mathcal{O}_{\widehat{K}^{\text{ur}}}^{\times}$  (which is not empty by Lemma 4.2), the homomorphism  $[\theta] := [\theta]_{f, f'} \in \text{Hom}_{\mathcal{O}_{\widehat{K}^{\text{ur}}}}(F_f, F_{f'})$  is an isomorphism of formal group laws.*

*Proof.* The  $[\theta]$  is an isomorphism because  $[\theta](X) \equiv \theta X \pmod{\text{deg } 2}$ .  $\square$

**Lemma 4.2.** *For  $L = \widehat{K}^{\text{ur}}$ , the map  $\mathcal{O}_L^{\times} \ni u \mapsto u^{\varphi}/u \in \mathcal{O}_L^{\times}$  is surjective.*

*Proof.* As  $\mathcal{O}_L^{\times} \cong \varprojlim_m (\mathcal{O}_L/\mathfrak{p}_L^{m+1})^{\times}$ , for  $x \in \mathcal{O}_L^{\times}$ , it suffices to show that, for all  $m \geq 0$ , there exists a  $u_m \in \mathcal{O}_L^{\times}$  such that  $u_m^{\varphi}/u_m \equiv x \pmod{\mathfrak{p}_L^{m+1}}$ . For  $m = 0$ , on  $(\mathcal{O}_L/\mathfrak{p}_L)^{\times} \cong \overline{\mathbb{F}}_q^{\times}$ , the map  $\bar{u} \mapsto \bar{u}^{\varphi}/\bar{u} = \bar{u}^{q-1}$  is surjective. Suppose we have  $u_m$ , and let  $x/(u_m^{\varphi}/u_m) = 1 + \alpha\pi^{m+1}$  for a uniformizer  $\pi$  of  $K$ . On  $\mathcal{O}_L/\mathfrak{p}_L \cong \overline{\mathbb{F}}_q$  the map  $\bar{u} \mapsto \bar{u}^{\varphi} - \bar{u} = \bar{u}^q - \bar{u}$  is surjective, hence there is  $\beta \in \mathcal{O}_L$  with  $\beta^{\varphi} - \beta \equiv \alpha \pmod{\mathfrak{p}_L}$ . Letting  $u_{m+1} = u_m(1 + \beta\pi^{m+1})$ , we get  $u_{m+1}^{\varphi}/u_{m+1} \equiv x \pmod{\mathfrak{p}_L^{m+2}}$ .  $\square$

Note that every complete unramified extension  $L$  of  $K$  is contained in  $\widehat{K}^{\text{ur}}$ , and all uniformizers of  $L$  are also uniformizers of  $\widehat{K}^{\text{ur}}$ , hence Lubin-Tate group laws  $F_f$  over  $\mathcal{O}_L$  can be considered as those over  $\mathcal{O}_{\widehat{K}^{\text{ur}}}$ .

**Proposition 4.3.** *Let  $L/K$  be finite unramified of degree  $n$ . Let  $f, f' \in \mathcal{O}_L[[X]]$  satisfy (1) for  $\pi, \pi' \in L$ , respectively, and  $[\theta] = [\theta]_{f, f'} \in \mathcal{O}_{\widehat{K}^{\text{ur}}}[[X]]$  as in Proposition 4.1. Then  $[\theta]^{\varphi^n} = [\theta] \circ [N_{L/K}(\pi'/\pi)]_f$ . In particular, if  $N_{L/K}(\pi) = N_{L/K}(\pi')$ , then  $[\theta]_{f, f'} \in \mathcal{O}_L[[X]]$ .*

*Proof.* Define  $f_m \in \mathcal{O}_L[[X]]$  for  $m \geq 1$  as in Proposition 3.5. Then we have  $f_n(X) \equiv \pi^{\varphi^{n-1}} \cdots \pi^{\varphi} \cdot \pi X = N_{L/K}(\pi)X \pmod{\text{deg } 2}$ , and  $f \circ f_n = (f_n)^{\varphi} \circ f$  because  $\varphi^n = \text{id}$  on  $L$ . Thus  $f_n = [N_{L/K}(\pi)]_f$  by the uniqueness in Lemma 3.2. Similarly  $f'_n = [N_{L/K}(\pi')]_{f'}$ . Now as  $f' \circ [\theta] = [\theta]^{\varphi} \circ f$ , we get  $f'_n \circ [\theta] = [\theta]^{\varphi^n} \circ f_n$ , and therefore  $[\theta]^{\varphi^n} \circ f_n = [N_{L/K}(\pi')]_{f'} \circ [\theta] = [\theta \cdot N_{L/K}(\pi')]_{f, f'} = [\theta] \circ [N_{L/K}(\pi')]_f = [\theta] \circ [N_{L/K}(\pi'/\pi)]_f \circ f_n$ . Now as  $f_n = f^{\varphi^{n-1}} \circ \cdots \circ f^{\varphi} \circ f$ , use the following lemma repeatedly for  $f, f^{\varphi}, \dots, f^{\varphi^{n-1}}$ .  $\square$

**Lemma 4.4.** *Let  $L$  be any complete unramified extension of  $K$ . Let  $\pi$  be a uniformizer of  $L$ , and let  $f \in \mathcal{O}_L[[X]]$  satisfy (1). For  $h \in \mathcal{O}_L[[X]]$  and  $m \geq 1$ , we have  $h \circ f \equiv 0 \pmod{\mathfrak{p}^m} \implies h \equiv 0 \pmod{\mathfrak{p}^m}$ . In particular, the following is an injection:*

$$\circ f : \mathcal{O}_L[[X]] \ni h \longmapsto h \circ f \in \mathcal{O}_L[[X]].$$

*Proof.* As the statement is empty for  $m = 0$ , use induction on  $m$ . If  $h \circ f = \pi^m \cdot g$ , then by induction hypothesis  $h = \pi^{m-1} \cdot h'$ , and  $h' \circ f = \pi \cdot g$ . Taking mod  $\mathfrak{p}$  we get  $h'(X^q) \equiv 0 \pmod{\mathfrak{p}}$ , hence  $h' \equiv 0 \pmod{\mathfrak{p}}$ , i.e.  $h \equiv 0 \pmod{\mathfrak{p}^m}$ .  $\square$

**4.2. Lubin-Tate extensions and Artin maps.** Now we turn to the extensions  $L(\boldsymbol{\mu}_{f,m})$ .

**Proposition 4.5.** *Let  $L$  be a complete unramified extension of  $K$ . Let monics  $f, f' \in \mathcal{O}_L[X]$  satisfy (1) for uniformizers  $\pi, \pi' \in L$ , respectively. For  $[\theta] = [\theta]_{f,f'} \in \mathcal{O}_{\widehat{K}^{\text{ur}}}[[X]]$  as in Proposition 4.1, substituting into  $[\theta]$  gives  $\boldsymbol{\mu}_{f,m} \cong \boldsymbol{\mu}_{f',m}$  as  $\mathcal{O}_K$ -modules for all  $m \geq 1$ . Moreover, if  $[\theta] \in \mathcal{O}_L[[X]]$ , then  $L(\boldsymbol{\mu}_{f,m}) = L(\boldsymbol{\mu}_{f',m})$  and  $\rho_{f,m} = \rho_{f',m}$ .*

*Proof.* Substituting into  $[\theta]$  maps  $\boldsymbol{\mu}_{f,m}$  into  $\boldsymbol{\mu}_{f',m}$  because  $f'_m \circ [\theta] = [\theta]^{\varphi^m} \circ f_m$ , and is  $\mathcal{O}_K$ -linear because  $[\theta] \circ [a]_f = [\theta \cdot a]_{f,f'} = [a]_{f'} \circ [\theta]$ . Considering  $[\theta^{-1}]$  shows  $\boldsymbol{\mu}_{f,m} \cong \boldsymbol{\mu}_{f',m}$ . If  $[\theta] \in \mathcal{O}_L[[X]]$ , then  $\boldsymbol{\mu}_{f',m} = [\theta](\boldsymbol{\mu}_{f,m}) \subset L(\boldsymbol{\mu}_{f,m})$ , and  $L(\boldsymbol{\mu}_{f,m}) = L(\boldsymbol{\mu}_{f',m})$  as  $[\theta^{-1}] = [\theta]^{-1} \in \mathcal{O}_L[[X]]$ . In this case, an  $L$ -automorphism  $\alpha \mapsto [u]_f(\alpha)$  of  $L(\boldsymbol{\mu}_{f,m})$  maps  $[\theta](\alpha)$  to  $[\theta]([u]_f(\alpha)) = [\theta \cdot u]_{f,f'}(\alpha) = [u]_{f'}([\theta](\alpha))$ , hence  $\rho_{f,m} = \rho_{f',m}$ .  $\square$

**Lemma 4.6.** *If  $L/K$  is finite unramified of degree  $n$ , then  $N = N_{L/K}$  surjects onto  $v_K^{-1}(n\mathbb{Z})$ .*

*Proof.* If we take a uniformizer  $\pi$  of  $K$ , then  $v_K^{-1}(n\mathbb{Z}) = \mathcal{O}_K^\times \times \langle \pi^n \rangle$ , hence it suffices to show  $N : \mathcal{O}_L^\times \rightarrow \mathcal{O}_K^\times$  is surjective. We have  $\mathcal{O}_K^\times \cong \varprojlim_m (\mathcal{O}_K/\mathfrak{p}^m)^\times$ , the same for  $\mathcal{O}_L^\times$ , and

$N(1+\mathfrak{p}_L^m) \subset 1+\mathfrak{p}^m$ . Therefore for  $x \in \mathcal{O}_K^\times$ , it is enough to construct  $u_m \bmod \mathfrak{p}^m \in (\mathcal{O}_L^\times/\mathfrak{p}^m)^\times$  for all  $m \geq 1$ , satisfying  $N(u_m) \equiv x \pmod{\mathfrak{p}^m}$  and  $u_{m+1} \equiv u_m \pmod{\mathfrak{p}^m}$ . For  $m = 1$ , the  $N$  induces the norm map  $(\mathcal{O}_L/\mathfrak{p}_L)^\times \rightarrow (\mathcal{O}_K/\mathfrak{p})^\times$ , which is surjective. Suppose we have  $u_m$ , and let  $x/N(u_m) = 1 + \alpha\pi^m$ . On  $(1 + \mathfrak{p}_L^m)/(1 + \mathfrak{p}_L^{m+1}) \cong \mathbb{F}_{q^n}$ , the  $N$  induces the trace map  $\mathcal{O}_L/\mathfrak{p}_L \rightarrow \mathcal{O}_K/\mathfrak{p}$ , which is surjective, hence there is  $\beta \in \mathcal{O}_L$  with trace  $\equiv \alpha \pmod{\mathfrak{p}}$ , hence letting  $u_{m+1} = u_m(1 + \beta\pi^m)$ , we get  $N(u_{m+1}) \equiv x \pmod{\mathfrak{p}^{m+1}}$ .  $\square$

**Definition 4.7.** Let  $x \in \mathfrak{p} \cap K^\times$  with  $v_K(x) = n$ , and let  $L/K$  be finite unramified of degree  $n$ . By Lemma 4.6, there is a uniformizer  $\pi$  of  $L$  with  $N_{L/K}(\pi) = x$ . Then  $L(\boldsymbol{\mu}_{f,m})$  and  $\rho_{f,m}$  for  $m \geq 1$  (for a monic  $f \in \mathcal{O}_L[X]$  satisfying (1) for  $\pi$ ) depend only on  $x$  by Propositions 4.3 and 4.5, so we denote them by  $K_x^m$  and  $\rho_m$ . We write  $K_x^{\text{ram}} := \bigcup_{m \geq 1} K_x^m$ , which is totally ramified over  $L$ , and  $K_x^{\text{LT}} := K_x^{\text{ram}} K^{\text{ur}}$ .

