ANNALES
DE LA FACULTÉ
DES SCIENCES
DE
TOULOUSE
Mathématiques

TERUYOSHI YOSHIDA

Local Class Field Theory via Lubin-Tate Theory

Tome XVII, nº 2 (2008), p. 411-438.

<http://afst.cedram.org/item?id=AFST_2008_6_17_2_411_0>

Annales de la Faculté des Sciences de Toulouse Vol. XVII, n° 2, 2008
pp. 411–438

Local Class Field Theory via Lubin-Tate Theory[(*)]

Teruyoshi Yoshida[(1)]

Abstract. — We give a self-contained exposition of local class field theory, via Lubin-Tate theory and the Hasse-Arf theorem, refining the arguments of Iwasawa [9].

Résumé. — Nous présentons une démonstration complète de la théorie du corps de classes locale via la théorie de Lubin-Tate et le théorème de Hasse-Arf, en raffinant des arguments d'Iwasawa [9].

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 Appendix I. We have tried to make the paper self-contained, to the extent of repeating proofs of standard results on local fields and avoiding topological arguments using compactness. Our argument is close to Iwasawa [9], but the main innovation here is to use the relative Lubin-Tate groups of de Shalit [5] to prove the base change property (Theorem 5.15) directly, without proving the local Kronecker-Weber theorem first.

Theorem A (Local Class Field Theory). —

(i) For any local field K, there is a unique homomorphism $\mathrm{Art}_K : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$*, characterized by the two properties :*

(a) If π is a uniformizer of K, then $\mathrm{Art}_K(\pi)|_{K^{\mathrm{ur}}} = \mathrm{Frob}_K$.

(*) Reçu le 05/06/2006, accepté le 07/07/2008
(1) Harvard University, Department of Mathematics, 1 Oxford Street, Cambridge, MA 02138, USA
yoshida@math.harvard.edu

(b) *If* K'/K *is a finite abelian extension, then* $\mathrm{Art}_K(N_{K'/K}(K'^{\times}))|_{K'} = \mathrm{id}$.

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

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

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 separable closure F^{sep}, and regard any algebraic (resp. separable) extension of F as a subfield of $\overline{F}$ (resp. F^{sep}). For a finite separable extension F'/F, we denote the norm map by $N_{F'/F} : F'^{\times} \to F^{\times}$. We denote the maximal abelian extension of F in $\overline{F}$ by F^{ab}.

For a positive integer n not divisible by $\mathrm{char} F$, 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. We denote a finite field consisting of q elements by $\mathbb{F}_q$. For each $n \geqslant 1$, we have $\mathbb{F}_{q^n} = \mathbb{F}_q(\boldsymbol{\mu}_{q^n-1})$ in $\overline{\mathbb{F}}_q$. The Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is isomorphic to $\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/(n)$, the *profinite completion* of $\mathbb{Z}$, by sending the q-th power *Frobenius map* $x \mapsto x^q$ to 1.

2. Local fields and complete extensions

2.1. Complete discrete valuation fields (see Appendix I)

Let K be the fraction field of a CDVR $\mathcal{O} := \mathcal{O}_K$ (the *ring of integers* of K) with maximal ideal $\mathfrak{p} := \mathfrak{p}_K$, such that its *residue field* $k := \mathcal{O}/\mathfrak{p}$ is a perfect field. A generator of $\mathfrak{p}$ is called a *uniformizer* of K. We denote its *valuation* by $v = v_K : K^{\times} \to \mathbb{Z}$. If K'/K is a finite separable extension, then K' is the fraction field of a CDVR $\mathcal{O}_{K'}$, namely the integral closure of $\mathcal{O}$ 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 $[K' : K] = ef$, and $v_{K'}|_{K^{\times}} = e \cdot v_K$ by definition. below) : If K''/K' is another finite separable extension, clearly

$e(K''/K) = e(K''/K')e(K'/K)$ and $f(K''/K) = f(K''/K')f(K'/K)$. We say K'/K is *unramified* if $e = 1$, and *totally ramified* if $f = 1$. By the multiplicativity of e and f, any intermediate extension of an unramified (resp. a totally ramified) extension is again unramified (resp. totally ramified). Now for any finite separable K'/K, if F is the Galois closure of K', then as the action of $\mathrm{Gal}(F/K)$ preserves $\mathcal{O}_F$ and hence also v_F, we have $v_K(N_{K'/K}(x)) = \frac{1}{e(F/K)}v_F(N_{K'/K}(x)) = \frac{[K':K]}{e(F/K)}v_F(x) = \frac{[K':K]}{e(K'/K)}v_{K'}(x) = f(K'/K)v_{K'}(x)$ for all $x \in K'^{\times}$, i.e. we have $v_K \circ N_{K'/K} = f \cdot v_{K'}$.

For any separable extension E/K (not necessarily finite) in K^{sep}, the *ring of integers* $\mathcal{O}_E$ of E is defined as the integral closure of $\mathcal{O}$ in E. If $E = \bigcup_{K'} K'$, where K'/K are finite separable, then $\mathcal{O}_E = \bigcup_{K'} \mathcal{O}_{K'}$. As $\mathfrak{p}_{K'} \subset \mathfrak{p}_{K''}$ whenever $K' \subset K''$, we have an ideal $\mathfrak{p}_E := \bigcup_{K'} \mathfrak{p}_{K'}$ of $\mathcal{O}_E$, and $\mathcal{O}_E^{\times} = \bigcup_{K'} \mathcal{O}_{K'}^{\times} = \mathcal{O}_E \setminus \mathfrak{p}_E$. Therefore $\mathcal{O}_E$ is a local ring with the maximal ideal $\mathfrak{p}_E$, and $E = \bigcup K' = \mathrm{Frac}(\mathcal{O}_E)$.

DEFINITION 2.1. — *We call a separable extension E/K* unramified *(resp.* totally ramified*) if it is a union of unramified (resp. totally ramified) finite extensions of K. We say E/K is* finitely ramified *if E is a finite extension of an unramified extension of K.*

LEMMA 2.2. — *Let $E \subset K^{\mathrm{sep}}$ be finitely ramified over K.*

(i) The ring of integers $\mathcal{O}_E$ is a DVR.

(ii) If E'/E is finite separable, then $E'\widehat{E} = \widehat{E}'$ and $\widehat{E} \cap E' = E$.

(iii) $\widehat{E} \cap K^{\mathrm{sep}} = E$. (Hence $\widehat{E} = \widehat{E}' \implies E = E'$ for $E, E'/K$ finitely ramified.)

Proof. — (i) : If E/K is unramified, then $\mathfrak{p}_{K'} = \mathfrak{p}\mathcal{O}_{K'}$ for all finite intermediate K'/K, therefore $\mathfrak{p}_E = \mathfrak{p}\mathcal{O}_E$ and $\mathcal{O}_E$ is a DVR. If E' is finite over E, then $\mathcal{O}_{E'}$ is the integral closure of the DVR $\mathcal{O}_E$ in E', hence a DVR. (ii) follows from Proposition 7.1(ii). (ii) implies (iii). □

2.2. Local fields and their complete extensions

In the rest of the article, we fix a prime p, and let K denote a *local field*, i.e. a complete discrete valuation field whose residue field k is a finite field $\mathbb{F}_q$ of characteristic p. Then $\mathrm{char}K = 0$ or p, and if $\mathrm{char}K = 0$, then K is a finite extension of the p-adic field $\mathbb{Q}_p$. Finite unramified extensions of local fields are classified using the following lemma (see Appendix I for its proof) :

LEMMA 2.3. — (Hensel's lemma) *Let $n \geqslant 1$ with $(p, n) = 1$. Then $\boldsymbol{\mu}_n \subset k \iff \boldsymbol{\mu}_n \subset K$.*

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

$$\mathrm{Gal}(K^{\mathrm{ur}}/K) \xrightarrow{\cong} \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \xrightarrow{\cong} \widehat{\mathbb{Z}}.$$

The *arithmetic Frobenius* $\varphi \in \mathrm{Gal}(K^{\mathrm{ur}}/K)$ is defined as the element which reduces mod$\mathfrak{p}$ to the q-th power Frobenius map of $\overline{\mathbb{F}}_q$, and its inverse is denoted by $\mathrm{Frob}_K := \varphi^{-1}$ (*geometric Frobenius*). Unramified extensions of K are none other than subfields of K^{ur}, hence always abelian over K. If E'/K is a separable extension, then E' and $E := E' \cap K^{\mathrm{ur}}$ have the same residue fields. When E'/K is Galois, we define its *Weil group* by $W(E'/K) := \{\sigma \in \mathrm{Gal}(E'/K) \mid \sigma|_E \in \mathrm{Frob}_K^{\mathbb{Z}}\}$, which is an extension of $W(E/K)$ (a quotient group of $\mathbb{Z}$) by $\mathrm{Gal}(E'/E)$. If E/K is finite, then $W(E'/K) = \mathrm{Gal}(E'/K)$.

Definition 2.4. — *We call the completion $L = \widehat{E}$ of a finitely ramified (§2.1) extension E of K a* complete extension *of K (if E/K is finite, then $L = E$). Then $\mathcal{O}_L = \widehat{\mathcal{O}}_E$ is a CDVR with the maximal ideal $\mathfrak{p}_L = \mathfrak{p}_E\mathcal{O}_L$. The complete extensions correspond bijectively to finitely ramified extensions E/K by Lemma 2.2(iii). When E/K is unramified, we call $L = \widehat{E}$ a* complete unramified extension *of K.*

The $\widehat{K} := \widehat{K}^{\mathrm{ur}}$ is a complete unramified extension of K, and we write $\widehat{\mathcal{O}} := \mathcal{O}_{\widehat{K}}$, $\widehat{\mathfrak{p}} := \mathfrak{p}_{\widehat{K}}$. We consider every complete unramified extension L/K as a subfield of $\widehat{K}$, in which case $\mathfrak{p}_L = \mathfrak{p}\mathcal{O}_L$ and a uniformizer of L is also a uniformizer of $\widehat{K}$. Let $L' = \widehat{E}'$ be a complete extension of K, and set $E := E' \cap K^{\mathrm{ur}}$. Then $L = \widehat{E}$ is a complete unramified extension of K, and L', E', E, L all have the same residue fields, i.e. L'/L is totally ramified. We consider every complete extension L'/K as a subfield of $\widehat{K}^{\mathrm{sep}}$ via $L \subset \widehat{K}$.

Definition 2.5. — *Let L' be a totally ramified extension of a complete unramified extension L/K. When L'/L is finite, we say L' is* Galois over K *if for all $i \in \mathbb{Z}$, the $\varphi^i = \mathrm{Frob}_K^{-i} \in \mathrm{Aut}(L/K)$ extends to $[L' : L]$ distinct elements of $\mathrm{Aut}(L'/K)$. In general, we say L' is* Galois over K *if it is a union of finite extensions of L which are Galois over K. In this case we define* *the* Weil group *of* L'/K *by* $W(L'/K) := \{\sigma \in \mathrm{Aut}(L'/K) \mid \sigma|_L \in \mathrm{Frob}_K^{\mathbb{Z}}\}$, *which is an extension of* $W(L/K)$ *(a quotient group of* $\mathbb{Z}$*) by* $\mathrm{Gal}(L'/L)$*. When* $L = \widehat{K}$*, define* $v = v_K : W(L'/K) \to \mathbb{Z}$ *by* $\sigma|_L = \mathrm{Frob}_K^{v(\sigma)}$*.*

This terminology coincides with the usual one when L/K is finite. When $L' = \widehat{E}'$ for finitely ramified Galois E'/K, then every $\sigma \in \mathrm{Gal}(E'/K)$ induces $\mathcal{O}$-automorphisms of $\mathcal{O}_{E'}$ and $\mathcal{O}_{E'}/\mathfrak{p}_{E'}^m$ for all $m \geqslant 1$, hence of $\mathcal{O}_{L'} = \widehat{\mathcal{O}}_{E'}$. Therefore it extends to a K-automorphism of L', and we have a canonical injection $\mathrm{Gal}(E'/K) \to \mathrm{Aut}(L'/K)$. Therefore, as a totally ramified extension of $L = \widehat{E}$ for $E = E' \cap K^{\mathrm{ur}}$, we see that L' is Galois over K (because $[L' : L] = [E' : E]$ by Lemma 2.2(ii)), and canonically $W(E'/K) \cong W(L'/K)$. By passing to the limit, this last isomorphism extends to the case where $L' = E'L$ with a general Galois extension E'/K.