We describe its Galois group. For  $m \leq m'$ , the restriction  $\text{Gal}(K_x^{m'}/L) \rightarrow \text{Gal}(K_x^m/L)$  is mapped to the natural surjection  $(\mathcal{O}_K/\mathfrak{p}^{m'})^\times \rightarrow (\mathcal{O}_K/\mathfrak{p}^m)^\times$  by  $\rho_{m'}, \rho_m$ . Taking the limit:

$$\text{Gal}(K_x^{\text{ram}}/L) \ni (\alpha \mapsto [u](\alpha)) \xrightarrow{\cong} u \in \mathcal{O}_K^\times,$$

where  $\alpha \mapsto [u](\alpha)$  means  $\alpha \in \boldsymbol{\mu}_{f,m}$  is mapped to  $[u]_f(\alpha)$  for any  $f$ . As  $K_x^{\text{ram}}/L$  is totally ramified, we have  $K_x^{\text{ram}} \cap K^{\text{ur}} = L$ . By  $K^{\text{ur}} = L^{\text{ur}}$ :

$$\begin{aligned} \text{Gal}(K_x^{\text{LT}}/L) &\xrightarrow{\cong} \text{Gal}(K_x^{\text{ram}}/L) \times \text{Gal}(K^{\text{ur}}/L) \xrightarrow{\cong} \mathcal{O}_K^\times \times \widehat{\mathbb{Z}} \\ &(\alpha \mapsto [u](\alpha), \text{Frob}_L^b) \longmapsto (u, b) \end{aligned}$$

By composing its inverse  $\mathcal{O}_K^\times \times \widehat{\mathbb{Z}} \xrightarrow{\cong} \text{Gal}(K_x^{\text{LT}}/L) \subset \text{Gal}(K_x^{\text{LT}}/K)$  with  $v_K^{-1}(n\mathbb{Z}) = \mathcal{O}_K^\times \times \langle x \rangle \ni u \cdot x^b \longmapsto (u, b) \in \mathcal{O}_K^\times \times \mathbb{Z}$ , we define the *Artin map* associated to  $x$ :

$$\text{Art}_K^x : v_K^{-1}(n\mathbb{Z}) \longrightarrow \text{Gal}(K_x^{\text{LT}}/K).$$

**Theorem 4.8.** (i) *The fields  $K_x^m K^{\text{ur}}$  for  $m \geq 1$ , hence their union  $K_x^{\text{LT}}$ , do not depend on the choice of  $x \in \mathfrak{p} \cap K^\times$  (we write  $K^{\text{LT}} := K_x^{\text{LT}}$ ).*  
(ii) *If  $v_K(x) = 1$ , then  $\text{Art}_K^x : K^\times \rightarrow \text{Gal}(K^{\text{LT}}/K)$  does not depend on the choice of  $x$ , and we write  $\text{Art}_K := \text{Art}_K^x$ . If  $v_K(x) = n$ , then  $\text{Art}_K^x = \text{Art}_K \big|_{v_K^{-1}(n\mathbb{Z})}$ .*

*Proof.* (i): For  $x_1, x_2 \in \mathfrak{p} \cap K^\times$  and  $m \geq 1$ , let  $K_{x_i}^m = L_i(\boldsymbol{\mu}_{f_i, m})$  for  $i = 1, 2$ . Considering  $F_{f_i}$  over  $\widehat{K}^{\text{ur}}$ , Propositions 4.1 and 4.5 show that  $\widehat{K}^{\text{ur}}(\boldsymbol{\mu}_{f_i, m}) = K_{x_i}^m \widehat{K}^{\text{ur}}$  are the same for  $i = 1, 2$ . By the following lemma, they are the completions of  $K_{x_i}^m K^{\text{ur}}$ , and  $K_{x_1}^m K^{\text{ur}} = K_{x_2}^m K^{\text{ur}}$ .

**Lemma 4.9.** *Let  $E$  be an unramified extension of  $K$  and  $E', E''$  be finite extensions of  $E$ . Then (i)  $E' \widehat{E} = \widehat{E}'$ ,  $\widehat{E} \cap E' = E$ , and  $[\widehat{E}' : \widehat{E}] = [E' : E]$ , (ii)  $\widehat{E}' = \widehat{E}'' \implies E' = E''$ .*

*Proof.* (i) follows from Proposition 7.1(ii). (i) implies  $\widehat{E} \cap \overline{K} = E$ , hence (ii).  $\square$

(ii): For  $x, x' \in \mathfrak{p} \cap K^\times$  with  $v_K(x) = v_K(x') = n$ , we prove  $\text{Art}_K^{x'}(x') = \text{Art}_K^x(x')$ . By definition,  $\text{Art}_K^{x'}(x')$  acts as  $\text{Frob}_K^n$  on  $K^{\text{ur}}$  and  $\text{id}$  on  $K_x^{\text{ram}}$ , and  $\text{Art}_K^x(x')$  acts as  $\text{Frob}_K^n$  on  $K^{\text{ur}}$  and  $\alpha \mapsto [x'/x](\alpha)$  on  $K_x^{\text{ram}}$ . Let  $K_x^m = L(\boldsymbol{\mu}_{f, m})$ ,  $K_{x'}^m = L(\boldsymbol{\mu}_{f', m})$  and  $[\theta] = [\theta]_{f, f'} : \boldsymbol{\mu}_{f, m} \cong \boldsymbol{\mu}_{f', m}$  as in Propositions 4.1 and 4.5. For  $\alpha \in \boldsymbol{\mu}_{f, m}$ , we have  $\text{Art}_K^{x'}(x')([\theta](\alpha)) = [\theta]^{\varphi^{-n}}([x'/x]_f(\alpha)) = ([\theta] \circ [x'/x]_f)^{\varphi^{-n}}(\alpha) = [\theta](\alpha)$  by Lemma 4.3, hence  $\text{Art}_K^{x'}(x')$  acts as  $\text{id}$  on  $K_x^{\text{ram}}$ . Thus  $\text{Art}_K^{x'}(x') = \text{Art}_K^x(x')$ . Now for any  $x'' \in \mathfrak{p} \cap K^\times$  with  $v_K(x'') = n$ , we get  $\text{Art}_K^{x'}(x'') = \text{Art}_K^{x''}(x'') = \text{Art}_K^x(x'')$ , and as  $v_K^{-1}(n\mathbb{Z})$  is generated by such elements,  $\text{Art}_K^{x'} = \text{Art}_K^x$ . As for the latter part, if  $v_K(x) = 1$  and  $K_x^m = K(\boldsymbol{\mu}_{f, m})$ , then  $K_x^m = L(\boldsymbol{\mu}_{f, m}) = K_x^m L$  for  $[L : K] = n$ , and  $\text{Art}_K^x = \text{Art}_K^x \big|_{v_K^{-1}(n\mathbb{Z})}$  follows from the definition.  $\square$

**Corollary 4.10.** *For an algebraic extension  $E/K$  with  $E \supset K^{\text{ur}}$ , we set:*

$$W(E/K) := \{\sigma \in \text{Gal}(E/K) \mid \sigma|_{K^{\text{ur}}} \in \text{Frob}_K^{\mathbb{Z}}\} \quad (\text{the Weil group of } E/K).$$

*Then we have  $\text{Art}_K : K^\times \xrightarrow{\cong} W(K^{\text{LT}}/K)$ . If  $x \in K^\times$ , then  $\sigma := \text{Art}_K(x)$  is the element of  $\text{Gal}(K^{\text{LT}}/K)$  characterized by  $\sigma|_{K^{\text{ur}}}(x) = \text{Frob}_K^{v_K(x)}$  and  $\sigma|_{K_x^{\text{ram}}} = \text{id}$ .*

## 5. NORM GROUPS AND THE BASE CHANGE

**5.1. Coleman operator and norm groups.** Here we let  $L/K$  be finite unramified, and fix a uniformizer  $\pi$  of  $L$  and a monic polynomial  $f \in \mathcal{O}_L[X]$  satisfying (1). We set  $x := N_{L/K}(\pi)$ . We write  $+_f$  for  $+_{F_f}$  and  $\boldsymbol{\mu}_m$  for  $\boldsymbol{\mu}_{f, m}$  (we will not see roots of unity here). First we determine the image of the map  $\circ_f$  of Lemma 4.4.

**Lemma 5.1.** *If  $g \in \mathcal{O}_L[[X]]$  satisfies  $g(X +_f \alpha) = g(X)$  for all  $\alpha \in \boldsymbol{\mu}_1$ , then  $g = h \circ f$  for some  $h(X)$  in  $\mathcal{O}_L[[X]]$ .*

*Proof.* If  $g(X +_f \alpha) = g(X)$  for all  $\alpha \in \boldsymbol{\mu}_1$ , then we can write  $g(X) - g(0) = g_1(X) \cdot f(X)$  by Lemma 3.6. Now as  $f(X +_f \alpha) = f(X) +_{F^\varphi} f(\alpha) = f(X)$ , we have  $g_1(X +_f \alpha) = g_1(X)$ .