3. Formal groups and Lubin-Tate groups

3.1. Formal groups

Let A be a ring, not the 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 $F \in A[[X_1, \dots, X_n]]$ with no constant term :

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

Definition 3.1. — *A* formal group over *A is a formal power series of two variables* $F(X,Y) \in A[[X,Y]]$ *which satisfies the following :*

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

Precisely speaking, these are *commutative formal groups of dimension 1.* 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 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 with 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 3.2. — *Let F, G be formal groups over A. A power series $f(X) \in (X) \subset A[[X]]$ is called a* homomorphism *from F to G if it satisfies*

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

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

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

3.2. Lubin-Tate groups

We return to the notation of §2.2, i.e. K is a local field with the ring of integers $\mathcal{O}$ and its maximal ideal $\mathfrak{p}$, and $\mathcal{O}/\mathfrak{p} \cong \mathbb{F}_q$ where q is a power of p. Let L be a *complete unramified extension* of K (§2.2). As $\mathfrak{p}_L = \mathfrak{p}\mathcal{O}_L$, we write $\mathrm{mod}\,\mathfrak{p}$ for $\mathrm{mod}\,\mathfrak{p}\mathcal{O}_L$. Let φ be the arithmetic Frobenius, extended to a K-automorphism of L. For $\alpha \in L$ and $i \in \mathbb{Z}$, we write $\alpha^{\varphi^i} := \varphi^i(\alpha)$. For a power series F over $\mathcal{O}_L$, we define F^{φ^i} by applying φ^i to all coefficients of F. If F is a formal group over $\mathcal{O}_L$, so is F^{φ^i}.

Definition 3.3. — *For uniformizers π, π' of L, set $\Theta^L_{\pi,\pi'} := \{\theta \in \mathcal{O}_L \mid \theta^\varphi/\theta = \pi'/\pi\}$. It is an additive group. If $\theta \in \Theta^L_{\pi,\pi'}$ and $\theta' \in \Theta^L_{\pi',\pi''}$, then $\theta\theta' \in \Theta^L_{\pi,\pi''}$. We have $\mathcal{O} \subset \Theta^L_{\pi,\pi}$ (actually we will see $\mathcal{O} = \Theta^L_{\pi,\pi}$ by Lemma 5.2(i)).*

Lemma 3.4. — *Let π be a uniformizer of L, and let $f \in \mathcal{O}_L[[X]]$ satisfy :*

$$f(X) \equiv \pi X \ (\mathrm{mod}\,\deg 2), \qquad f(X) \equiv X^q \ (\mathrm{mod}\ \mathfrak{p}). \tag{3.2.1}$$

Let π', f' be another such pair. Assume that $\theta_1, \dots, \theta_t \in \Theta^L_{\pi,\pi'}$. Then there is a unique $F \in \mathcal{O}_L[[X_1, \dots, X_t]]$ satisfying the following :

$$F \equiv \theta_1 X_1 + \cdots + \theta_t X_t \pmod{\deg 2}, \qquad f' \circ F = F^{\varphi} \circ f.$$

Proof. — It suffices to show that for each $m \geqslant 1$, there is a unique polynomial F_m of degree $\leqslant m$ that satisfies the conditions $\bmod \deg(m+1)$. 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 π'. Now we show that a homogeneous polynomial $H_{m+1} := F_{m+1} - F_m$ of degree $m+1$ is uniquely determined. We need $f' \circ F_{m+1} - F_{m+1}^{\varphi} \circ f \equiv G_{m+1} + (f' \circ H_{m+1} - H_{m+1}^{\varphi} \circ f) \equiv G_{m+1} + (\pi' H_{m+1} - \pi^{m+1} H_{m+1}^{\varphi}) \pmod{\deg(m+2)}$ to vanish. For any monomial of degree $m+1$, if we let $\pi'\beta$ be its coefficient in G_{m+1}, and α its coefficient in H_{m+1}, then $\pi'\beta + \pi'\alpha - \pi^{m+1}\alpha^{\varphi} = 0$, hence $\alpha = -\beta - \sum_{i=1}^{\infty} (\pi^{m+1}/\pi')^{1+\varphi+\cdots\varphi^{i-1}} \beta^{\varphi^i}$. □

Proposition 3.5. — *Let $f, f' \in \mathcal{O}_L[[X]]$ be as above, with linear coefficients π, π' respectively.*

(i) There exists a unique formal group F_f over $\mathcal{O}_L$ such that $f \in \mathrm{Hom}_{\mathcal{O}_L}(F_f, F_f^{\varphi})$. (We call F_f the Lubin-Tate group *associated to f.)*

(ii) There is a unique map $[\cdot]_{f,f'} : \Theta^L_{\pi,\pi'} \to (X) \subset \mathcal{O}_L[[X]]$ such that :

$$[\theta]_{f,f'}(X) \equiv \theta X \pmod{\deg 2}, \qquad f' \circ [\theta]_{f,f'} = [\theta]^{\varphi}_{f,f'} \circ f.$$

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

(iii) We have $[\theta]_{f,f'} \in \mathrm{Hom}_{\mathcal{O}_L}(F_f, F_{f'})$ for all $\theta \in \Theta^L_{\pi,\pi'}$.

Proof. — (i) : Lemma 3.4 for $\pi = \pi'$, $f = f'$, $t = 2$, $\theta_1 = \theta_2 = 1$ gives 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 $t = 3$ and $\theta_1 = \theta_2 = \theta_3 = 1$, hence are equal. Thus F_f is a formal group and $f \in \mathrm{Hom}_{\mathcal{O}_L}(F_f, F_f^{\varphi})$. (ii) : Lemma 3.4 for $t = 1$ gives $[\theta]_{f,f'}$. The properties characterizing $[\theta + \theta']_{f,f'}$ (resp. $[\theta\theta']_{f,f''}$) are shared by $[\theta]_{f,f'} +_{F_{f'}} [\theta']_{f,f'}$ (resp. $[\theta']_{f',f''} \circ [\theta]_{f,f'}$) because :

$$f' \circ ([\theta] +_{F_{f'}} [\theta']) = (f' \circ [\theta]) +_{F_{f'}^{\varphi}} (f' \circ [\theta']) = ([\theta]^{\varphi} +_{F_{f'}^{\varphi}} [\theta']^{\varphi}) \circ f = ([\theta] +_{F_{f'}} [\theta'])^{\varphi} \circ f$$

$$(\text{resp.} f'' \circ ([\theta'] \circ [\theta]) = [\theta']^{\varphi} \circ f' \circ [\theta]) = [\theta']^{\varphi} \circ [\theta]^{\varphi} \circ f = ([\theta'] \circ [\theta])^{\varphi} \circ f\ ).$$

(iii) : For $[\theta] := [\theta]_{f,f'}$, we have $[\theta] \circ F_f = F_{f'} \circ [\theta]$, because the equalities :

$$f' \circ ([\theta] \circ F_f) = [\theta]^{\varphi} \circ f \circ F_f = ([\theta]^{\varphi} \circ F_f^{\varphi}) \circ f = ([\theta] \circ F_f)^{\varphi} \circ f,$$

$$f' \circ (F_{f'} \circ [\theta]) = F_{f'}^{\varphi} \circ f' \circ [\theta] = (F_{f'}^{\varphi} \circ [\theta]^{\varphi}) \circ f = (F_{f'} \circ [\theta])^{\varphi} \circ f,$$

show that both sides satisfy the conditions of Lemma 3.4 for $\pi = \pi',\ t = 2,\ \theta_1 = \theta_2 = \theta$. □

Example 3.6. — *If $K = \mathbb{Q}_p$, $\pi = p$ and $f = (1+X)^p - 1$, then $F_f = \widehat{\mathbb{G}}_m = X + Y + XY$.*

Corollary 3.7. —

(i) *The map $[\cdot]_f := [\cdot]_{f,f} : \mathcal{O} \longrightarrow \mathrm{End}_{\mathcal{O}_L}(F_f)$ is an injective ring homomorphism. (Hence $(F_f, [\cdot]_f)$ is a* formal $\mathcal{O}$-module.*)*

(ii) *If $\theta \in \Theta^{L,\times}_{\pi,\pi'} := \Theta^{L}_{\pi,\pi'} \cap \mathcal{O}_L^{\times}$, then $[\theta]_{f,f'}$ is an isomorphism with the inverse $[\theta^{-1}]_{f',f}$.*

Example 3.8. — *We have $\pi \in \Theta^L_{\pi,\pi^{\varphi}}$, and $[\pi]_{f,f^{\varphi}} = f : F_f \to F_f^{\varphi}$ for f satisfying (3.2.1), by uniqueness. (Also note that $F_f^{\varphi} = F_{f^{\varphi}}$ and $[\theta]^{\varphi}_{f,f'} = [\theta^{\varphi}]_{f^{\varphi},f'^{\varphi}}$ by uniqueness.)*

Definition 3.9. — *Generalizing Example 3.8, define $f_m := f^{\varphi^{m-1}} \circ \cdots \circ f^{\varphi} \circ f \in \mathcal{O}_L[[X]]$ for $m \geqslant 1$, and set $f_0(X) := X$. Then, by Example 3.8 and Proposition 3.5(ii) :*

$$f_m = [\pi^{\varphi^{m-1}}]_{f^{\varphi^{m-1}},f^{\varphi^m}} \circ \cdots \circ [\pi^{\varphi}]_{f^{\varphi},f^{\varphi^2}} \circ [\pi]_{f,f^{\varphi}} = [\pi_m]_{f,f^{\varphi^m}} \quad (\forall m \geqslant 0),$$

where we define $\pi_m \in \mathcal{O}_L$ by $\pi_m := \prod_{t=0}^{m-1} \pi^{\varphi^t}$ and $\pi_0 := 1$.

4. Lubin-Tate extensions and Artin maps

4.1. Lubin-Tate extensions

Here we fix a complete unramified extension L of K.

Definition 4.1. — *Let $f \in \mathcal{O}_L[X]$ be a monic polynomial satisfying (3.2.1) for a uniformizer π of L. For $m \geqslant 1$, let L_f^m be the splitting field of $f_m \in \mathcal{O}_L[X]$ (Definition 3.9) over L, and let $\boldsymbol{\mu}_{f,m} := \{\alpha \in L_f^m \mid f_m(\alpha) = 0\}$.*

Example 4.2. — *In Example 3.6, we have $f_m(X) = [p^m]_f(X) = (1+X)^{p^m} - 1$, $\boldsymbol{\mu}_{f,m} = \{\zeta - 1 \mid \zeta \in \boldsymbol{\mu}_{p^m}\}$ and $L_f^m = L(\boldsymbol{\mu}_{p^m})$ for all $m \geqslant 0$.*

LEMMA 4.3. — *Let $m \geqslant 1$ and $f \in \mathcal{O}_L[X]$ as above, and set $L' := L_f^m$ and $[\cdot] := [\cdot]_f$.*

(i) The extension L'/L is separable and $\boldsymbol{\mu}_{f,m} \subset \mathfrak{p}_{L'}$. (In particular, we can substitute the elements of $\boldsymbol{\mu}_{f,m}$ into power series over $\mathcal{O}_L$ (see Appendix I).)