Repeating this procedure and setting  $g_0 := g$  and  $g_i(X) - g_i(0) = g_{i+1}(X) \cdot f(X)$ , we get  $g(X) = \sum_{i=0}^{\infty} g_i(0) \cdot f(X)^i$ , hence  $h(X) := \sum_{i=0}^{\infty} g_i(0) X^i$  gives  $g = h \circ f$ .  $\square$

**Definition 5.2** (Coleman [1], de Shalit [2]). For  $g \in \mathcal{O}_L[[X]]$ , coefficients of the product  $\prod_{\alpha \in \mu_1} g(X +_f \alpha)$  are symmetric polynomials of  $\mu_1$ , hence in  $\mathcal{O}_L$ . Therefore by Lemma 4.4 and Lemma 5.1 we get a unique  $N(g) \in \mathcal{O}_L[[X]]$  satisfying:

$$(2) \quad N(g) \circ f(X) = \prod_{\alpha \in \mu_1} g(X +_f \alpha).$$

We have  $N(g_1 g_2) = N(g_1) N(g_2)$  by definition. Also, we set  $N^0(g) := g$  and

$$N^m(g) := N^{m-1}(N(g)^{\varphi^{-1}})^{\varphi} \quad (m \geq 1)^7.$$

**Lemma 5.3.** For  $m \geq 1$ , we have  $N^m(g) \circ f_m(X) = \prod_{\alpha \in \mu_m} g(X +_f \alpha)$ .

*Proof.* The case  $m = 1$  is the definition. We use induction on  $m$ . Fix a set  $A$  of representatives of  $\mu_m/\mu_1$  (regarded as  $\mathcal{O}_K$ -modules), and extend  $\varphi$  arbitrarily to  $L(\mu_m)$ . Then:

$$\prod_{\alpha \in \mu_m} g(X +_f \alpha) = \prod_{\beta \in A} \prod_{\alpha \in \mu_1} g(X +_f \beta +_f \alpha) = \prod_{\beta \in A} N(g) \circ f(X +_f \beta),$$

and  $f(X +_f \beta) = f(X) +_{f\varphi} f(\beta)$ , but as  $A \ni \beta \mapsto f(\beta)^{\varphi^{-1}} \in \mu_{m-1}$  is a bijection,

$$\text{RHS} = \prod_{\alpha \in \mu_{m-1}} N(g)(f(X) +_{f\varphi} \alpha^{\varphi}) = \left( \prod_{\alpha \in \mu_{m-1}} N(g)^{\varphi^{-1}}(f^{\varphi^{-1}}(X) +_f \alpha) \right)^{\varphi}$$

equals  $(N^{m-1}(N(g)^{\varphi^{-1}}) \circ f_{m-1}(f^{\varphi^{-1}}(X)))^{\varphi} = N^m(g) \circ f_m(X)$  by inductive hypothesis.  $\square$

**Lemma 5.4.** (i)  $N(g) \equiv g^{\varphi} \pmod{\mathfrak{p}}$ . In particular,  $N(\mathcal{O}_L[[X]]^{\times}) \subset \mathcal{O}_L[[X]]^{\times}$ .

(ii) For  $m \geq 1$ , if  $g \equiv 1 \pmod{\mathfrak{p}^m}$ , then  $N(g) \equiv 1 \pmod{\mathfrak{p}^{m+1}}$ .

(iii) If  $g \in \mathcal{O}_L[[X]]^{\times}$  and  $m \geq 1$ , then  $N^m(g)/N^{m-1}(g)^{\varphi} \equiv 1 \pmod{\mathfrak{p}^m}$ .

*Proof.* (i): As  $f(X) \equiv X^q \pmod{\mathfrak{p}}$ , LHS of (2)  $\equiv N(g)(X^q) \pmod{\mathfrak{p}}$ . On the other hand, if we write  $L' = K_x^1$ , then  $\mu_1 \subset \mathfrak{p}_{L'}$ , hence  $g(X +_f \alpha) \equiv g(X) \pmod{\mathfrak{p}_{L'}}$  for all  $\alpha \in \mu_1$ . Therefore RHS of (2)  $\equiv g(X)^q \equiv g^{\varphi}(X^q) \pmod{\mathfrak{p}}$ , and we see  $N(g) \equiv g^{\varphi} \pmod{\mathfrak{p}}$ .

(ii): If we let  $g = 1 + \pi^m h$  and  $L' = K_x^1$ , then

$$\begin{aligned} N(g) \circ f &= \prod_{\alpha \in \mu_1} (1 + \pi^m h(X +_f \alpha)) \equiv (1 + \pi^m h(X))^q \pmod{\mathfrak{p}^m \mathfrak{p}_{L'}} \\ &\equiv 1 + q\pi^m h(X) + \cdots + \pi^{mq} h(X)^q \equiv 1 \pmod{\mathfrak{p}^m \mathfrak{p}_{L'}}, \end{aligned}$$

hence  $(N(g) - 1) \circ f \equiv 0 \pmod{\mathfrak{p}^m \mathfrak{p}_{L'}}$ , and as it belongs to  $\mathcal{O}_L[[X]]$ , we have  $(N(g) - 1) \circ f \equiv 0 \pmod{\mathfrak{p}^{m+1}}$ . Therefore, by Lemma 4.4, we get  $N(g) - 1 \equiv 0 \pmod{\mathfrak{p}^{m+1}}$ .

(iii): As  $N(g)/g^{\varphi} \equiv 1 \pmod{\mathfrak{p}}$  from (i), apply (ii) to this  $m - 1$  times.  $\square$

<sup>7</sup>If we write  $N = N_f$ , this means  $N^m = N_{f\varphi^{m-1}} \circ \cdots \circ N_{f\varphi} \circ N_f$ .

**Definition 5.5.** For a finite extension  $K'/K$ , we denote the image  $N_{K'/K}(K'^{\times})$  of the norm map  $N_{K'/K} : K'^{\times} \rightarrow K^{\times}$  by  $N(K'/K)$ . For any algebraic extension  $E/K$ , define  $N(E/K) := \bigcap_{K'} N(K'/K)$  where  $K'$  runs through all the finite extensions contained in  $E$ .

**Proposition 5.6.**  $N(K_x^m/K) \subset (1 + \mathfrak{p}^m) \times \langle x \rangle$  for all  $m \geq 1$ . (It is actually an equality.<sup>8</sup>)

*Proof.* Write  $L' = L(\boldsymbol{\mu}_m) = K_x^m$  and take  $\alpha \in \boldsymbol{\mu}_m \setminus \boldsymbol{\mu}_{m-1}$ . By Proposition 3.5(ii) we have  $L'^{\times} = \mathcal{O}_{L'}^{\times} \times \langle -\alpha \rangle$  and  $N_{L'/K}(-\alpha) = N_{L/K}(\pi^{\varphi^{m-1}}) = x$ , hence it suffices to show  $N_{L'/K}(\mathcal{O}_{L'}^{\times}) \subset 1 + \mathfrak{p}^m$ . By the following Lemma 5.7, any  $u \in \mathcal{O}_{L'}^{\times}$  can be written as  $u = g(\alpha)$ ,  $g \in \mathcal{O}_L[[X]]^{\times}$ . For  $i \geq 0$ , set  $u_i := N^i(g)(0)$ . Then by Lemma 5.3 we have  $u_i = \prod_{\alpha \in \boldsymbol{\mu}_i} g(\alpha)$ , hence  $N_{L'/L}(u) = u_m/u_{m-1}$ . Lemma 5.4(iii) shows that  $u_m/u_{m-1}^{\varphi} \in 1 + \mathfrak{p}_L^m$ . Hence  $N_{L'/K}(u) = N_{L/K}(u_m/u_{m-1}) = N_{L/K}(u_m/u_{m-1}^{\varphi}) \in N_{L/K}(1 + \mathfrak{p}_L^m) \subset 1 + \mathfrak{p}^m$ , where we used  $(1 + \mathfrak{p}_L^m) \cap \mathcal{O}_K = 1 + \mathfrak{p}^m$  in the last inclusion.  $\square$

**Lemma 5.7.** If  $L'/L$  is totally ramified and  $\alpha$  is a uniformizer of  $L'$ , then  $\mathcal{O}_{L'} = \mathcal{O}_L[\alpha]$ .

*Proof.* If  $[L' : L] = n$  and  $x = \sum_{i=0}^{n-1} a_i \alpha^i$  ( $a_i \in L$ ), then  $v_{L'}(x) = \min_i \{v_{L'}(a_i \alpha^i)\}$ , as  $v_{L'}(a_i \alpha^i)$  are all distinct. Thus (i)  $x = 0 \Rightarrow a_i = 0$  ( $\forall i$ ), (ii)  $x \in \mathcal{O}_{L'} \Leftrightarrow a_i \in \mathcal{O}_L$  ( $\forall i$ ). By (i), the set  $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$  is a basis of  $L'$  over  $L$ . This and (ii) imply  $\mathcal{O}_{L'} \subset \mathcal{O}_L[\alpha]$ .  $\square$

**Corollary 5.8.** If  $E/L$  is totally ramified and  $E \supset K_x^{\text{ram}}$ , then  $N(E/K) = \langle x \rangle$ .

*Proof.* Proposition 5.6 and  $\bigcap_{m \geq 1} (1 + \mathfrak{p}^m) = \{1\}$  show that  $N(E/K) \subset N(K_x^{\text{ram}}/K) \subset \langle x \rangle$ . Therefore it suffices to show that  $N(E/K)$  contains an element with valuation  $[L : K]$ . This follows if, setting  $P = v_L^{-1}(\{1\})$ , we can show  $N(E/L) \cap P \neq \emptyset$ . We show this for general totally ramified extension  $E/L$ . For any uniformizer  $\pi$  of  $L$ , we have  $P = \pi \cdot \mathcal{O}_L^{\times}$  and  $\mathcal{O}_L^{\times} \cong \varprojlim_m \mathcal{O}_L^{\times}/(1 + \mathfrak{p}_L^m)$ , hence  $P \cong \varprojlim_m P/(1 + \mathfrak{p}_L^m)$  as sets. Therefore it is enough to show, for each  $m$ , that  $(N(E/L) \cap P)/(1 + \mathfrak{p}_L^m) \neq \emptyset$ . As any finite  $L'/L$  contained in  $E$  is totally ramified,  $(N(L'/L) \cap P)/(1 + \mathfrak{p}_L^m)$  is a non-empty subset of the finite set  $P/(1 + \mathfrak{p}_L^m)$ . If  $L', L'' \subset E$  then  $L'L'' \subset E$  and  $N(L'L''/L) \subset N(L'/L) \cap N(L''/L)$ , hence the intersection  $(N(E/L) \cap P)/(1 + \mathfrak{p}_L^m)$  of all  $(N(L'/L) \cap P)/(1 + \mathfrak{p}_L^m)$  is non-empty.  $\square$

## 5.2. Base change and LCFT for Lubin-Tate extensions.

**Theorem 5.9.** (Base change) For a finite extension  $K'/K$ , we have  $K'^{\text{LT}} \subset K'^{\text{LT}}$  and the following commutes, i.e. for all  $x' \in K'^{\times}$  we have  $\text{Art}_{K'}(x')|_{K^{\text{LT}}} = \text{Art}_K(N_{K'/K}(x'))$ .

$$\begin{array}{ccc} K'^{\times} & \xrightarrow{\text{Art}_{K'}} & \text{Gal}(K'^{\text{LT}}/K') \\ \downarrow N_{K'/K} & & \downarrow \text{res} \\ K^{\times} & \xrightarrow{\text{Art}_K} & \text{Gal}(K^{\text{LT}}/K) \end{array}$$

<sup>8</sup>The other inclusion is seen as follows.  $x \in N(K_x^m/K)$  and  $K_x^m$  is the fixed field of  $\text{Art}_K((1 + \mathfrak{p}^m) \times \langle x \rangle)$ . Hence if  $x'/x \in 1 + \mathfrak{p}^m$  then  $K_x^m = K_{x'}^m$ , therefore  $x' \in N(K_x^m/K)$ . Thus  $1 + \mathfrak{p}^m \subset N(K_x^m/K)$ .

*Proof.* Take a uniformizer  $x'$  of  $K'$ , and extend  $\text{Art}_{K'}(x') \in \text{Gal}(K'^{\text{LT}}/K')$  to  $\sigma \in \text{Gal}(\overline{K}/K')$ . Then  $\sigma|_{K'^{\text{ur}}} = \text{Frob}_{K'}$  and  $\sigma|_{K'^{\text{ram}}} = \text{id}$ , hence the fixed field  $E_\sigma \subset \overline{K}$  of  $\sigma$  contains  $K'^{\text{ram}}$ , and  $E_\sigma \cap K'^{\text{ur}} = K'$ . Hence  $N(E_\sigma/K') = \langle x' \rangle$  by Corollary 5.8 and  $N(E_\sigma/K) = \langle N_{K'/K}(x') \rangle$ . Now if  $L := K' \cap K^{\text{ur}}$ , then  $\sigma|_{K^{\text{ur}}} = \text{Frob}_{K'}|_{K^{\text{ur}}} = \text{Frob}_K^{[L:K]}$ . For  $x := \text{Art}_K^{-1}(\sigma|_{K^{\text{LT}}})$ , we have  $\sigma|_{K_x^{\text{ram}}} = \text{Art}_K(x)|_{K_x^{\text{ram}}} = \text{id}$  by Corollary 4.10, i.e.  $K_x^{\text{ram}} \subset E_\sigma$ . As  $E_\sigma \cap K^{\text{ur}} = K' \cap K^{\text{ur}} = L$ , we have  $N(E_\sigma/K) = \langle x \rangle$  by Corollary 5.8, hence  $x = N_{K'/K}(x')$  as  $v_K(x) = [L : K] = v_K(N_{K'/K}(x'))$ . As the intersection of  $E_\sigma$  for all extensions  $\sigma$  of  $\text{Art}_{K'}(x')$  is  $K_x^{\text{ram}}$ , we see  $K_x^{\text{ram}} \subset K_x'^{\text{ram}}$ . This and  $K'^{\text{ur}} = K'K^{\text{ur}}$  shows  $K'^{\text{LT}} \subset K^{\text{LT}}$ , and we showed  $\text{Art}_{K'}(x')|_{K^{\text{LT}}} = \sigma|_{K^{\text{LT}}} = \text{Art}_K(x)$ . As the uniformizers generate  $K'^{\times}$ , this completes the proof.  $\square$

We call a finite extension  $K'/K$  a *Lubin-Tate extension* if it is contained in  $K'^{\text{LT}}$ .

**Corollary 5.10.** (LCFT minus Local Kronecker-Weber)<sup>9</sup>

- (i) *There is a unique homomorphism  $\text{Art}_K : K^\times \rightarrow \text{Gal}(K^{\text{LT}}/K)$  satisfying the following properties:*
  - (a) *If  $\pi$  is a uniformizer of  $K$ , then  $\text{Art}_K(\pi)|_{K^{\text{ur}}} = \text{Frob}_K$ .*
  - (b) *If  $K'/K$  is a Lubin-Tate extension, then  $\text{Art}_K(N(K'/K))|_{K'} = \text{id}$ .**Moreover,  $\text{Art}_K$  is an isomorphism onto  $W(K^{\text{LT}}/K) \subset \text{Gal}(K^{\text{LT}}/K)$ .*
- (ii) *If  $K'/K$  is a finite extension, then  $\text{Art}_{K'}(x)|_{K^{\text{LT}}} = \text{Art}_K(N_{K'/K}(x))$  for all  $x \in K'^{\times}$ , and  $\text{Art}_K$  induces an isomorphism  $K^\times/N(K'/K) \xrightarrow{\cong} \text{Gal}((K' \cap K^{\text{LT}})/K)$ .*

*Proof.* (i):  $\text{Art}_K$  satisfies (a) by definition, and (b) by Theorem 5.9. Conversely, if  $\text{Art}'_K$  satisfies these, then for any uniformizer  $\pi$  of  $K$ , (b) and Proposition 3.5(ii) imply that  $\text{Art}'_K(\pi)|_{K_x^{\text{ram}}} = \text{id}$ . This and (a) show that  $\text{Art}'_K(\pi) = \text{Art}_K(\pi)$  by Corollary 4.10. As  $K^\times$  is generated by the uniformizers, we get  $\text{Art}'_K = \text{Art}_K$ . The last assertion is Corollary 4.10.

(ii): The first part follows from Theorem 5.9, and in view of Corollary 4.10,  $\text{Art}_K$  induces  $K^\times/N(K'/K) \cong W(K^{\text{LT}}/K)/\text{Im}(W(K'^{\text{LT}}/K'))$ . This is isomorphic to  $\text{Gal}((K' \cap K^{\text{LT}})/K)$ , because  $W(K^{\text{LT}}/K)$  surjects onto  $\text{Gal}((K' \cap K^{\text{LT}})/K)$  and  $W(K'^{\text{LT}}/K')$  is the inverse image of  $W(K^{\text{LT}}/K)$  under  $\text{Gal}(K'^{\text{LT}}/K') \rightarrow \text{Gal}(K^{\text{LT}}/K)$ .  $\square$

<sup>9</sup>The classical theorems of LCFT for Lubin-Tate extensions (instead of abelian extensions) follow easily.

- (i) If  $K'/K$  is a Lubin-Tate extension, then  $K^\times/N(K'/K) \xrightarrow{\cong} \text{Gal}(K'/K)$ .
- (ii) For any finite  $K'/K$ , we have  $N(K'/K) = N((K' \cap K^{\text{LT}})/K)$  and  $[K^\times : N(K'/K)] \leq [K' : K]$ . Equality holds if and only if  $K'/K$  is Lubin-Tate.
- (iii) If  $K'/K$  is finite and  $K''/K$  is Lubin-Tate, then  $N(K'/K) \subset N(K''/K) \iff K'' \subset K'$ . If  $K'/K$  is also Lubin-Tate, then  $N(K''/K)/N(K'/K) \xrightarrow{\cong} \text{Gal}(K'/K'')$  by  $\text{Art}_{K'}$ .
- (iv) If  $K', K''/K$  are Lubin-Tate extensions, then:  
 $N(K'K''/K) = N(K'/K) \cap N(K''/K)$ ,  $N((K' \cap K'')/K) = N(K'/K)N(K''/K)$ .
- (v) (*Existence theorem*) For any finite index closed subgroup  $H \subset K^\times$ , there is a unique Lubin-Tate extension  $K'/K$  such that  $N(K'/K) = H$ .

<sup>10</sup>This proof shows that we only need totally ramified Lubin-Tate extensions for the characterization.

## 6. THE LOCAL KRONECKER-WEBER THEOREM

We finish the proof of Theorem A by proving the local Kronecker-Weber theorem, i.e.  $K^{\text{LT}} = K^{\text{ab}}$ . This follows easily from the Hasse-Arf theorem (Gold [3] or Iwasawa [4], §7.4; see also Lubin [5], Rosen [7]). We first prove the Hasse-Arf theorem following Sen [8].

**6.1. Ramification groups.** Let  $K'/K$  be a finite totally ramified Galois extension of local fields, and set  $G := \text{Gal}(K'/K)$ . For a uniformizer  $\pi$  of  $K'$ , we have  $\mathcal{O}_{K'} = \mathcal{O}_K[\pi]$  by Lemma 5.7. We write  $v := v_{K'}$  and  $q = |\mathcal{O}_K/\mathfrak{p}| = |\mathcal{O}_{K'}/\mathfrak{p}_{K'}|$ .