(ii) For $x \in K^\times$ with $v(x) = m$ and $\alpha \in \mathfrak{p}_{L^{\mathrm{sep}}}$:

$$\alpha \in \boldsymbol{\mu}_{f,m} \iff [x](\alpha) = 0 \iff [a](\alpha) = 0 \ (\forall a \in \mathfrak{p}^m).$$

Proof. — (i) : The separability of L'/L is automatic when $\mathrm{char}K = 0$, and in general it follows from Proposition 8.1 in the Appendix II (which in turn follows from Proposition 4.4(i) when $\mathrm{char}K = 0$). Now $\boldsymbol{\mu}_{f,m} \subset \mathcal{O}_{L'}$ as f_m is a monic in $\mathcal{O}_L[X]$. If $\alpha \in \mathcal{O}_{L'}^\times$, then $f_m(\alpha)$, being $\equiv \alpha^{q^m} (\mathrm{mod} \mathfrak{p}_{L'})$, will also be in $\mathcal{O}_{L'}^\times$. Thus $\boldsymbol{\mu}_{f,m} \subset \mathfrak{p}_{L'}$. (ii) : By Definition 3.9, we have $[x] = [x/\pi_m]_{f^{\varphi^m},f} \circ f_m$. As $[x/\pi_m]$ is invertible, we see the first equivalence. The second one follows by $\mathfrak{p}^m = (x)$. □

PROPOSITION 4.4. — *Let $m \geqslant 1$ and $f \in \mathcal{O}_L[X]$ as above, with the linear coefficient π.*

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

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

(ii) If $\alpha \in \boldsymbol{\mu}_{f,m}^\times$, then $L_f^m = L(\alpha)$, $N_{L_f^m/L}(-\alpha) = \pi^{\varphi^{m-1}}$ and α is a uniformizer of L_f^m. The L_f^m/L is totally ramified Galois extension of degree $|\boldsymbol{\mu}_{f,m}^\times| = q^{m-1}(q-1)$.

(iii) We have canonical isomorphisms of abelian groups :

$$\rho_{f,m} : \mathrm{Gal}(L_f^m/L) \xrightarrow{\cong} \mathrm{Aut}_{\mathcal{O}}(\boldsymbol{\mu}_{f,m}) \xrightarrow{\cong} (\mathcal{O}/\mathfrak{p}^m)^\times.$$

$$(\alpha \mapsto [u]_f(\alpha), \ \forall \alpha \in \boldsymbol{\mu}_{f,m}) \longmapsto u \bmod \mathfrak{p}^m$$

Proof. — We write $+_f := +_{F_f}$ and $L' := L_f^m$. (i) : Lemma 4.3(ii) shows that $\boldsymbol{\mu}_{f,m}$ is an $\mathcal{O}$-module by $+_f, [\cdot]$, killed by $\mathfrak{p}^m$. The stated $\mathcal{O}$-homomorphism is injective as $[a](\alpha) \neq 0$ for some $a \in \mathfrak{p}^{m-1}$ by Lemma 4.3(ii), hence surjective as $|\mathcal{O}/\mathfrak{p}^m| = q^m = \deg f_m \geqslant |\boldsymbol{\mu}_{f,m}|$. (Thus $|\boldsymbol{\mu}_{f,m}| = q^m$ and hence $\boldsymbol{\mu}_{f,m}^\times$ is the set of all roots of f_m/f_{m-1}.) (ii) : We have $\boldsymbol{\mu}_{f,m} \subset L(\alpha)$

by (i), hence $L' = L(\alpha)$ and L'/L is Galois. Now the constant term of f_m/f_{m-1} reads $\pi^{\varphi^{m-1}} = \prod_{\alpha\in\boldsymbol{\mu}_{f,m}^\times}(-\alpha)$, and taking the $v_{L'}$ of both sides shows $e(L'/L) = \sum v_{L'}(-\alpha) \geqslant |\boldsymbol{\mu}_{f,m}^\times|$ by Lemma 4.3(i). But $|\boldsymbol{\mu}_{f,m}^\times| = \deg(f_m/f_{m-1}) \geqslant [L' : L] \geqslant e(L'/L)$, hence all are equalities and f_m/f_{m-1} is irreducible. (iii) : As $+_f, [\cdot]$ have coefficients in $\mathcal{O}_L$, for all $\sigma \in \mathrm{Gal}(L'/L)$, we have $\sigma(\alpha +_f \alpha') = \sigma(\alpha) +_f \sigma(\alpha')$ and $\sigma([a](\alpha)) = [a](\sigma(\alpha))$, i.e. $\mathrm{Gal}(L'/L)$ acts on $\boldsymbol{\mu}_{f,m}$ by $\mathcal{O}$-homomorphisms. Hence we have a group homomorphism $\rho_{f,m} : \mathrm{Gal}(L'/L) \longrightarrow \mathrm{Aut}_{\mathcal{O}}(\boldsymbol{\mu}_{f,m})$. This is injective as $L' = L_f^m$, and $\mathrm{Aut}_{\mathcal{O}}(\boldsymbol{\mu}_{f,m}) \cong (\mathcal{O}/\mathfrak{p}^m)^\times$ by (i). It is surjective as $|\mathrm{Gal}(L'/L)| = [L' : L] = |(\mathcal{O}/\mathfrak{p}^m)^\times|$ by (ii). □

4.2. Artin map

In this subsection we use the notation $(\ )^{(i)} := (\ )^{\varphi^i}$ and $\boldsymbol{\mu}_{f,m}^{(i)} := \boldsymbol{\mu}_{f^{(i)},m}$ for all $i \in \mathbb{Z}$. We extend Definition 3.9 to define $\pi_j \in L^\times$ for all $j \in \mathbb{Z}$ by requiring $\pi_{j+j'} = \pi_{j'}^{(j)}\pi_j$ for all $j, j' \in \mathbb{Z}$, i.e. $\pi_j := (\pi_{-j}^{-1})^{(j)}$ for $j < 0$. Then $v_L(\pi_j) = j$ for all $j \in \mathbb{Z}$.

Lemma 4.5. — *If $\theta \in \Theta^L_{\pi,\pi'}$, then $\theta^{(j)}/\theta = \pi'_j/\pi_j$ for all $j \in \mathbb{Z}$. Also, $\pi_j \in \Theta^L_{\pi,\pi^{(j)}}$.*

Proof. — Using $\pi'_{j+1}/\pi_{j+1} = (\pi'_j/\pi_j)(\pi'/\pi)^{(j)} = (\pi'_j/\pi_j)(\theta^\varphi/\theta)^{(j)} = (\pi'_j/\pi_j)(\theta^{(j+1)}/\theta^{(j)})$, argue by induction in both directions. Take $\pi' = \pi^\varphi$ and $\theta = \pi$ for the second claim. □

Lemma 4.6. — *Let $f, f' \in \mathcal{O}_L[X]$ be as above with linear coefficients π, π', respectively. If $\theta \in \Theta^{L,\times}_{\pi,\pi'}$ (see Corollary 3.7(ii)), then for all $m \geqslant 1$, it gives an isomorphism $[\theta] = [\theta]_{f,f'} : \boldsymbol{\mu}_{f,m} \to \boldsymbol{\mu}_{f',m}$ of $\mathcal{O}$-modules, and $L^m_f = L^m_{f'}$.*

Proof. — The $[\theta]$ maps $\boldsymbol{\mu}_{f,m}$ to $\boldsymbol{\mu}_{f',m}$ because $f'_m \circ [\theta] = [\theta]^{(m)} \circ f_m$. It is an $\mathcal{O}$-homomorphism by Proposition 3.5(ii),(iii), and is an isomorphism as $[\theta^{-1}]$ gives its inverse. As $[\theta], [\theta^{-1}] \in \mathcal{O}_L[[X]]$, we have $\boldsymbol{\mu}_{f',m} = [\theta](\boldsymbol{\mu}_{f,m}) \subset L^m_f$ and $\boldsymbol{\mu}_{f,m} \subset L^m_{f'}$, thus $L^m_f = L^m_{f'}$. □

Proposition 4.7. — *Let $m \geqslant 1$ and $f \in \mathcal{O}_L[X]$ as above, with the linear coefficient π.*

(i) *The L^m_f is Galois over K, and the following map is bijective for any $\alpha \in \boldsymbol{\mu}^\times_{f,m}$:*

$$K^\times/(1+\mathfrak{p}^m) \ni x \bmod 1+\mathfrak{p}^m \longmapsto [x\pi_j]_{f,f^{(j)}}(\alpha) \in \coprod_{j\in\mathbb{Z}} \boldsymbol{\mu}^{(j),\times}_{f,m}\ (v(x) = -j).$$

(ii) Let $L = \widehat{K}$. The $\rho_{f,m}$ of Proposition 4.4(iii) extend to isomorphisms :

$$\rho_{f,m} : W(\widehat{K}_f^m/K) \xrightarrow{\cong} K^\times/(1+\mathfrak{p}^m).$$

$$(\varphi^j \text{ on } \widehat{K},\ \alpha \mapsto [x\pi_j](\alpha),\ \forall \alpha \in \boldsymbol{\mu}_{f,m}) \longmapsto x \bmod 1+\mathfrak{p}^m \ \ (v(x) = -j)$$

Setting $\widehat{K}_f^{\mathrm{LT}} := \bigcup_{m \geqslant 1} \widehat{K}_f^m$, we get $\rho_f : W(\widehat{K}_f^{\mathrm{LT}}/K) \xrightarrow{\cong} K^\times$ by passing to the limit.

Proof. — (i) : If $v(x) = -j$, then $x\pi_j \in \Theta^{L,\times}_{\pi,\pi^{(j)}}$ by Lemma 4.5, hence $[x\pi_j] : \boldsymbol{\mu}_{f,m} \xrightarrow{\cong} \boldsymbol{\mu}^{(j)}_{f,m}$ by Lemma 4.6. As $[x\pi_j]$ is $\mathcal{O}$-linear, $v^{-1}(-j)/(1+\mathfrak{p}^m) \ni x \mapsto [x\pi_j](\alpha) \in \boldsymbol{\mu}^{(j),\times}_{f,m}$ is bijective for each j. As $L(\alpha) = L_f^m = L^m_{f^{(j)}}$ by Proposition 4.4(ii) and Lemma 4.6, the $\varphi^j \in \mathrm{Aut}(L/K)$ extends to L_f^m by $\alpha \mapsto \alpha'$ for each $\alpha' \in \boldsymbol{\mu}^{(j),\times}_{f,m}$, hence L_f^m is Galois over K. (ii): Let $\sigma \in W(\widehat{K}_f^m/K)$ with $\sigma|_{\widehat{K}} = \varphi^j$. If $\alpha \in \boldsymbol{\mu}^\times_{f,m}$, then $\sigma(\alpha) \in \boldsymbol{\mu}^{(j),\times}_{f,m}$, hence $\sigma(\alpha) = [x\pi_j](\alpha)$ for a unique $x \bmod 1+\mathfrak{p}^m$ by (i). This holds for all $\alpha \in \boldsymbol{\mu}_{f,m}$ because $\sigma([a]_f(\alpha)) = [a]_f^{(j)}(\sigma(\alpha)) = [a]_{f^{(j)}}[x\pi_j](\alpha) = [x\pi_j][a]_f(\alpha)$ for all $a \in \mathcal{O}$ (this shows the compatibility of $\rho_{f,m}$ for varying m). The map $\rho_{f,m}$ is a group homomorphism because if $\tau(\alpha) = [y\pi_{j'}](\alpha)$, then $\sigma\tau(\alpha) = \sigma([y\pi_{j'}](\alpha)) = [y\pi_{j'}]^{(j)}[x\pi_j](\alpha) = [y\pi_{j'}^{(j)} \cdot x\pi_j](\alpha) = [xy \cdot \pi_{j+j'}](\alpha)$. It is bijective because it restricts to $\mathrm{Gal}(\widehat{K}_f^m/\widehat{K}) \cong (\mathcal{O}/\mathfrak{p}^m)^\times = \mathcal{O}^\times/(1+\mathfrak{p}^m)$ by Proposition 4.4(iii) and the quotient $W(\widehat{K}/K) = \mathrm{Frob}_K^{\mathbb{Z}}$ is mapped onto $K^\times/\mathcal{O}^\times \cong \mathbb{Z}$, i.e. $v \circ \rho_{f,m} = v$. □

Proposition 4.8. — *The map $\psi : \widehat{\mathcal{O}}^\times \ni \theta \longmapsto \theta^\varphi/\theta \in \widehat{\mathcal{O}}^\times$ is surjective. In particular, for any pair of uniformizers π, π' of $\widehat{K}$, we have $\Theta^{\widehat{K},\times}_{\pi,\pi'} \neq \emptyset$.*

Proof. — As $\widehat{\mathcal{O}}^\times \cong \varprojlim (\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^m)^\times = \varprojlim \widehat{\mathcal{O}}^\times/(1+\widehat{\mathfrak{p}}^m)$ and $\psi(1+\widehat{\mathfrak{p}}^m) \subset 1+\widehat{\mathfrak{p}}^m$, it suffices to show for every $u \in \widehat{\mathcal{O}}^\times$ and all $m \geqslant 1$, there is $\theta_m \in \widehat{\mathcal{O}}^\times$ with $\psi(\theta_m) \equiv u \pmod{\mathfrak{p}^m}$ and $\theta_{m+1} \equiv \theta_m \pmod{\mathfrak{p}^m}$. We get θ_1 because $\overline{\theta} \mapsto \overline{\psi(\theta)} = \overline{\theta}^{q-1}$ is surjective on $(\widehat{\mathcal{O}}/\widehat{\mathfrak{p}})^\times \cong \overline{\mathbb{F}}_q^\times$. Suppose we have θ_m, and let $u/\psi(\theta_m) = 1 + \alpha\pi^m$ for a uniformizer π of K. Then there is $\beta \in \widehat{\mathcal{O}}$ with $\beta^\varphi - \beta \equiv \alpha \pmod{\mathfrak{p}}$ because $\overline{\beta} \mapsto \overline{\beta^\varphi} - \overline{\beta} = \overline{\beta}^q - \overline{\beta}$ is surjective on $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \overline{\mathbb{F}}_q$, and $\theta_{m+1} := \theta_m(1+\beta\pi^m)$ will do. □

Corollary 4.9. — *The $\widehat{K}_f^m$ and $\rho_{f,m}$, hence also $\widehat{K}_f^{\mathrm{LT}}$ and ρ_f, of Proposition 4.7(ii) do not depend on f. (We will drop the subscript f and write $\widehat{K}^m$, ρ_m, $\widehat{K}^{\mathrm{LT}}$ and ρ.)*

Proof. — For f, f' with linear coefficients π, π', take $\theta \in \Theta_{\pi,\pi'}^{\widehat{K},\times}$ and $[\theta] : \boldsymbol{\mu}_{f,m} \xrightarrow{\cong} \boldsymbol{\mu}_{f',m}$ by Proposition 4.8. Lemma 4.6 shows $\widehat{K}_f^m = \widehat{K}_{f'}^m$. If $\sigma(\alpha) = [x\pi_j](\alpha)$ for $\sigma \in W(\widehat{K}_f^m/K)$, then $\sigma([\theta](\alpha)) = [\theta]^{(j)}[x\pi_j](\alpha) = [x\pi_j'][\theta](\alpha)$ by Lemma 4.5, hence $\rho_{f,m} = \rho_{f',m}$. □

Definition 4.10. — *For any $f \in \mathcal{O}_L[X]$ with L/K finite, set $K^m := K^{\mathrm{ur}}L_f^m$. Then K^m/K is finitely ramified, and Galois by Proposition 4.7(i). By Lemma 2.2, the completion of K^m is $\widehat{K}L_f^m = \widehat{K}^m$ and $K^m = \widehat{K}^m \cap K^{\mathrm{sep}}$, thus independent of f. Setting $K^{\mathrm{LT}} := \bigcup_{m\geqslant 1} K^m = \widehat{K}^{\mathrm{LT}} \cap K^{\mathrm{sep}}$, we have $W(K^{\mathrm{LT}}/K) \cong W(\widehat{K}^{\mathrm{LT}}/K)$ by the remark after Definition 2.5. We call a finite extension of K a* Lubin-Tate extension *if it is contained in K^{LT}. We call the inverse of ρ the* Artin map *of K and write $\mathrm{Art}_K : K^\times \xrightarrow{\cong} W(K^{\mathrm{LT}}/K)$. We have $v \circ \mathrm{Art}_K = v$.*

5. Galois Groups, Norm Groups and the Base Change

5.1. Galois groups

Now let $L = K_n/K$ be the *finite* unramified extension of degree n.

Proposition 5.1. — *Let $\theta \in \Theta_{\pi,\pi'}^{\widehat{K},\times}$ for $\pi, \pi' \in L$. Then $\theta \in \mathcal{O}_L^\times \iff N_{L/K}(\pi) = N_{L/K}(\pi')$.*

Proof. — Lemma 4.5 for $j = n$ shows $\theta^{\varphi^n}/\theta = N_{L/K}(\pi')/N_{L/K}(\pi)$, so use Lemma 5.2(i). □

Lemma 5.2. —

(i) For $n \geqslant 1$, the fixed field of φ^n in $\widehat{K}$ is K_n.

(ii) If $L = K_n$, then $N = N_{L/K}$ surjects onto $v^{-1}(n\mathbb{Z}) \subset K^\times$.

Proof. — (i) : As a set of representatives of $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \overline{\mathbb{F}}_q$, we can take $C := \{0\} \cup \bigcup_{n\geqslant 1} \boldsymbol{\mu}_{q^n-1}$ by Lemma 2.3. Then φ^n acts on C, and its fixed set is $C_n = \{0\} \cup \boldsymbol{\mu}_{q^n-1} \subset K_n$. Now take a uniformizer π of K, and consider the π-adic expansion in $\widehat{K}$ with respect to C (see Appendix I). If $x = \sum_{i=v(x)}^{\infty} a_i\pi^i$ for $a_i \in C$, then $x^{\varphi^n} = \sum_i a_i^{\varphi^n}\pi^i$, hence $x^{\varphi^n} = x \iff a_i \in C_n$ $(\forall i) \iff x \in K_n$. (ii) : For a uniformizer π of K, we have $v^{-1}(n\mathbb{Z}) = \mathcal{O}^\times \times \langle \pi^n \rangle$ and $N(\pi) = \pi^n$, hence it suffices to show that $N : \mathcal{O}_L^\times \to \mathcal{O}^\times$ is surjective. We have $\mathcal{O}^\times \cong \varprojlim \mathcal{O}^\times/(1 + \mathfrak{p}^m)$, $\mathcal{O}_L^\times \cong \varprojlim \mathcal{O}_L^\times/(1 + \mathfrak{p}_L^m)$, and $N(1+\mathfrak{p}_L^m) \subset 1+\mathfrak{p}^m$, because $N(1+\mathfrak{p}_L^m) \subset (1+\mathfrak{p}_L^m) \cap \mathcal{O} = 1+\mathfrak{p}^m$. Therefore it suffices to show that, for every $x \in \mathcal{O}^\times$ and all $m \geqslant 1$, there is $u_m \in \mathcal{O}_L^\times$ satisfying $N(u_m) \equiv x \pmod{\mathfrak{p}^m}$ and $u_{m+1} \equiv u_m \pmod{\mathfrak{p}^m}$. We get u_1 by the surjectivity of the norm map $(\mathcal{O}_L/\mathfrak{p}_L)^\times \to (\mathcal{O}/\mathfrak{p})^\times$ induced by N. Suppose we have u_m, and let $x/N(u_m) = 1+\alpha\pi^m$. Then there is $\beta \in \mathcal{O}_L$ whose trace $\equiv \alpha \pmod{\mathfrak{p}}$ because the trace map $\mathcal{O}_L/\mathfrak{p}_L \to \mathcal{O}/\mathfrak{p}$ is surjective, and $u_{m+1} := u_m(1+\beta\pi^m)$ will do. $\square$

Definition 5.3. — *Let $x \in K^\times$ with $v(x) = n > 0$. Take a uniformizer π of $L = K_n$ with $N_{L/K}(\pi) = x$ by Lemma 5.2(ii), and a monic $f \in \mathcal{O}_L[X]$ satisfying (3.2.1) for π. Then for $m \geqslant 1$, the fields L_f^m depend only on x by Proposition 5.1 and Lemma 4.6, so we denote them by $K_x^m := L_f^m$, and set $K_x^{\mathrm{ram}} := \bigcup_{m\geqslant 1} K_x^m$, which are totally ramified over L.*

Proposition 5.4. — *For $x \in K^\times$ with $v(x) = n > 0$, the element $\sigma := \mathrm{Art}_K(x) \in W(K^{\mathrm{LT}}/K)$ is characterized by $v(\sigma) = v(x)$ and $\sigma|_{K_x^{\mathrm{ram}}} = \mathrm{id}$. For all $m \geqslant 1$, the Artin map induces the isomorphism $K^\times/\big((1+\mathfrak{p}^m) \times \langle x\rangle\big) \xrightarrow{\cong} \mathrm{Gal}(K_x^m/K)$.*

Proof. — The σ acts as Frob_K^n on L, and $\pi_n = x$ implies $[x\pi_{-n}] = [1] = \mathrm{id}$ on $\boldsymbol{\mu}_{f,m}$, hence σ fixes K_x^{ram}. This characterizes σ because $K^{\mathrm{LT}} = K^{\mathrm{ur}}K_x^{\mathrm{ram}}$. It also shows that Art_K (or ρ_m^{-1}) descends to the claimed map, which is bijective because it restricts to $(\mathcal{O}/\mathfrak{p}^m)^\times \cong \mathrm{Gal}(K_x^m/L)$ and induces $K^\times/\big(\mathcal{O}^\times \times \langle x\rangle\big) \cong \mathrm{Gal}(L/K)$ on the quotients, as $v \circ \mathrm{Art}_K = v$. $\square$

5.2. Coleman operator and norm groups

As above, let $f \in \mathcal{O}_L[X]$ be a monic polynomial satisfying (3.2.1) for a uniformizer π of $L = K_n$, and 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), so $K_x^m = L(\boldsymbol{\mu}_m)$.

Lemma 5.5. — *Let $g \in \mathcal{O}_L[[X]]$.*

(i) If $g(\alpha) = 0$ for all $\alpha \in \boldsymbol{\mu}_1$, then $g = g' \cdot f$ for some $g' \in \mathcal{O}_L[[X]]$.

(ii) For $h \in \mathcal{O}_L[[X]]$ and $m \geqslant 1$, we have $h \circ f \equiv 0 \pmod{\mathfrak{p}^m} \Longrightarrow h \equiv 0 \pmod{\mathfrak{p}^m}$.

(iii) If $g(X +_f \alpha) = g(X)$ for all $\alpha \in \boldsymbol{\mu}_1$, then $g = h \circ f$ for a unique $h \in \mathcal{O}_L[[X]]$.