**Definition 6.1.** Let  $i(\sigma) := v(\sigma(\pi) - \pi)$ , where we set  $i(\text{id}) = \infty$ . For  $n \geq 0$ , define  $G_n := \{\sigma \in G \mid i(\sigma) > n\} = \{\sigma \in G \mid \sigma(\pi)/\pi \in 1 + \mathfrak{p}_{K'}^n\}$ . Then  $G = G_0$  as  $K'/K$  is totally ramified, and  $G_n = \{\text{id}\}$  for sufficiently large  $n$ . They are normal subgroups of  $G$ , independent of the choice of  $\pi$ , because  $G_n = \{\sigma \in G \mid v(\sigma(a) - a) > n \text{ for all } a \in \mathcal{O}_{K'}\}$  which is the kernel of the group homomorphism:

$$G \ni \sigma \longmapsto \sigma|_{\mathcal{O}_{K'}} \bmod \mathfrak{p}_{K'}^{n+1} \in \text{Aut}(\mathcal{O}_{K'}/\mathfrak{p}_{K'}^{n+1}).$$

**Proposition 6.2.** For  $n \in \mathbb{Z}_{\geq 0}$ , we have following injective group homomorphisms<sup>11</sup>, independent of the choice of  $\pi$ :

$$\begin{aligned} \theta_0 : G_0/G_1 \ni \sigma &\longmapsto \sigma(\pi)/\pi \bmod \mathfrak{p}_{K'} \in \mathcal{O}_{K'}^\times/(1 + \mathfrak{p}_{K'}) = (\mathcal{O}_{K'}/\mathfrak{p}_{K'})^\times \cong \mathbb{F}_q^\times, \\ \theta_n : G_n/G_{n+1} \ni \sigma &\longmapsto (\sigma(\pi)/\pi) - 1 \bmod \mathfrak{p}_{K'}^{n+1} \in \mathfrak{p}_{K'}^n/\mathfrak{p}_{K'}^{n+1} \cong \mathbb{F}_q \quad (n \geq 1) \end{aligned}$$

*Proof.* The maps are well-defined and injective by definition of  $G_n$ . For a different uniformizer  $\pi' = u\pi$  with  $u \in \mathcal{O}_{K'}^\times$ , we have  $\sigma(\pi')/\pi' = (\sigma(\pi)/\pi) \cdot (\sigma(u)/u)$ , and if  $\sigma \in G_n$  then  $\sigma(u) \equiv u \pmod{\mathfrak{p}_{K'}^{n+1}}$ , hence  $\sigma(u)/u \in 1 + \mathfrak{p}_{K'}^{n+1}$ , hence the maps  $\theta_n$  do not depend on the choice of  $\pi$ . For  $\sigma, \tau \in G_n$ , if  $u = \tau(\pi)/\pi$ , then  $\sigma\tau(\pi)/\pi = (\sigma(\pi)/\pi) \cdot (\tau(\pi)/\pi) \cdot (\sigma(u)/u)$ , and as  $u \in \mathcal{O}_{K'}^\times$ , we have  $\sigma(u)/u \in 1 + \mathfrak{p}_{K'}^{n+1}$ , therefore  $\theta_n$  are group homomorphisms.  $\square$

**Corollary 6.3.** If  $G$  is abelian and  $G_n \neq G_{n+1}$ , then  $e_0 := |G_0/G_1|$  divides  $n$ .

*Proof.* Let  $\tau \in G_n$  and  $\sigma \in G$ . We compute  $\theta_n(\sigma\tau\sigma^{-1})$  using  $\pi' = \sigma^{-1}(\pi)$ . If  $\tau(\pi') = \pi'(1+a)$  for  $a \in \mathfrak{p}_{K'}^n$ , then  $\theta_n(\tau) = a \bmod \mathfrak{p}_{K'}^{n+1}$  by definition. Then  $\sigma\tau\sigma^{-1}(\pi) = \sigma\tau(\pi') = \sigma(\pi'(1+a)) = \pi(1 + \sigma(a))$ , hence  $\theta_n(\sigma\tau\sigma^{-1}) = \sigma(a) \bmod \mathfrak{p}_{K'}^{n+1}$ . If we write  $a = b\pi^n$  for  $b \in \mathcal{O}_{K'}$  and  $\sigma(\pi) = u\pi$  for  $u \in \mathcal{O}_{K'}^\times$ , then  $\sigma(a) = \sigma(b)\sigma(\pi)^n = \sigma(b)u^n\pi^n$ , and as  $\sigma(b) \equiv b \bmod \mathfrak{p}_{K'}$ , we have  $\sigma(a) \equiv bu^n\pi^n = u^n a \pmod{\mathfrak{p}_{K'}^{n+1}}$ . Therefore  $\theta_n(\sigma\tau\sigma^{-1}) = u^n a \bmod \mathfrak{p}_{K'}^{n+1}$ .

If  $G$  is abelian, then  $\sigma\tau\sigma^{-1} = \tau$ , hence  $a \equiv u^n a \bmod \mathfrak{p}_{K'}^{n+1}$ . If  $G_n \neq G_{n+1}$ , we can choose  $\tau \in G_n$  with  $\theta_n(\tau) \neq 0$ , i.e.  $a \in \mathfrak{p}_{K'}^n \setminus \mathfrak{p}_{K'}^{n+1}$ . Also, choose  $\sigma \in G$  which generates  $G_0/G_1$ , i.e.  $\theta_0(\sigma) = u \bmod \mathfrak{p}$  has order  $e_0$  in  $(\mathcal{O}_{K'}/\mathfrak{p}_{K'})^\times$ . Then  $a \equiv u^n a \pmod{\mathfrak{p}_{K'}^{n+1}}$  implies  $e_0 \mid n$ .  $\square$

**Lemma 6.4.** For  $\sigma \in G_1$ , we have  $v(\sum_{i=0}^{p-1} \sigma^i(\alpha)) > v(\alpha)$  for all  $\alpha \in K'$ .

<sup>11</sup>Therefore  $G$  is supersolvable, i.e.  $G \triangleright G_i$  and  $G_{i-1}/G_i$  cyclic for all  $i$ , with  $G_n = \{\text{id}\}$  for large  $n$ .

*Proof.* Let  $(\sigma-1)(\alpha) := \sigma(\alpha) - \alpha$ . Then  $v((\sigma-1)(\alpha)) > v(\alpha)$  as  $\sigma \in G_1$  implies  $v((\sigma(\alpha)/\alpha) - 1) > 0$ . The claim follows from<sup>12</sup>  $\sum_{i=0}^{p-1} \sigma^i(x) \equiv (\sigma-1)^{p-1}(x) \pmod{px}$ .  $\square$

**Proposition 6.5** (Sen [8]). *Let  $\sigma \in G_1$ . We have  $\langle \sigma \rangle \cong \mathbb{Z}/p^m\mathbb{Z}$  for  $m \geq 1$  by Proposition 6.2. Let  $H_n := G_n \cap \langle \sigma \rangle$  for  $n \geq 1$  and  $i_j := i(\sigma^{p^j})$  for  $j \geq 0$  ( $i_j = \infty$  for  $j \geq m$ ). Then:*

- (i)  $i_{j-1} < i_j$  if  $j \leq m$ . Also,  $H_n = \langle \sigma^{p^j} \rangle$  if and only if  $i_{j-1} \leq n < i_j$ .
- (ii)  $i(\sigma^a) = i_{v_p(a)}$  for  $a \geq 1$ , where  $v_p := v_{\mathbb{Q}_p}$ .
- (iii)  $i_{j-1} \equiv i_j \pmod{p^j}$ , where  $\infty$  is understood to be congruent to any integer.

*Proof.* (i):  $i_{j-1} < i_j$  is seen by applying Lemma 6.4 to  $\alpha = \sigma^{p^{j-1}}(\pi) - \pi$ . We have  $\langle \sigma^{p^j} \rangle \subset H_n$  if and only if  $\sigma^{p^j} \in H_n$ , i.e.  $i_j > n$ . As all subgroups of  $\langle \sigma \rangle$  are of the form  $\langle \sigma^{p^j} \rangle$ , we have  $\langle \sigma^{p^j} \rangle \supset H_n \Leftrightarrow \langle \sigma^{p^{j-1}} \rangle \not\subset H_n \Leftrightarrow i_{j-1} \leq n$ . (ii): This is  $\infty = \infty$  if  $p^m \mid a$ . If  $j := v_p(a) < m$ , then  $H_{i_{j-1}} = \langle \sigma^{p^j} \rangle$  and  $H_{i_j} = \langle \sigma^{p^{j+1}} \rangle$  by (i), therefore  $\sigma^a \in H_{i_{j-1}} \setminus H_{i_j}$ , i.e.  $i(\sigma^a) = i_j$ . (iii): We can assume  $i_j < \infty$ , and use induction on  $j$ . The assertion is empty when  $j = 0$ . We first show that the inductive hypothesis implies that  $i_{j-1}$  and  $n + i(\sigma^n)$  for  $n \in \mathbb{Z}$ ,  $v_p(n) < j$  are all distinct from each other. First,  $v_p(n) \leq j-1$  implies  $i(\sigma^n) = i_{v_p(n)} \equiv i_{j-1} \pmod{p^{v_p(n)+1}}$  by inductive hypothesis, i.e.  $v_p(i_{j-1} - i(\sigma^n)) > v_p(n)$ , hence  $i_{j-1} \neq n + i(\sigma^n)$ . Second, assume  $n + i(\sigma^n) = n' + i(\sigma^{n'})$ . If  $v_p(n) \neq v_p(n')$ , then  $v_p(n - n') = \min\{v_p(n), v_p(n')\}$ , and by inductive hypothesis  $v_p(i(\sigma^n) - i(\sigma^{n'})) > \min\{v_p(n), v_p(n')\}$ , which is impossible. Hence  $v_p(n) = v_p(n')$ , therefore  $i(\sigma^n) = i(\sigma^{n'})$  and  $n = n'$ . Thus we proved the claim. Now, applying the inductive hypothesis to  $\sigma^p \in G_1$ , we have  $i_{j-1} \equiv i_j \pmod{p^{j-1}}$ . Let  $s := i_{j-1} - i_j$  and assume  $v_p(s) = j-1$ . We will show that this leads to contradiction.