Proof. — (i) : For $\alpha \in \boldsymbol{\mu}_1$, 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 $i \geqslant 0$, then $g(X) = (X-\alpha)\cdot\sum_{i=0}^\infty b_i X^i$ in $\mathcal{O}_{L'}[[X]]$. As f is separable (by Proposition 8.1, or Proposition 4.4(i) when char$K = 0$), repeating this, we get $g(X) = f(X) \cdot g'(X)$, and as $g, f \in \mathcal{O}_L[[X]]$, also g' has coefficients in $L \cap \mathcal{O}_{L'} = \mathcal{O}_L$. (ii) : If $m = 1$, then $h \circ f \equiv h(X^q) \pmod{\mathfrak{p}}$ proves the claim. Use induction for $m > 1$. If $h \circ f = \pi^m g$, then by induction $h = \pi^{m-1} \cdot h'$, thus $h' \circ f = \pi g$ but the $m = 1$ case implies $h' \equiv 0 \pmod{\mathfrak{p}}$. (iii) : 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 (i). 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 $g = h \circ f$. Uniqueness follows from (ii), which implies $h \circ f = 0 \Longrightarrow h = 0$. □

Definition 5.6 (Coleman [4], de Shalit [5]) *For $g \in \mathcal{O}_L[[X]]$, coefficients of the product $\prod_{\alpha \in \boldsymbol{\mu}_1} g(X +_f \alpha)$ are $\mathcal{O}_L$-polynomials in the symmetric functions of $\boldsymbol{\mu}_1$, hence they lie in $\mathcal{O}_L$. Therefore by Lemma 5.5(iii), we get a unique $N(g) \in \mathcal{O}_L[[X]]$ satisfying :*

$$N(g) \circ f(X) = \prod_{\alpha \in \boldsymbol{\mu}_1} g(X +_f \alpha). \tag{5.2.1}$$

Clearly $N(g_1 g_2) = N(g_1) N(g_2)$. Also, we set $N^0(g) := g$ and

$$N^m(g) := \left(N^{m-1}(N(g)^{\varphi^{-1}})\right)^{\varphi} \quad (m \geqslant 1).$$

If we write $N = N_f$ (called the Coleman operator*), this means $N^m = N_{f^{\varphi^{m-1}}} \circ \cdots \circ N_{f^\varphi} \circ N_f$.*

Lemma 5.7. — *For $m \geqslant 1$, we have $N^m(g) \circ f_m(X) = \prod_{\alpha \in \boldsymbol{\mu}_m} g(X +_f \alpha)$.*

Proof. — The case $m = 1$ is the definition. Use induction on m. Fix a set C of representatives of $\boldsymbol{\mu}_m / \boldsymbol{\mu}_1$ as $\mathcal{O}$-modules, and extend φ to a $\widetilde{\varphi} \in \mathrm{Gal}(K_x^m / K)$ (Proposition 4.7(i)). Then :

$$\prod_{\alpha \in \boldsymbol{\mu}_m} g(X +_f \alpha) = \prod_{\beta \in C} \prod_{\alpha \in \boldsymbol{\mu}_1} g(X +_f \beta +_f \alpha) = \prod_{\beta \in C} N(g) \circ f(X +_f \beta),$$

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

$$\mathrm{RHS} = \prod_{\alpha \in \boldsymbol{\mu}_{m-1}} N(g)(f(X) +_{f^\varphi} \alpha^{\widetilde{\varphi}}) = \Big(\prod_{\alpha \in \boldsymbol{\mu}_{m-1}} N(g)^{\varphi^{-1}} (f^{\varphi^{-1}}(X) +_f \alpha) \Big)^{\varphi}$$

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

Lemma 5.8. —

(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* $m \geqslant 1$*, 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* $m \geqslant 1$*, 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 (5.2.1) $\equiv N(g)(X^q) \pmod{\mathfrak{p}}$. On the other hand, if we write $L' = K_x^1$, then $\boldsymbol{\mu}_1 \subset \mathfrak{p}_{L'}$, hence $g(X +_f \alpha) \equiv g(X) \pmod{\mathfrak{p}_{L'}}$ for all $\alpha \in \boldsymbol{\mu}_1$. Therefore RHS of (5.2.1) $\equiv g(X)^q \equiv g^{\varphi}(X^q) \pmod{\mathfrak{p}_{L'}}$, 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

$$N(g) \circ f = \prod_{\alpha \in \boldsymbol{\mu}_1} \big(1 + \pi^m h(X +_f \alpha)\big) \equiv \big(1 + \pi^m h(X)\big)^q \pmod{\mathfrak{p}^m \mathfrak{p}_{L'}}$$

$$\equiv 1 + q\pi^m h(X) + \cdots \pi^{mq} h(X)^q \equiv 1 \pmod{\mathfrak{p}^m \mathfrak{p}_{L'}},$$

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 5.5(ii), 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. ☐

Definition 5.9. — *For a finite separable extension K'/K, we denote the image $N_{K'/K}(K'^{\times})$ of the norm map $N_{K'/K} : K'^{\times} \to K^{\times}$ by $N(K'/K)$. For any separable extension E/K, define $N(E/K) := \bigcap_{K'} N(K'/K)$ where K' runs through all the finite extensions in E.*

Proposition 5.10. — $N(K_x^m/K) = (1 + \mathfrak{p}^m) \times \langle x \rangle$ *for all* $m \geqslant 1$.

Proof. — Write $L' = K_x^m$ and take $\alpha \in \boldsymbol{\mu}_m^{\times}$. By Proposition 4.4(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 $N_{L'/K}(\mathcal{O}_{L'}^{\times}) = 1+\mathfrak{p}^m$. First we show $N_{L'/K}(\mathcal{O}_{L'}^{\times}) \subset 1+\mathfrak{p}^m$. By the following Lemma 5.11, any $u \in \mathcal{O}_{L'}^{\times}$ can be written as $u = g(\alpha)$, $g \in \mathcal{O}_L[[X]]^{\times}$. For $i \geqslant 0$, set $u_i := N^i(g)(0)$. Then by Lemma 5.7 we have $u_i = \prod_{\alpha \in \boldsymbol{\mu}_i} g(\alpha)$, hence $N_{L'/L}(u) = \prod_{\alpha \in \boldsymbol{\mu}_m^{\times}} g(\alpha) = u_m/u_{m-1}$. Lemma 5.8(iii) shows that $u_m/u_{m-1}^{\varphi} \in 1 + \mathfrak{p}_L^m$. Hence $N_{L'/K}(u) = N_{L/K}(u_m/u_{m-1}) = N_{L/K}(u_m/u_{m-1}^{\varphi}) \in N_{L/K}(1+\mathfrak{p}_L^m) \subset 1+\mathfrak{p}^m$. The other inclusion (not used in the sequel) is seen as follows : as K_x^m is the fixed field of $\mathrm{Art}_K((1+\mathfrak{p}^m)\times\langle x \rangle)$ by Proposition 5.4, if $x'/x \in 1 + \mathfrak{p}^m$ then $K_x^m = K_{x'}^m$. Therefore $x' \in N(K_{x'}^m/K) = N(K_x^m/K)$ and $1 + \mathfrak{p}^m \subset N(K_x^m/K)$. ☐

Lemma 5.11. — *If L'/L is totally ramified and α 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 $\{1, \alpha, \alpha^2 \ldots, \alpha^{n-1}\}$ is a basis of L' over L. This and (ii) imply $\mathcal{O}_{L'} \subset \mathcal{O}_L[\alpha]$. □

Corollary 5.12. — *If E/L is totally ramified and E contains K_x^{ram}, then $N(E/K) = \langle x\rangle$.*

Proof. — Proposition 5.10 and $\bigcap_{m\geqslant 1}(1+\mathfrak{p}^m) = \{1\}$ imply $N(E/K) \subset N(K_x^{\mathrm{ram}}/K) \subset \langle x\rangle$, and $N(E/K)$ contains an element with valuation $[L : K]$ by the following lemma. □

Lemma 5.13. — *Let $P = P_L := v_L^{-1}(1)$ be the set of all uniformizers of a local field L, and E/L a totally ramified extension. Then $N(E/L)^P := N(E/L) \cap P$ is non-empty.*

Proof. — If L'/L is finite totally ramified, then $N(L'/L)^P \neq \emptyset$ as $N_{L'/L}$ maps $P_{L'}$ into P. For a uniformizer π of L, we have $P = \pi \cdot \mathcal{O}_L^\times = \varprojlim P/(1+\mathfrak{p}_L^m)$, where the quotient is taken by the multiplicative action. As $N_{L'/L}(1+\mathfrak{p}_{L'}^m) \subset 1+\mathfrak{p}_L^m$ for all $m \geqslant 1$, the $N_{L'/L}$ is the $\varprojlim$ of $N_m = N_m^{L'} : P_{L'}/(1+\mathfrak{p}_{L'}^m) \to P_L/(1+\mathfrak{p}_L^m)$. We show $N(L'/L)^P = \varprojlim\big(\mathrm{Im} N_m\big)$ as subsets of P. If $\pi = (\pi_m)_m \in \varprojlim\big(\mathrm{Im} N_m\big)$, then there is $\pi' \in \varprojlim N_m^{-1}(\pi_m)$ as the $\varprojlim$ of non-empty finite sets is non-empty, and $N(\pi') = \pi$. Converse is clear. Now for general E/L, every finite L'/L contained in E is totally ramified, and if $L', L'' \subset E$ then $L'L'' \subset E$ and $\mathrm{Im} N_m^{L'L''} \subset \mathrm{Im} N_m^{L'} \cap \mathrm{Im} N_m^{L''}$. Hence the intersection $\bigcap_{L'} \mathrm{Im} N_m^{L'}$ in the finite set $P/(1+\mathfrak{p}_L^m)$, where L' runs through all finite extensions in E, is non-empty. Thus $\varprojlim\big(\bigcap_{L'} \mathrm{Im} N_m^{L'}\big) \neq \emptyset$, and it is contained in $\varprojlim\big(\mathrm{Im} N_m^{L'}\big) = N(L'/L)^P$ for all L', hence in $N(E/L)^P$. □

5.3. Base change and LCFT for Lubin-Tate extensions

Proposition 5.14. — *For $\sigma \in W(K^{\mathrm{sep}}/K)$ with $v(\sigma) > 0$, let $E_\sigma \subset K^{\mathrm{sep}}$ be its fixed field. Then $N(E_\sigma/K) = \langle \mathrm{Art}^{-1}(\sigma|_{K^{\mathrm{LT}}})\rangle$.*

Proof. — Let $x := \mathrm{Art}^{-1}(\sigma|_{K^{\mathrm{LT}}})$. By Proposition 5.4, we have $K_x^{\mathrm{ram}} \subset E_\sigma$, and $E_\sigma \cap K^{\mathrm{ur}}$ is the unramified extension of K of degree $v(\sigma) = v(x)$. Hence Corollary 5.12 applies. □

THEOREM 5.15. — (Base change) *For a finite separable K'/K, we have $K^{\mathrm{LT}} \subset K'^{\mathrm{LT}}$ and the following commutes, i.e. for all $x' \in K'^{\times}$ we have $\mathrm{Art}_{K'}(x')|_{K^{\mathrm{LT}}} = \mathrm{Art}_K(N_{K'/K}(x'))$.*

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

Proof. — Take $x \in \mathfrak{p}_{K'} \cap K'^{\times}$, and extend $\mathrm{Art}_{K'}(x) \in W(K'^{\mathrm{LT}}/K')$ to $\sigma \in W(K^{\mathrm{sep}}/K')$. By Proposition 5.14, we have $\langle N_{K'/K}(x)\rangle = N_{K'/K}(\langle x\rangle) = N_{K'/K}(N(E_\sigma/K')) = N(E_\sigma/K) = \langle \mathrm{Art}_K^{-1}(\sigma|_{K^{\mathrm{LT}}})\rangle$. As $v_K(\sigma|_{K^{\mathrm{LT}}}) = f(K'/K)v_{K'}(\sigma) = f(K'/K)v_{K'}(x) = v_K(N_{K'/K}(x))$, we obtain $N_{K'/K}(x) = \mathrm{Art}_K^{-1}(\sigma|_{K^{\mathrm{LT}}})$. Therefore $\sigma|_{K^{\mathrm{LT}}} = \mathrm{Art}_K(N_{K'/K}(x))$ depends only on $\sigma|_{K'^{LT}}$, which shows $K^{\mathrm{LT}} \subset K'^{\mathrm{LT}}$ and the commutativity, as $\mathfrak{p}_{K'} \cap K'^{\times}$ generates $K'^{\times}$. □

COROLLARY 5.16. — (LCFT minus Local Kronecker-Weber)

(i) There is a unique homomorphism $\mathrm{Art}_K : K^{\times} \to \mathrm{Gal}(K^{\mathrm{LT}}/K)$ satisfying :

(a) if π is a uniformizer of K, then $\mathrm{Art}_K(\pi)|_{K^{\mathrm{ur}}} = \mathrm{Frob}_K$, and

(b) if K'/K is a Lubin-Tate extension, then $\mathrm{Art}_K(N(K'/K))|_{K'} = \mathrm{id}$.

Moreover, the Art_K is an isomorphism onto $W(K^{\mathrm{LT}}/K) \subset \mathrm{Gal}(K^{\mathrm{LT}}/K)$.

(ii) If K'/K is finite separable, then $K^{\mathrm{LT}} \subset K'^{\mathrm{LT}}$, and $\mathrm{Art}_{K'}(x)|_{K^{\mathrm{LT}}} = \mathrm{Art}_K(N_{K'/K}(x))$ for all $x \in K'^{\times}$. The Art_K induces $K^{\times}/N(K'/K) \xrightarrow{\cong} \mathrm{Gal}((K' \cap K^{\mathrm{LT}})/K)$.

Proof. — (i) : The map Art_K satisfies (a) by definition, and (b) by Theorem 5.15. Conversely, if Art'_K satisfies these, then for any uniformizer π of K, (b) and Proposition 4.4(ii) imply $\mathrm{Art}'_K(\pi)|_{K_\pi^{\mathrm{ram}}} = \mathrm{id}$. This and (a) show $\mathrm{Art}'_K(\pi) = \mathrm{Art}_K(\pi)$ by Proposition 5.4. As $K^{\times}$ is generated by the uniformizers, we get $\mathrm{Art}'_K = \mathrm{Art}_K$. The last claim was seen in Definition 4.10. (ii) : The first part is Theorem 5.15, and Art_K induces $K^{\times}/N(K'/K) \cong W(K^{\mathrm{LT}}/K)/\mathrm{Im}(W(K'^{\mathrm{LT}}/K'))$. This is isomorphic to $\mathrm{Gal}((K' \cap K^{\mathrm{LT}})/K)$, as $W(K^{\mathrm{LT}}/K)$ surjects onto $\mathrm{Gal}((K' \cap K^{\mathrm{LT}})/K)$ and $W(K'^{\mathrm{LT}}/K')$ is the inverse image of $W(K^{\mathrm{LT}}/K)$ under $\mathrm{Gal}(K'^{\mathrm{LT}}/K') \to \mathrm{Gal}(K^{\mathrm{LT}}/K)$. □

Above proof of (i) shows that we only need totally ramified Lubin-Tate extensions for the characterization of Art_K. The classical theorems of LCFT for Lubin-Tate extensions (instead of abelian extensions) follow easily from Corollary 5.16, for example :

(i) For any finite K'/K, we have $N(K'/K) = N((K' \cap K^{\mathrm{LT}})/K))$ and $[K^\times : N(K'/K)] \leqslant [K' : K]$. Equality holds if and only if K'/K is Lubin-Tate.

(ii) If K'/K is finite and K''/K is Lubin-Tate, then $N(K'/K) \subset N(K''/K) \iff K'' \subset K'$. If both are Lubin-Tate, then $N(K''/K)/N(K'/K) \cong \mathrm{Gal}(K'/K'')$ by $\mathrm{Art}_{K'}$.

(iii) If $K', K''/K$ are Lubin-Tate extensions, then :
$N(K'K''/K) = N(K'/K) \cap N(K''/K)$,
$N((K' \cap K'')/K) = N(K'/K)N(K''/K)$.

(iv) (*Existence theorem*) For any finite index subgroup $H \subset K^\times$ containing $1 + \mathfrak{p}^m$ for some m, there is a unique Lubin-Tate extension K'/K such that $N(K'/K) = H$.

6. The Local Kronecker-Weber theorem

We finish the proof of Theorem A by proving the local Kronecker-Weber theorem, i.e. $K^{\mathrm{LT}} = K^{\mathrm{ab}}$. This follows easily from the Hasse-Arf theorem (Gold [7] or Iwasawa [9], §7.4; see also Lubin [10], Rosen [13]). We first prove the Hasse-Arf theorem following Sen [14].

6.1. Ramification groups

Let K'/K be a finite totally ramified Galois extension of local fields, and set $G := \mathrm{Gal}(K'/K)$. For a uniformizer π of K', we have $\mathcal{O}_{K'} = \mathcal{O}[\pi]$ by Lemma 5.11. We write $v := v_{K'}$ and $q = |\mathcal{O}/\mathfrak{p}| = |\mathcal{O}_{K'}/\mathfrak{p}_{K'}|$.

Definition 6.1. — *Let $i(\sigma) := v(\sigma(\pi) - \pi)$, where we set $i(\mathrm{id}) = \infty$. For $n \geqslant 0$, 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 $G_n = \{\mathrm{id}\}$ for sufficiently large n. They are normal subgroups of G, independent of the choice of π, because $G_n = \{\sigma \in G \mid v(\sigma(a) - a) > n$ for all $a \in \mathcal{O}_{K'}\}$ is the kernel of the group homomorphism $G \ni \sigma \longmapsto \sigma|_{\mathcal{O}_{K'}} \bmod \mathfrak{p}_{K'}^{n+1} \in \mathrm{Aut}(\mathcal{O}_{K'}/\mathfrak{p}_{K'}^{n+1})$.*

Proposition 6.2. — *For $n \in \mathbb{Z}_{\geqslant 0}$, we have the following injective group homomorphisms, independent of the choice of π (they show that G is supersoluble) :*

$$\theta_0 : G_0/G_1 \ni \sigma \longmapsto \sigma(\pi)/\pi \mod \mathfrak{p}_{K'} \in (\mathcal{O}_{K'}/\mathfrak{p}_{K'})^\times \cong \mathbb{F}_q^\times,$$

$$\theta_n : G_n/G_{n+1} \ni \sigma \longmapsto (\sigma(\pi)/\pi) - 1 \mod \mathfrak{p}_{K'}^{n+1} \in \mathfrak{p}_{K'}^n/\mathfrak{p}_{K'}^{n+1} \cong \mathbb{F}_q \quad (n \geqslant 1).$$

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 θ_n do not depend on the choice of π. 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 θ_n are group homomorphisms. □

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 $e_0 \mid n$. □

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

Proof. — Replacing α by αx for $x \in K^\times$, we can assume $\alpha \in \mathcal{O}_{K'}$. Let $(\sigma-1)(\alpha) := \sigma(\alpha)-\alpha$. Then $\sigma \in G_1$ implies $v((\sigma-1)^{p-1}(\alpha)) > \cdots > v((\sigma-1)(\alpha)) > v(\alpha)$. The claim follows by $\sum_{i=0}^{p-1}\sigma^i(\alpha) \equiv (\sigma-1)^{p-1}(\alpha) \pmod{p\alpha}$, which follows from $(-1)^i p - 1i \equiv 1 \pmod{p}$. This is seen from $\sum_{i=0}^{p-1} X^i = (X^p-1)/(X-1) = (X-1)^{p-1}$ in $\mathbb{F}_p[X]$. □

LEMMA 6.5. — *Let $\sigma \in G_1$. For each $n \in \mathbb{Z}$, there exists $\alpha \in K'^\times$ such that $v(\alpha) = n$ and $v(\sigma(\alpha)-\alpha) = n + i(\sigma^n)$. Moreover, any $x \in K'^\times$ can be written as a sum $x = \sum_{n=v(x)}^{\infty} x_n$ (see Appendix I) where each x_n satisfies above two properties for n if $x_n \neq 0$.*

Proof. — For the first part, if $n \geqslant 0$, then let $\alpha = \prod_{i=0}^{n-1}\sigma^i(\pi)$ for a uniformizer π 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, α^{-1} satisfies the properties for $-n$. For the second part, note that $C := \{0\} \cup \boldsymbol{\mu}_{q-1}$ is a complete set of representatives for $\mathcal{O}_{K'} \bmod \mathfrak{p}_{K'}$, and σ 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 α_n is the α we constructed above. Thus $x_n := c_n\alpha_n$ has the required properties if $c_n \neq 0$. □

Proposition 6.6 (Sen [14]). — *Let $\sigma \in G_1$, and $|\langle\sigma\rangle| = p^m$ for $m \geqslant 1$ (by Proposition 6.2). Let $H_n := G_n \cap \langle\sigma\rangle$ for $n \geqslant 1$ and $i_j := i(\sigma^{p^j})$ for $j \geqslant 0$ (and $i_j := \infty$ for $j \geqslant m$). Then :*

(i) $i_{j-1} < i_j$ if $j \leqslant m$. Also, $H_n = \langle\sigma^{p^j}\rangle$ if and only if $i_{j-1} \leqslant n < i_j$.

(ii) $i(\sigma^a) = i_{v_p(a)}$ for $a \geqslant 1$, where $v_p := v_{\mathbb{Q}_p}$.

(iii) $i_{j-1} \equiv i_j \pmod{p^j}$, where ∞ is understood to be congruent to any integer.

Proof. — (i) : Lemma 6.4 for $\alpha = \sigma^{p^{j-1}}(\pi) - \pi$ shows $i_{j-1} < i_j$. 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 $\langle\sigma^{p^j}\rangle \supset H_n \Leftrightarrow \langle\sigma^{p^{j-1}}\rangle \not\subset H_n \Leftrightarrow i_{j-1} \leqslant n$. (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 $\sigma^a \in H_{i_j-1} \backslash H_{i_j}$, i.e. $i(\sigma^a) = i_j$. (iii) : We can assume $i_j < \infty$, and use induction on j. The assertion is empty when $j = 0$. Let $j = 1$, and assume the *Inductive Hypothesis* (the assertion of (iii) for $j-1$). We first prove the *Claim : the i_{j-1} and $n+i(\sigma^n)$ for $n \in \mathbb{Z}$, $v_p(n) < j$ are all distinct from each other.* As $v_p(n) \leqslant j-1$, the *Inductive Hypothesis* shows $i(\sigma^n) = i_{v_p(n)} \equiv i_{j-1} \pmod{p^{v_p(n)+1}}$, i.e. $v_p(i_{j-1} - i(\sigma^n)) > v_p(n)$, hence $i_{j-1} \neq n+i(\sigma^n)$. Now assume $n+i(\sigma^n) = n'+i(\sigma^{n'})$. If $v_p(n) \neq v_p(n')$, then $v_p(n-n') = \min\{v_p(n), v_p(n')\}$, but the *Inductive Hypothesis* shows $v_p(i(\sigma^n) - i(\sigma^{n'})) > \min\{v_p(n), v_p(n')\}$, which is impossible. Hence $v_p(n) = v_p(n')$, therefore $i(\sigma^n) = i(\sigma^{n'})$ and $n = n'$. Thus the *Claim* is proven. 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 $v_p(s) = j-1$, to see it leads to contradiction. The first part of Lemma 6.5 for σ^p shows that there is $x \in K'^{\times}$ 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 Lemma 6.5 : $v(\sigma(y_n) - y_n) = n + i(\sigma^n)$ 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 $z_n \neq 0$. The *Claim* shows $v\big(z - \sum_{v_p(n)<j} z_n\big) \leqslant i_{j-1}$. If $v_p(n) \geqslant j$ and $z_n \neq 0$, then $v(z_n) = n + i(\sigma^n) \geqslant n + i_j \geqslant v(y) + i_j > i_{j-1}$, hence $v\big(\sum_{v_p(n)\geqslant j} z_n\big) > i_{j-1}$, a contradiction. □

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

6.2. The Hasse-Arf theorem

Let $G = \mathrm{Gal}(K'/K)$ with K'/K totally ramified as before, and let $G \rhd H$ with $G/H = \mathrm{Gal}(K''/K)$. For $\sigma \in G$, let $\overline{\sigma} = \sigma H \in G/H$ be its image.