**Lemma 6.6.** *Let  $\sigma \in G_1$ . For each  $n \in \mathbb{Z}$ , there exists  $\alpha \in K'$  such that  $v(\alpha) = n$  and  $v(\sigma(\alpha) - \alpha) = n + i(\sigma^n)$ . Moreover, any  $x \in K'$  can be written as a sum  $x = \sum_{n=v(x)}^{\infty} x_n$  (see §7) where each  $x_n$  satisfies above two properties for  $n$  if  $x_n \neq 0$ .*

*Proof.* For the first part, if  $n \geq 0$ , then let  $\alpha = \prod_{i=0}^{n-1} \sigma^i(\pi)$  for a uniformizer  $\pi$  of  $K'$  (set  $\alpha = 1$  for  $n = 0$ ). Then clearly  $v(\alpha) = n$ , and  $\sigma(\alpha)/\alpha = \sigma^n(\pi)/\pi$ , thus  $v(\sigma(\alpha) - \alpha) = v(\alpha) + v((\sigma(\alpha)/\alpha) - 1) = n + i(\sigma^n)$ . Also,  $\alpha^{-1}$  satisfies the properties for  $-n$ . For the second part, note that  $C := \mu_{q-1} \cup \{0\}$  is a complete set of representatives for  $\mathcal{O}_{K'} \pmod{\mathfrak{p}_{K'}}$ , and  $\sigma$  acts trivially on  $C$  as  $C \subset K$ . Hence we can write  $x = \sum_{n=v(x)}^{\infty} c_n \alpha_n$  where  $c_n \in C$  and  $\alpha_n$  is the  $\alpha$  we constructed above. Thus  $x_n := c_n \alpha_n$  has the required properties if  $c_n \neq 0$ .  $\square$

Applying the first part of the lemma to  $\sigma^p$ , there is  $x \in K'$  with  $v(x) = s$  and  $v(\sigma^p(x) - x) = s + i((\sigma^p)^s) = s + i_j = i_{j-1}$ . Letting  $y := \sum_{i=0}^{p-1} \sigma^i(x)$ , we have  $v(y) > v(x) = s$  by Lemma 6.4 and  $v(\sigma(y) - y) = v(\sigma^p(x) - x) = i_{j-1}$ . Now expand  $y = \sum_{n=v(y)}^{\infty} y_n$  as in the lemma:  $v(\sigma(y_n) - y_n) = n + i(\sigma^n)$  if  $y_n \neq 0$ . Let  $z := \sigma(y) - y$ . Then  $v(z) = i_{j-1}$  and  $z = \sum_{n=v(y)}^{\infty} z_n$ , where  $z_n := \sigma(y_n) - y_n$ , hence  $v(z_n) = n + i(\sigma^n)$  whenever  $z_n \neq 0$ . Our previous observation shows  $v(z - \sum_{v_p(n) < j} z_n) \leq i_{j-1}$ . If  $v_p(n) \geq j$  and  $z_n \neq 0$ ,

<sup>12</sup>For any  $\mathbb{F}_p$ -algebra  $A$ , the equality  $\sum_{i=0}^{p-1} X^i = (X^p - 1)/(X - 1) = (X - 1)^{p-1}$  holds in  $A[X]$ .

then  $v(z_n) = n + i(\sigma^n) \geq n + i_j \geq v(y) + i_j > i_{j-1}$ , hence  $v(\sum_{v_p(n) \geq j} z_n) > i_{j-1}$ , a contradiction.  $\square$

**Corollary 6.7.** *Assume  $G \cong \mathbb{Z}/p^m\mathbb{Z}$ . Then there exist  $n_0, n_1, \dots, n_{m-1} \in \mathbb{Z}_{\geq 1}$  such that, for  $1 \leq j \leq m-1$ , we have  $|G_n| = p^{m-j}$  if and only if  $\sum_{i=0}^{j-1} n_i p^i < n \leq \sum_{i=0}^j n_i p^i$ .*

**6.2. The Hasse-Arf theorem.** Let  $G = \text{Gal}(K'/K)$  with  $K'/K$  totally ramified as before, and let  $G \triangleright H$  with  $G/H = \text{Gal}(K''/K)$ . For  $\sigma \in G$ , let  $\bar{\sigma} = \sigma H \in G/H$  be its image.

**Lemma 6.8.** *For all  $\sigma \in G$ , we have  $i(\bar{\sigma}) = \frac{1}{|H|} \sum_{\tau \in H} i(\sigma\tau)$ .*

*Proof.* For  $\sigma = \text{id}$ , we understand the equality as  $\infty = \infty$ . Let  $\sigma \neq \text{id}$ , and take uniformizers  $\pi$  and  $\pi'$  of  $K'$  and  $K''$  respectively, so that  $\mathcal{O}_{K'} = \mathcal{O}_K[\pi]$  and  $\mathcal{O}_{K''} = \mathcal{O}_K[\pi']$  by Lemma 5.7. As  $i(\bar{\sigma}) = v_{K''}(\bar{\sigma}(\pi') - \pi') = \frac{1}{|H|} \cdot v_{K'}(\bar{\sigma}(\pi') - \pi')$ , if we let  $a = \bar{\sigma}(\pi') - \pi'$  and  $b = \prod_{\tau \in H} (\sigma\tau(\pi) - \pi)$ , it suffices to show  $v_{K'}(a) = v_{K'}(b)$ . Let the minimal polynomial of  $\pi$  over  $\mathcal{O}_{K''}$  be  $f = \prod_{\tau \in H} (X - \tau(\pi)) \in \mathcal{O}_{K''}[X]$ . Applying  $\sigma$ , we get  $f^{\bar{\sigma}} = \prod_{\tau \in H} (X - \sigma\tau(\pi))$ , where  $f^{\bar{\sigma}} \in \mathcal{O}_{K''}[X]$  is obtained by applying  $\bar{\sigma}$  to the coefficients of  $f$ . Hence  $f^{\bar{\sigma}}(\pi) = \prod_{\tau \in H} (\pi - \sigma\tau(\pi)) = \pm b$ . First we prove  $a \mid b$ . As  $\mathcal{O}_{K''} = \mathcal{O}_K[\pi']$ , we have  $a \mid \bar{\sigma}(x) - x$  for any  $x \in \mathcal{O}_{K''}$ , hence  $a \mid f^{\bar{\sigma}} - f$ , therefore  $a \mid f^{\bar{\sigma}}(\pi) - f(\pi) = \pm b$ . Now we prove  $b \mid a$ . Write  $\pi' = g(\pi)$  for  $g \in \mathcal{O}_K[X]$ . The polynomial  $g(X) - \pi' \in \mathcal{O}_{K''}[X]$  has  $\pi$  as a root, hence divisible by  $f$  in  $\mathcal{O}_{K''}[X]$ . Applying  $\bar{\sigma}$ , we have  $f^{\bar{\sigma}} \mid g(X) - \bar{\sigma}(\pi')$  in  $\mathcal{O}_{K''}[X]$ , hence  $g(\pi) - \bar{\sigma}(\pi') = -a$  is divisible by  $f^{\bar{\sigma}}(\pi) = \pm b$ .  $\square$

**Proposition 6.9** (Herbrand). *Define  $\phi_H(n) = -1 + \frac{1}{|H|} \sum_{\tau \in H} \min\{i(\tau), n+1\}$  for  $n \in \mathbb{R}_{\geq 0}$ . Also, for  $n \in \mathbb{R}_{\geq 0}$ , define  $G_n := \{\sigma \in G \mid i(\sigma) \geq n+1\}$ , i.e.  $G_n = G_i$  if  $i \in \mathbb{Z}_{\geq 0}$  and  $n \in (i-1, i]$ . Then  $G_n H/H = (G/H)_{\phi_H(n)}$  for all  $n \in \mathbb{R}_{\geq 0}$ .*

*Proof.* For  $\bar{\sigma} \in G/H$ , replace  $\sigma$  by the element in  $\sigma H$  which has the maximal value of  $i$ , and let  $i(\sigma) = m$ . Let  $\tau \in H$ . If  $i(\tau) \geq m$ , then  $i(\sigma\tau) \geq m$ . If  $i(\tau) < m$ , then  $i(\tau) \geq \min\{i(\sigma\tau), i(\sigma^{-1})\}$ , hence  $i(\sigma\tau) = i(\tau)$ . Therefore  $i(\sigma\tau) = \min\{i(\tau), m\}$ . Now the Lemma 6.8 gives  $i(\bar{\sigma}) = \phi_H(m-1) + 1$ . Therefore, as  $\phi_H$  is increasing, for  $n \in \mathbb{R}_{\geq 0}$  we have  $\bar{\sigma} \in G_n H/H \iff m \geq n+1 \iff i(\bar{\sigma}) \geq \phi_H(n) + 1 \iff \bar{\sigma} \in (G/H)_{\phi_H(n)}$ .  $\square$

**Lemma 6.10.** *Let  $\phi_G(n) := -1 + \frac{1}{|G|} \sum_{\tau \in G} \min\{i(\tau), n+1\}$  for  $n \in \mathbb{R}_{\geq 0}$ . Then:*

- (i)  $\phi_G(0) = 0$ ,  $\phi_G(n) = \frac{1}{|G|} \sum_{i=1}^n |G_i|$  for  $n \in \mathbb{Z}_{\geq 1}$ .
- (ii)  $\phi_G = \phi_{G/H} \circ \phi_H$  on  $\mathbb{R}_{\geq 0}$ .

*Proof.* (i):  $\sum_{\tau \in G} \min\{i(\tau), n+1\} = \sum_{i=0}^{n-1} \left( \sum_{\tau \in G_i \setminus G_{i+1}} (i+1) \right) + \sum_{\tau \in G_n} (n+1) = \sum_{i=0}^n |G_i|$ .

(ii): As  $\phi(0) = 0$  and  $\phi$  is continuous and piecewise linear, we only need to compare the derivatives of both sides at  $n \in (i-1, i)$  for  $i \in \mathbb{Z}_{>0}$ . For LHS it is  $|G_n|/|G|$ , and for RHS it is  $(|(G/H)_{\phi_H(n)}|/|G/H|) \cdot (|H_n|/|H|) = |G_n H/H| |H_n|/|G| = |G_n|/|G|$  by Proposition 6.9 and  $G_n/H_n = G_n/(H \cap G_n) \cong G_n H/H$ .  $\square$

**Theorem 6.11** (Hasse-Arf). *If  $G$  is abelian,  $n \in \mathbb{Z}_{\geq 0}$  and  $G_n \neq G_{n+1}$ , then  $\phi_G(n) \in \mathbb{Z}_{\geq 0}$ .*

*Proof.* First assume  $G = G_1$ . Then  $G \cong \bigoplus_{i=1}^j \mathbb{Z}/p^{m_i}\mathbb{Z}$  by Proposition 6.2, and we proceed by induction on  $j$ . When  $j = 1$ , i.e.  $G \cong \mathbb{Z}/p^m\mathbb{Z}$ , if  $G_n \neq G_{n+1}$  then  $n = \sum_{i=0}^j n_i p^i$  for some  $0 \leq j \leq m-1$  by Corollary 6.7, in which case  $\phi_G(n) = \frac{1}{p^m}(n_0 \cdot p^m + n_1 p \cdot p^{m-1} + \cdots + n_j p^j \cdot p^{m-j}) \in \mathbb{Z}_{\geq 0}$  by Lemma 6.10(i). For  $j > 1$ , if  $G_n \neq G_{n+1}$  we can find  $H$  with  $G/H \cong \mathbb{Z}/p^{m_i}\mathbb{Z}$ , and  $G_n H/H \neq G_{n+1} H/H$ . We have  $\phi_H(n) \in \mathbb{Z}_{\geq 0}$  by inductive hypothesis, and  $(G/H)_{\phi_H(n)} \neq (G/H)_{\phi_H(n+1)} = (G/H)_{\phi_H(n)+1}$  by Proposition 6.9. As  $G/H$  is cyclic, we see  $\phi_{G/H}(\phi_H(n)) \in \mathbb{Z}_{\geq 0}$ , which is  $\phi_G(n)$  by Lemma 6.10(ii).