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

Proof. — For $\overline{\sigma} = \mathrm{id}$, we understand the equality as $\infty = \infty$. Let $\overline{\sigma} \neq \mathrm{id}$, and take uniformizers π' and π'' of K' and K'' respectively, so that $\mathcal{O}_{K'} = \mathcal{O}[\pi']$ and $\mathcal{O}_{K''} = \mathcal{O}[\pi'']$ by Lemma 5.11. As $i(\overline{\sigma}) = v_{K''}(\overline{\sigma}(\pi'') - \pi'') = \frac{1}{|H|} \cdot v_{K'}(\overline{\sigma}(\pi'') - \pi'')$, if we let $a = \overline{\sigma}(\pi'') - \pi''$ 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 π' over $\mathcal{O}_{K''}$ be $f = \prod_{\tau \in H}(X - \tau(\pi')) \in \mathcal{O}_{K''}[X]$. Applying σ, we get $f^{\overline{\sigma}} = \prod_{\tau \in H}(X - \sigma\tau(\pi'))$, where $f^{\overline{\sigma}} \in \mathcal{O}_{K''}[X]$ is obtained by applying $\overline{\sigma}$ to the coefficients of f. Hence $f^{\overline{\sigma}}(\pi') = \prod_{\tau \in H}(\pi' - \sigma\tau(\pi')) = \pm b$. First we prove $a \mid b$. As $\mathcal{O}_{K''} = \mathcal{O}[\pi'']$, we have $a \mid \overline{\sigma}(x) - x$ for any $x \in \mathcal{O}_{K''}$, hence $a \mid f^{\overline{\sigma}} - f$, therefore $a \mid f^{\overline{\sigma}}(\pi') - f(\pi') = \pm b$. Now we prove $b \mid a$. Write $\pi'' = g(\pi')$ for $g \in \mathcal{O}[X]$. The polynomial $g(X) - \pi'' \in \mathcal{O}_{K''}[X]$ has π' as a root, hence divisible by f in $\mathcal{O}_{K''}[X]$. Applying $\overline{\sigma}$, we have $f^{\overline{\sigma}} \mid g(X) - \overline{\sigma}(\pi'')$ in $\mathcal{O}_{K''}[X]$, hence $g(\pi') - \overline{\sigma}(\pi'') = -a$ is divisible by $f^{\overline{\sigma}}(\pi') = \pm b$. □

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

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

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

(i) *$\phi_G(0) = 0$, $\phi_G(n) = \frac{1}{|G|} \sum_{i=1}^{n} |G_i|$ for $n \in \mathbb{Z}_{\geqslant 1}$.*

(ii) *$\phi_G = \phi_{G/H} \circ \phi_H$ on $\mathbb{R}_{\geqslant 0}$.*

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

(ii) : As $\phi(0)=0$ and ϕ 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 $(|(G/H)_{\phi_H(n)}|/|G/H|)\cdot(|H_n|/|H|) = |G_nH/H||H_n|/|G| = |G_n|/|G|$ by Proposition 6.9 and $G_n/H_n = G_n/(H\cap G_n)\cong G_nH/H$. □

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

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 $n=\sum_{i=0}^{j}n_ip^i$ for some $0\leqslant j\leqslant m-1$ by Corollary 6.7, in which case $\phi_G(n)=\frac{1}{p^m}(n_0\cdot p^m+n_1p\cdot p^{m-1}+\cdots+n_jp^j\cdot p^{m-j})\in\mathbb{Z}_{\geqslant 0}$ 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 $G_nH/H\neq G_{n+1}H/H$. We have $\phi_H(n)\in\mathbb{Z}_{\geqslant 0}$ 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 $\phi_{G/H}(\phi_H(n))\in\mathbb{Z}_{\geqslant 0}$, which is $\phi_G(n)$ by Lemma 6.10(ii). Now when $G\neq G_1$, set $H=G_1$ and $|G/H|=e_0$. As $\phi_{G/H}(n)=n/e_0$ for $n\in\mathbb{R}_{\geqslant 0}$ by definition, by Lemma 6.10(ii) it suffices to show $e_0\mid\phi_H(n)$ when $n\in\mathbb{Z}_{\geqslant 0}$ and $G_n\neq G_{n+1}$ (we know $\phi_H(n)\in\mathbb{Z}_{\geqslant 0}$). If $n=0$ then $\phi_H(0)=0$. Let $n>0$. For any $i\in\mathbb{Z}_{\geqslant 1}$ (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). □

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

Corollary 6.13. —

(i) If $G\rhd H$, then $G^mH/H=(G/H)^m$ for all $m\in\mathbb{R}_{\geqslant 0}$.

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

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

Proof. — (i) : By Proposition 6.9 and Lemma 6.10(ii), we compute $G^mH/H = G_{\phi_G^{-1}(m)}H/H = (G/H)_{\phi_H(\phi_G^{-1}(m))} = (G/H)_{\phi_{G/H}^{-1}(m)} = (G/H)^m$.

(ii) : If $G = \mathrm{Gal}(K'K''/K)$ and $G/H = \mathrm{Gal}(K''/K)$, then $G^m H/H = (G/H)^m = \{\mathrm{id}\}$ shows $G^m \subset H = \mathrm{Gal}(K'K''/K'')$. Similarly $G^m \subset \mathrm{Gal}(K'K''/K')$, hence $G^m = \{\mathrm{id}\}$. (iii) : If $n-1 < \phi_G^{-1}(m) \leqslant n$ for $n \in \mathbb{Z}_{\geqslant 0}$, then $G^m = G_n$. Consider G_i for integers $1 \leqslant i \leqslant n$. Then, by Theorem 6.11, $G_{i-1} \neq G_i$ can only happen when $\phi_G(i-1) \in \mathbb{Z}$, and as $0 \leqslant \phi_G(i-1) \leqslant \phi_G(n-1) < m$, 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 $i>1$. □

6.3. The Local Kronecker-Weber theorem

Proposition 6.14. — *Let $x \in K^\times$ with $v(x) = n > 0$. Let $L = K_n$ and K_x^m as in Definition 5.3. Then we have $\mathrm{Gal}(K_x^m/L)^m = \{\mathrm{id}\}$ for all $m \geqslant 1$ (see Definition 6.12).*

Proof. — Let $K_x^m = L_f^m$ and $\alpha \in \boldsymbol{\mu}_{f,m}^\times$. For $\sigma \in \mathrm{Gal}(K_x^m/L) \setminus \{\mathrm{id}\}$, we have $i(\sigma) = v(\sigma(\alpha)-\alpha)$ by Proposition 4.4(ii), where $v = v_{K_x^m}$. If $\rho_{f,m}(\sigma) = u \bmod \mathfrak{p}^m \in (\mathcal{O}/\mathfrak{p}^m)^\times$ (see Proposition 4.4(iii)), then $\sigma(\alpha) = [u]_f(\alpha)$. For $\sigma \neq \mathrm{id}$, set $\beta := [u-1]_f(\alpha)$. If $v_K(u-1) = i$ for $0 \leqslant i < m$, then $\beta \in \boldsymbol{\mu}_{f,m-i}^\times$ by Lemma 4.3(ii). Hence β is a uniformizer of K_x^{m-i} by Proposition 4.4(ii), which shows $v(\beta) = q^i$. Now $\sigma(\alpha) = [u]_f(\alpha) = \alpha +_f \beta \equiv \alpha + \beta \pmod{\alpha\beta}$, hence $i(\sigma) = v(\sigma(\alpha)-\alpha) = v(\beta) = q^i$. Thus for $G = \mathrm{Gal}(K_x^m/L)$ and $1 \leqslant i \leqslant m$, we have $|G_n| = |\rho_{f,m}^{-1}(1+\mathfrak{p}^i)| = q^{m-i}$ for $q^{i-1}-1 < n \leqslant q^i - 1$. Thus $\phi_G(q^m-1) = \frac{1}{|G|}\sum_{i=1}^{q^m-1}|G_i| = \frac{1}{(q-1)q^{m-1}}\left(\sum_{i=1}^m (q^i - q^{i-1})\cdot q^{m-i}\right) = m$ and $G^m = G_{q^m-1} = \{\mathrm{id}\}$. □

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

Proof. — Take a $\sigma \in W(K^{\mathrm{LT}}/K)$ with $v(\sigma) = n > 0$, and let $L = K_n$. Extend σ arbitrarily to $\sigma \in W(K^{\mathrm{ab}}/K)$, and let $E_\sigma \subset K^{\mathrm{ab}}$ be its fixed field. Then $E_\sigma \cap K^{\mathrm{ur}} = L$ and E_σ/L is totally ramified Galois. Now $\mathrm{Gal}(K^{\mathrm{ab}}/E_\sigma) \cong \widehat{\mathbb{Z}}$ with $\sigma \mapsto 1$ by the definition of E_σ. On the other hand, $\mathrm{Gal}(K^{\mathrm{ur}}E_\sigma/E_\sigma) \cong \mathrm{Gal}(K^{\mathrm{ur}}/L) \cong \widehat{\mathbb{Z}}$ by $\sigma \mapsto 1$, as $\sigma|_{K^{\mathrm{ur}}} = \mathrm{Frob}_L$. Therefore $\mathrm{Gal}(K^{\mathrm{ab}}/E_\sigma) \cong \mathrm{Gal}(K^{\mathrm{ur}}E_\sigma/E_\sigma)$, i.e. $K^{\mathrm{ab}} = K^{\mathrm{ur}}E_\sigma$. Now set $x := \mathrm{Art}_K^{-1}(\sigma)$. Then $K_x^{\mathrm{ram}} \subset E_\sigma$ by Proposition 5.4. As $K^{\mathrm{LT}} = K^{\mathrm{ur}}K_x^{\mathrm{ram}}$, it suffices to show $E_\sigma \subset K_x^{\mathrm{ram}}$. Let K'/L be any finite Galois extension contained in E_σ. It is totally ramified, and $\mathrm{Gal}(K'/L)^m = \{\mathrm{id}\}$ for a large m. Then we have $\mathrm{Gal}(K'K_x^m/L)^m = \{\mathrm{id}\}$ by Proposition 6.14 and Corollary 6.13(ii), hence $[K'K_x^m : L] \mid (q-1)q^{m-1} = [K_x^m : L]$ by Corollary 6.13(iii), thus $K' \subset K_x^m$. □

7. Appendix I : Basic facts on DVR

Here we gather some facts on DVR that are used in this article. The proofs omitted here can be found in Atiyah-Macdonald [1] and the Chapters I, II of Serre [15]. A ring A is called a *discrete valuation ring (DVR)* if it is a local ring (i.e. has a unique maximal ideal), a PID and not a field. Let A be a DVR with the maximal ideal P, and let K be its fraction field. A generator of P is called a *uniformizer* of A. Each uniformizer π gives a following isomorphism of abelian groups :

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

The second projection (*valuation*) $v_K : K^\times \to \mathbb{Z}$ does not depend on π, and setting $v_K(0) := \infty$, we have $A = \{x \in K \mid v_K(x) \geqslant 0\}$ 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 $K = \mathrm{Frac}(A)$, 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 $A \to \widehat{A}$ is always injective (hence $K \subset \widehat{K}$), and if it is an isomorphism we call A a *complete discrete valuation ring (CDVR)*. For example, the *ring of p-adic integers* $\mathbb{Z}_p := \varprojlim \mathbb{Z}/(p^m)$ is a CDVR with (p) as its maximal ideal, and its fraction field $\mathbb{Q}_p$ is the *p-adic field*. A completion of a DVR is a CDVR, and $A/P^m \overset{\cong}{\longrightarrow} \widehat{A}/\widehat{P}^m$. If A is a DVR, choosing a complete set of representatives C for A mod P and elements $x_n \in A$ with $v(x_n) = n$ for all $n \geqslant 0$, we can write any element of $\widehat{A} = \varprojlim A/P^m$ 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 π, this is called a π-*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 $y + \sum_{v(x) \leqslant n < 0} c_n x_n$ for some $y \in \widehat{A}$, hence as $x = \sum_{n=v(x)}^{\infty} c_n x_n$.