When  $G \neq G_1$ , set  $H = G_1$  and  $|G/H| = e_0$ . As  $\phi_{G/H}(n) = n/e_0$  for  $n \in \mathbb{R}_{\geq 0}$  by definition, by Lemma 6.10(ii) it suffices to show  $e_0 \mid \phi_H(n)$  when  $n \in \mathbb{Z}_{\geq 0}$  and  $G_n \neq G_{n+1}$  (we know  $\phi_H(n) \in \mathbb{Z}_{\geq 0}$ ). If  $n = 0$  then  $\phi_H(0) = 0$ . Let  $n > 0$ . For any  $i \in \mathbb{Z}_{\geq 1}$  (where  $H_i = G_i$ ) with  $H_i \neq H_{i+1}$ , we have  $e_0 \mid i$  by Corollary 6.3, hence  $e_0 \mid \sum_{i=1}^n |H_i|$ . As  $e_0$  and  $|H|$  are coprime, we have  $e_0 \mid \phi_H(n)$  by Lemma 6.10(i).  $\square$

**Definition 6.12.** For  $m \in \mathbb{R}_{\geq 0}$ , set  $G^m := G_{\phi_G^{-1}(m)}$ .

**Corollary 6.13.** (i) *If  $G \triangleright H$ , then  $G^m H/H = (G/H)^m$  for all  $m \in \mathbb{R}_{\geq 0}$ .*

(ii) *Let  $K'/K$  and  $K''/K$  be two Galois extensions with  $K'K''/K$  totally ramified. If  $\text{Gal}(K'/K)^m = \text{Gal}(K''/K)^m = \{\text{id}\}$  for  $m \in \mathbb{R}_{\geq 0}$ , then  $\text{Gal}(K'K''/K)^m = \{\text{id}\}$ .*

(iii) *Let  $G$  be abelian. Then  $|G/G^m|$  divides  $(q-1)q^{m-1}$  for  $m \in \mathbb{Z}_{\geq 0}$ .*

*Proof.* (i): By Proposition 6.9 and Lemma 6.10(ii), we compute  $G^m H/H = G_{\phi_G^{-1}(m)} H/H = (G/H)_{\phi_H(\phi_G^{-1}(m))} = (G/H)_{\phi_{G/H}^{-1}(m)} = (G/H)^m$ . (ii): If  $G = \text{Gal}(K'K''/K)$  and  $G/H = \text{Gal}(K''/K)$ , then  $G^m H/H = (G/H)^m = \{\text{id}\}$  shows  $G^m \subset H = \text{Gal}(K'K''/K'')$ . Similarly  $G^m \subset \text{Gal}(K'K''/K')$ , hence  $G^m = \{\text{id}\}$ . (iii): If  $n-1 < \phi^{-1}(m) \leq n$  for  $n \in \mathbb{Z}_{\geq 0}$ , then  $G^m = G_n$ . Consider  $G_i$  for integers  $1 \leq i \leq n$ . Then, by Theorem 6.11,  $G_{i-1} \neq G_i$  can only happen when  $\phi(i-1) \in \mathbb{Z}$ , and as  $0 \leq \phi(i-1) \leq \phi(n-1) < m$ , at most  $m-1$  times for  $i > 1$ . By Proposition 6.2,  $|G_{i-1}/G_i|$  divides  $q-1$  when  $i = 1$  and  $q$  when  $i > 1$ .  $\square$

### 6.3. The Local Kronecker-Weber theorem.

**Proposition 6.14.** *Let  $\pi$  be a uniformizer of  $K$  and  $m \geq 1$ . Then  $\text{Gal}(K_\pi^m/K)^m = \{\text{id}\}$ .*

*Proof.* Let  $K_\pi^m = K(\boldsymbol{\mu}_{f,m})$  and  $\alpha \in \boldsymbol{\mu}_{f,m} \setminus \boldsymbol{\mu}_{f,m-1}$ . For  $\sigma \in \text{Gal}(K_\pi^m/K) \setminus \{\text{id}\}$ , we have  $i(\sigma) = v(\sigma(\alpha) - \alpha)$  by Proposition 3.5(ii), where  $v = v_{K_\pi^m}$ . If  $\rho_{f,m}(\sigma) = u \bmod \mathfrak{p}^m \in (\mathcal{O}_K^\times/\mathfrak{p}^m)^\times$  (see Proposition 3.5(iii)), then  $\sigma(\alpha) = [u]_f(\alpha)$ . For  $\sigma \neq \text{id}$ , set  $\beta := [u-1]_f(\alpha)$ . If  $v_K(u-1) = i$  for  $0 \leq i < m$ , then  $\beta \in \boldsymbol{\mu}_{f,m-i} \setminus \boldsymbol{\mu}_{f,m-i-1}$  is a uniformizer of  $K_\pi^{m-i}$  by Proposition 3.5(ii), hence  $v(\beta) = q^i$ . As  $[u]_f(\alpha) = \alpha +_f \beta \equiv \alpha + \beta \pmod{\alpha\beta}$ , we have  $[u]_f(\alpha) - \alpha \equiv \beta \pmod{\alpha\beta}$ , hence  $i(\sigma) = v(\beta) = q^i$ . Thus for  $G = \text{Gal}(K_\pi^m/K)$  and  $1 \leq i \leq m$ , we have  $|G_n| = |\rho_{f,m}^{-1}(1 + \mathfrak{p}^i)| = q^{m-i}$  for  $q^{i-1} - 1 < n \leq q^i - 1$ . Thus  $\phi(q^m - 1) = \frac{1}{|G|} \sum_{i=1}^{q^m-1} |G_i| = \frac{1}{(q-1)q^{m-1}} (\sum_{i=1}^m (q^i - q^{i-1}) \cdot q^{m-i}) = m$  and  $G^m = G_{q^m-1} = \{\text{id}\}$ .  $\square$

**Theorem 6.15.** (Local Kronecker-Weber theorem) *Every finite abelian extension of a local field  $K$  is a Lubin-Tate extension, i.e.  $K^{\text{LT}} = K^{\text{ab}}$ .*

*Proof.* Extend  $\text{Frob}_K \in \text{Gal}(K^{\text{LT}}/K)$  arbitrarily to  $\sigma \in \text{Gal}(K^{\text{ab}}/K)$ , and let  $E$  be a fixed field of  $\sigma$ . Then  $E/K$  is totally ramified as  $E \cap K^{\text{ur}} = K$ . We will show  $K^{\text{ab}} = EK^{\text{ur}}$ . As  $\text{Gal}(K^{\text{ab}}/E) \cong \widehat{\mathbb{Z}}$  with  $\sigma \mapsto 1$ , the extension  $K^{\text{ab}}/E$  has a unique intermediate extension of degree  $n$  for each  $n \geq 1$ , but  $EK_n/E$ , where  $K_n/K$  is finite unramified of degree  $n$ , is such an extension because  $E \cap K^{\text{ur}} = K$ . Thus there is no other finite intermediate field of  $K^{\text{ab}}/E$ , i.e.  $K^{\text{ab}} = EK^{\text{ur}}$ .

Now if we set  $\pi := \text{Art}_K^{-1}(\sigma|_{K^{\text{LT}}})$ , it is a uniformizer of  $K$ , and  $\sigma|_{K^{\text{LT}}}$  fixes  $K_\pi^{\text{ram}}$ , hence  $K_\pi^{\text{ram}} \subset E$ . As  $K^{\text{LT}} = K_\pi^{\text{ram}}K^{\text{ur}}$ , it suffices to show  $E \subset K_\pi^{\text{ram}}$ . Let  $K'/K$  be any finite Galois extension contained in  $E$ . It is totally ramified, and  $\text{Gal}(K'/K)^m = \{\text{id}\}$  for a large  $m$ . Then we have  $\text{Gal}(K'K_\pi^m/K)^m = \{\text{id}\}$  by Proposition 6.14 and Corollary 6.13(ii), hence  $[K'K_\pi^m : K] \mid (q-1)q^{m-1} = [K_\pi^m : K]$  by Corollary 6.13(iii), thus  $K' \subset K_\pi^m$ .  $\square$

## 7. APPENDIX: BASIC FACTS ON DVR

Here we gather some facts on DVR that are used in this article<sup>13</sup>.

A ring  $A$  is called a *discrete valuation ring (DVR)* if it is a local ring (i.e. has a unique maximal ideal) and a PID. Let  $A$  be a DVR and  $P$  its maximal ideal. A generator of  $P$  is called a *uniformizer* of  $A$ . Each uniformizer  $\pi$  gives a following isomorphism of abelian groups:

$$A^\times \times \mathbb{Z} \ni (u, b) \xrightarrow{\cong} u \cdot \pi^b \in K^\times.$$

The second projection (*valuation*)  $v_K : K^\times \rightarrow \mathbb{Z}$  does not depend on  $\pi$ , and  $A = \{x \in K \mid v_K(x) \geq 0\}$  and  $P = \{x \in K \mid v_K(x) > 0\}$ .

The *completion* of  $A$  is defined as  $\widehat{A} := \varprojlim_m A/P^m$ , which is also a DVR with the maximal ideal  $\widehat{P} := P\widehat{A}$ . If  $K = \text{Frac}(A)$ , then  $\widehat{K} := K \otimes_A \widehat{A}$  is the fraction field of  $\widehat{A}$ , which is called the *completion* of  $K$ . The canonical map  $A \rightarrow \widehat{A}$  is always injective (hence  $K \subset \widehat{K}$ ), and if it is an isomorphism we call  $A$  a *complete discrete valuation ring (CDVR)*. A completion of a DVR is a CDVR, and  $A/P^m \xrightarrow{\cong} \widehat{A}/\widehat{P}^m$ . If  $A$  is a DVR, choosing a complete set of representatives  $C$  for  $A \bmod P$  and elements  $x_n \in A$  with  $v(x_n) = n$  for all  $n \geq 0$ , we can write any element of  $\widehat{A} = \varprojlim_m A/P^m$  uniquely as  $\left( \sum_{n=0}^{m-1} c_n x_n \bmod P^m \right)_m$  with  $c_n \in C$ . (Incidentally, this shows that if  $|C| < \infty$  then  $|A/P^m| = |C|^m$ .) We write this element as  $\sum_{n=0}^{\infty} c_n x_n$  (when  $x_n = \pi^n$  for a uniformizer  $\pi$ , this is called a  *$\pi$ -adic expansion*). Choosing  $x_n \in K$  with  $v(x_n) = n$  for all  $n \in \mathbb{Z}$ , any  $x \in \widehat{K}$  can be written as  $y + \sum_{v(x) \leq n < 0} c_n x_n$  for some  $y \in \widehat{A}$ , hence as  $x = \sum_{n=v(x)}^{\infty} c_n x_n$ . Also, if  $A$  is a CDVR, then we can substitute  $x_1, \dots, x_n \in P$  into any power series  $F \in A[[X_1, \dots, X_n]]$  with coefficient in  $A$  to get

<sup>13</sup>For proofs, see e.g. <http://abel.math.harvard.edu/~yoshida/AlgebraicNumberTheory.dvi>.

$F(x_1, \dots, x_n) \in A$ . This is defined using  $A[[X_1, \dots, X_n]] \cong \varprojlim_m (A[X_1, \dots, X_n]/(\deg m))$  and  $A \cong \varprojlim_m A/P^m$ , by taking the limit of:

$$A[X_1, \dots, X_n]/(\deg m) \ni F \bmod \deg m \longmapsto F(x_1, \dots, x_n) \bmod P^m \in A/P^m.$$

Let  $A$  be a DVR,  $K$  its fraction field,  $L$  a separable extension of  $K$  of degree  $n$ , and  $B$  the integral closure of  $A$  in  $L$ , so that  $L \cong B \otimes_A K$  and  $L = \text{Frac}(B)$ . Then  $B$  is a finitely generated  $A$ -module, and as  $A$  is a PID, it is a free  $A$ -module of rank  $n = [L : K]$ . Also,  $B$  is a Dedekind domain (1-dimensional integrally closed noetherian domain). If  $PB = \prod_{i=1}^g Q_i^{e_i}$  is the prime ideal decomposition of the ideal  $PB$  of  $B$  generated by the elements of  $P$ , then  $Q_1, \dots, Q_g$  are all the maximal ideals of  $B$ . Let  $\widehat{B}_i := \varprojlim_m B/Q_i^m$ . As  $B$  is a free  $A$ -module,  $B \otimes_A$  and inverse limits commute, hence the following canonical maps are isomorphisms:

$$B \otimes_A \widehat{A} \cong B \otimes \left( \varprojlim_m A/P^m \right) \cong \varprojlim_m B/(PB)^m \cong \varprojlim_m \prod_{i=1}^g B/Q_i^{e_i m} \cong \prod_{i=1}^g \widehat{B}_i.$$

**Proposition 7.1.** (i) *If  $A$  is a CDVR, then so is  $B$ .*

(ii) *If  $B$  is also a DVR, then the completion  $\widehat{L}$  of  $L$  is isomorphic to  $L \otimes_K \widehat{K}$  (i.e. it is the composite field  $L\widehat{K}$ ), and  $L \cap \widehat{K} = K$  in  $\widehat{L}$ .*

*Proof.* (i):  $B \cong B \otimes_A \widehat{A}$  and  $B$  is a domain, hence  $g = 1$  and  $B \cong \widehat{B}$ .

(ii):  $B \otimes_A \widehat{A} \cong \widehat{B}$  gives  $L \otimes_K \widehat{K} \cong L \otimes_K (K \otimes_A \widehat{A}) \cong L \otimes_B (B \otimes_A \widehat{A}) \cong L \otimes_B \widehat{B} \cong \widehat{L}$ , hence  $[\widehat{L} : \widehat{K}] = [L : K]$ . For the second statement, it suffices to show when  $L/K$  is Galois. Then the restriction  $\text{Gal}(\widehat{L}/\widehat{K}) \rightarrow \text{Gal}(L/(L \cap \widehat{K}))$  is injective, hence  $[\widehat{L} : \widehat{K}] \leq [L : L \cap \widehat{K}] \leq [L : K]$  but it is an equality, therefore  $L \cap \widehat{K} = K$ .  $\square$

Assume  $g = 1$  and  $Q = Q_1$  in the following. As  $Q \cap A = P$ , the field  $k_Q := B/Q$  is an extension of  $k_P := A/P$ , and as  $B$  is a finitely generated  $A$ -module,  $k_Q/k_P$  is finite. The *ramification index*  $e$  and *residue degree*  $f$  are defined by  $PB = Q^e$  and  $f = [k_Q : k_P]$ . As vector spaces over  $k_P$ , we have  $B/PB \cong (k_Q)^e$  (use  $Q$ -adic expansion), and the dimension of RHS is  $ef$ , and the dimension of LHS is the rank of  $B$  as an  $A$ -module, which is  $n$ . Therefore  $n = ef$ . We say  $L/K$  is *unramified* if  $e = 1$  and *totally ramified* when  $f = 1$ .

Assume moreover that  $L/K$  is Galois and  $k_P$  is perfect. An element of  $\text{Gal}(L/K)$  induces an automorphism of  $B$  which maps  $Q$  onto itself, hence we have a group homomorphism:

$$\text{Gal}(L/K) \ni \sigma \longmapsto \sigma|_B \bmod Q \in \text{Aut}(k_Q/k_P).$$

We can show that  $k_Q/k_P$  is Galois and the homomorphism is surjective. As  $|\text{Gal}(k_Q/k_P)| = f$ , the order of the kernel is  $e$ . The following gives an unramified example:

**Proposition 7.2.** *Let  $L = K(\mu_n)$  (and  $g = 1$ ). If  $\text{char } k_P \nmid n$ , then  $L/K$  is unramified.*

*Proof.* We show that the above homomorphism is injective. As any element of  $\text{Gal}(K(\mu_n)/K)$  is determined by the image of a generator  $\zeta \in B^\times$  of  $\mu_n$ , it suffices to show that if  $\zeta^i \equiv \zeta^j \pmod{Q}$  then  $\zeta^i = \zeta^j$ . As  $\zeta^i - \zeta^j \in Q$  implies  $\zeta^{i-j} - 1 \in Q$ , we only need to show  $\zeta^i - 1 \notin Q$  for  $1 \leq i \leq n-1$ . Substituting  $X = 1$  to the identity  $\prod_{i=1}^{n-1} (X - \zeta^i) = (X^n - 1)/(X - 1) = X^{n-1} + X^{n-2} + \cdots + X + 1$ , we get  $\prod_{i=1}^{n-1} (1 - \zeta^i) = n$ , and as  $n \notin Q$  we have  $\prod_{i=1}^{n-1} (1 - \zeta^i) \neq 0$  in the field  $k_Q$ , hence  $\zeta^i - 1 \notin Q$ .  $\square$

*Proof of Lemma 2.1.* ( $\Leftarrow$ ) follows from  $\zeta^i \equiv \zeta^j \pmod{\mathfrak{p}} \implies \zeta^i = \zeta^j$ , which we showed in the proof of Proposition 7.2. We show ( $\Rightarrow$ ). As there is a generator of  $\mu_n$  in  $k = \mathcal{O}_K/\mathfrak{p}$ , take its representative  $\zeta_1 \in \mathcal{O}_K$ . As  $\mathcal{O}_K = \varprojlim_m \mathcal{O}_K/\mathfrak{p}^m$ , it is enough to construct  $\zeta_m \in \mathcal{O}_K$  for each  $m \geq 1$  such that  $\zeta_m^n \equiv 1 \pmod{\mathfrak{p}^m}$  and  $\zeta_{m+1} \equiv \zeta_m \pmod{\mathfrak{p}^m}$ . If we have  $\zeta_m$ , let  $\zeta_m^n \equiv 1 + \alpha\pi^m \pmod{\mathfrak{p}^{m+1}}$ . Setting  $\zeta_{m+1} = \zeta_m + \beta\pi^m$ , we need  $\zeta_{m+1}^n \equiv \zeta_m^n + n\zeta_m^{n-1}\beta\pi^m \equiv 1 + (\alpha + n\zeta_m^{n-1}\beta)\pi^m \pmod{\mathfrak{p}^{m+1}}$ , hence  $\beta = -\alpha/n\zeta_m^{n-1}$  will do.  $\square$

## 8. REMARKS ON THE LITERATURE

The materials of Sections 3, 4 and 5.1 (the “relative” Lubin-Tate groups) are due to de Shalit [2], although proofs are omitted there. Our Sections 3 and 4 follow Iwasawa [4]. This book treats the norm operator  $N$  only for the “classical” Lubin-Tate groups, which proves the base change theorem for totally ramified extensions (and the part (i) of Theorem A), and then appeals to the local Kronecker-Weber theorem to prove the base change in the unramified case. Here we provided a uniform proof by using the norm operator in the general setting. In Section 6 we combined Sen [8] with the standard material from Serre [9]. Throughout this article we avoided the use of topological rings/fields, and instead used the language of commutative algebra, which might be a somewhat new way of exposition.

## REFERENCES

- [1] R. Coleman, *Division values in local fields*, Invent. Math. **53** (1979), 91-116.
- [2] E. de Shalit, *Relative Lubin-Tate groups*, Proc. Amer. Math. Soc. **95** (1985), 1-4.
- [3] R. Gold, *Local class field theory via Lubin-Tate groups*, Indiana Univ. Math. J. **30** (1981), 795-798.
- [4] K. Iwasawa, *Local Class Field Theory*, Oxford Univ. Press, 1986.
- [5] J. Lubin, *The local Kronecker-Weber theorem*, Trans. Amer. Math. Soc. **267-1** (1981), 133-138.
- [6] J. Lubin, J. Tate, *Formal complex multiplication in local fields*, Ann. Math. **81** (1965), 380-387.
- [7] M. Rosen, *An elementary proof of the Kronecker-Weber theorem*, Trans. Amer. Math. Soc. **265-2** (1981), 599-605.
- [8] S. Sen, *On automorphisms of local fields*, Ann. Math. **90** (1969), 33-46.
- [9] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1962.