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 coefficients in A to get $F(x_1, \dots, x_n) \in A$. This is defined using $A[[X_1, \dots, X_n]] \cong \varprojlim_m \big(A[X_1, \dots, X_n]/(\deg m)\big)$ 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 $L = \mathrm{Frac}(B)$. 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*, i.e. 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 $Q_1, \ldots, Q_g$ are all the maximal ideals of B. Let $\widehat{B}_i := \varprojlim_m B/Q_i^m$ for $1 \leqslant i \leqslant g$. As B is a finite free A-module, the functor $B \otimes_A$ 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 $L \otimes_K \widehat{K} \cong L \otimes_K (K \otimes_A \widehat{A}) \cong L \otimes_B (B \otimes_A \widehat{A}) \cong L \otimes_B \widehat{B} \cong \widehat{L}$. Now let $K' := L \cap \widehat{K}$ and $[K' : K] = m$. As K'/K is separable, let $K' \cong K[X]/(f)$ with $\deg f = m$. Assume $m > 1$. As f has a root in $K' \subset L$, we have $L \otimes_K K' \cong L[X]/(f) \cong L \times L'$ with an L-algebra L'; but then $\widehat{L} \cong L \otimes_K \widehat{K} \cong (L \otimes_K K') \otimes_{K'} \widehat{K} \cong (L \times L') \otimes_{K'} \widehat{K} \cong (L \otimes_{K'} \widehat{K}) \times (L' \otimes_{K'} \widehat{K})$, a contradiction because $\widehat{L}$ is a field. □

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 $n = ef$. Assume moreover that L/K is Galois and k_P is perfect. We say L/K is *unramified* if $e = 1$ and *totally ramified* when $f = 1$. An element of $\mathrm{Gal}(L/K)$ induces an automorphism of B which maps Q onto itself, hence we have a group homomorphism :

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

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

Proposition 7.2. — *Let $L = K(\boldsymbol{\mu}_n)$ (and $g = 1$). If* $\mathrm{char} k_P \nmid n$*, then L/K is unramified.*

Proof. — We show that the above homomorphism is injective. As any element of $\mathrm{Gal}(K(\boldsymbol{\mu}_n)/K)$ is determined by the image of a generator $\zeta \in B^\times$ of $\boldsymbol{\mu}_n$, 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 $1 \leqslant i \leqslant n-1$. 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 $\prod_{i=1}^{n-1}(1 - \overline{\zeta^i}) \neq 0$ in the field k_Q, hence $\zeta^i - 1 \notin Q$. □

Proof of Lemma 2.3. — ($\Leftarrow$) 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 $\boldsymbol{\mu}_n$ in $k = \mathcal{O}/\mathfrak{p}$, take its representative $\zeta_1 \in \mathcal{O}$. As $\mathcal{O} = \varprojlim \mathcal{O}/\mathfrak{p}^m$, it is enough to construct $\zeta_m \in \mathcal{O}$ for each $m \geqslant 1$ 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 ζ_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 $\zeta_{m+1}^n \equiv \zeta_m^n + n\zeta_m^{n-1}\beta\pi^m \equiv 1 + (\alpha + n\zeta_m^{n-1}\beta)\pi^m \pmod{\mathfrak{p}^{m+1}}$ to be $\equiv 1 \bmod \mathfrak{p}^{m+1}$, hence $\beta = -\alpha/n\zeta_m^{n-1}$ will do. □

8. Appendix II : Separability of f_m

Here we prove the separability of f_m of Definition 4.1 directly. It is used in the proof of Lemma 4.3(i) only when $\mathrm{char} K = p$. On the other hand, it follows from Proposition 4.4(i) when $\mathrm{char}\, K = 0$.

Proposition 8.1. — *For $\forall m \geqslant 0$, $f_m \in \mathcal{O}_L[X]$ is separable.*

Proof. — Lemma 8.3 will show that $f_m(\alpha) = 0 \implies f'_m(\alpha) \neq 0$ for all $\alpha \in \overline{L}$. □

Lemma 8.2. — *Let $\mathcal{O}'$ be an $\mathcal{O}_L$-algebra, and $f \in \mathcal{O}_L[X]$ as above.*

(i) Let $\mathcal{O}'$ be a domain and $\alpha \in \mathcal{O}'$. If $\alpha \notin \mathcal{O}'^\times$, then $f'(\alpha) \neq 0$.

(ii) Let $\mathcal{O}'$ be a domain and integral over $\mathcal{O}_L$, and $f(\alpha) = \beta$ for $\alpha, \beta \in \mathcal{O}'$. If $\alpha \in \mathcal{O}'^\times$, then (a) $\beta \neq 0$, and (b) if $\beta \mid \pi$ in $\mathcal{O}'$, then $\beta \in \mathcal{O}'^\times$.

Proof. — (i) : As $\pi \mid q$ in $\mathcal{O}$, we have $f'(X) = \pi(1 + Xg(X))$ with $g \in \mathcal{O}_L[X]$, hence if $\alpha \notin \mathcal{O}'^\times$, then $1 + \alpha g(\alpha) \neq 0$ and $f'(\alpha) \neq 0$. (ii) : As $\beta = f(\alpha) = \alpha^n + \pi g(\alpha)$ with $g \in \mathcal{O}_L[X]$, we have $\beta - \pi g(\alpha) \in \mathcal{O}'^\times$ if $\alpha \in \mathcal{O}'^\times$. As $\pi \notin \mathcal{O}'^\times$ because $\mathcal{O}_L$ is integrally closed, we have $\beta \neq 0$. If $\pi = \beta\beta'$, then $\beta(1 - \beta' g(\alpha)) \in \mathcal{O}'^\times$, hence $\beta \in \mathcal{O}'^\times$. □

LEMMA 8.3. — *Let $\alpha \in \overline{L}$, and let $\mathcal{O}_L[\alpha]$ be the $\mathcal{O}_L$-subalgebra of $\overline{L}$ generated by α.*

(i) If $f_i(\alpha) \notin \mathcal{O}_L[\alpha]^\times$ for all $0 \leqslant i \leqslant m-1$, then $f'_m(\alpha) \neq 0$.

(ii) If $f_m(\alpha) = 0$, then $f_i(\alpha) \notin \mathcal{O}_L[\alpha]^\times$ for all $0 \leqslant i \leqslant m-1$.

Proof. — (i) : The claim is empty when $m = 0$ as $f'_0(X) = 1$. We prove by induction on m : assume it is true for $m-1$. As $f_{m-1}(\alpha) \notin \mathcal{O}[\alpha]^\times$, by Lemma 8.2(i), we have $(f^{\varphi^{m-1}})'(f_{m-1}(\alpha)) \neq 0$. By the induction hypothesis, we have $f'_{m-1}(\alpha) \neq 0$. Hence $f'_m(\alpha) \neq 0$. (ii) : If $f_i(\alpha) = 0$, then $f_j(\alpha) = 0$ for $\forall j \geqslant i$, so we can assume $f_i(\alpha) \neq 0$ for $0 \leqslant i \leqslant m-1$. Then we have $\alpha \mid f(\alpha) \mid \cdots \mid f_{m-1}(\alpha) \mid \pi^{\varphi^{m-1}}$ in $\mathcal{O}[\alpha]$, which is finite, hence integral, over $\mathcal{O}$, as α is a root of a monic $f_m \in \mathcal{O}_L[X]$. Now assume $f_i(\alpha) \in \mathcal{O}[\alpha]^\times$ for some i. If $i \neq m-1$, then $f_{i+1}(\alpha) \mid \pi$, hence $f_{i+1}(\alpha) \in \mathcal{O}[\alpha]^\times$ by Lemma 8.2(ii). Therefore $f_{m-1}(\alpha) \in \mathcal{O}[\alpha]^\times$, but then $f_m(\alpha) \neq 0$ by Lemma 8.2(ii), a contradiction. □

9. Remarks on the literature

The "relative" Lubin-Tate groups treated in §3, §4 and §5 are due to de Shalit [5], although proofs are omitted there. The exposition is based on Iwasawa [9], with two notable differences. Firstly, in Iwasawa [9] the norm operator N is treated 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. Secondly, we separated the "geometric" (§3, §4) and "arithmetic" (§5) parts of the theory by defining the Artin map through an arbitrary Lubin-Tate group over $\widehat{\mathcal{O}}$, in the spirit of Carayol [2]. In §6 we combined Sen [14] with the standard material from Serre [15], Chapter IV. 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. Needless to say, there are many other important approaches to local class field theory, see e.g. [3], [6], [8], [12], [15], and [16].

Acknowledgments. — The author thanks his former fellow students at Harvard University, especially Jay Pottharst, who read the first draft and gave valuable comments. The revision of this paper was helped by the careful reading of Brian Conrad and suggestions by the referee. Ideas for simplification came through giving a course at the University of Cambridge in Fall

2007, and the author is grateful to all who attended the course. This work was partially supported by the EPSRC grant on Zeta Functions from the University of Nottingham, during the author's stay at Nottingham in the summer of 2005. The author was supported by the Society of Fellows at Harvard University and the Clay Mathematics Institute during the revision period.

Bibliography

[1] Atiyah (M.F.), Macdonald (I.G.). — *Introduction to commutative algebra*, Addison-Wesley, (1969).

[2] Carayol (H.). — *Non-abelian Lubin-Tate theory*, in : *Automorphic Forms, Shimura Varieties, and L-functions* (Academic Press, 1990), p. 15-39.

[3] Cassels (J.W.S.). — *Local Fields*, London Mathematical Society Student Texts 3, Cambridge Univ. Press, (1986).

[4] Coleman (R.). — *Division values in local fields*, Invent. Math. 53, p. 91-116 (1979).

[5] de Shalit (E.). — *Relative Lubin-Tate groups*, Proc. Amer. Math. Soc. 95, p. 1-4 (1985).

[6] Fesenko (I.B.), Vostokov (S.V.). — *Local Fields and their Extensions*, 2nd ed., Translations of Mathematical Monographs 121, AMS, (2002).

[7] Gold (R.). — *Local class field theory via Lubin-Tate groups*, Indiana Univ. Math. J. 30, p. 795-798 (1981).

[8] Hazewinkel (M.). — *Local class field theory is easy*, Advances in Math. 18-2, p. 148-181 (1975).

[9] Iwasawa (K.). — *Local Class Field Theory*, Oxford Univ. Press, (1986).

[10] Lubin (J.). — *The local Kronecker-Weber theorem*, Trans. Amer. Math. Soc. 267-1, p. 133-138 (1981).

[11] Lubin (J.), Tate (J.). — *Formal complex multiplication in local fields*, Ann. Math. 81, p. 380-387 (1965).

[12] Neukirch (J.). — *Class Field Theory*, Grundlehren der Mathematischen Wissenschaften 280, Springer-Verlag, (1986).

[13] Rosen (M.). — *An elementary proof of the Kronecker-Weber theorem*, Trans. Amer. Math. Soc. 265-2, p. 599-605. (1981)

[14] Sen (S.). — *On automorphisms of local fields*, Ann. Math. 90 (1969), p. 33-46.

[15] Serre (J.-P.). — *Corps Locaux*, 2nd ed., Hermann, 1968. (English translation : *Local fields*, Graduate Texts in Mathematics 67, Springer-Verlag, (1979).)

[16] Serre (J.-P.). — *Local class field theory*, in : *Algebraic Number Theory* (Thompson, 1967), p. 128-161.