Local class field theory

Mehdi Hachimi and Truong Tuan Nghia

May 31, 2024

Abstract

In classical analysis, we construct the set of real number by completing the metric $(\mathbb{Q}, |\cdot|_\infty)$ with euclidean multiplicative norm. Similarly, in number theory, we can consider the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ with respect to a multiplicative norm given by a prime number p.

This report introduces some properties of these objects, in the more general set up of valuation fields and especially local fields, i.e the finite extension of $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$.

In addition, via Lubin-Tate theory, we construct an extension K^{LT} of a local field K, which is actually the maximal abelian extension of K. By this description, we study the Galois group of this extension by constructing an explicit homomorphism

$$\mathrm{Art}_K : K^\times \to \mathrm{Gal}\left(K^{\mathrm{LT}}|K\right)$$

which is an isomorphism onto the Weil group $\mathrm{W}\left(K^{\mathrm{ab}}|K\right)$.

We are grateful to our supervisor Nataniel Marquis, who motivated us to study a wide range of knowledge.

Contents

1 Introduction

Analysis tools allow us to understand the solutions of a polynomial with rational coefficients in $\mathbb{R}$, but it seems hard to come back to $\mathbb{Q}$, so we need the p-adic numbers. To focus on a prime p and allow p-adic analysis, Kurt Hensel invented the p-adic number fields, more precisely $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ with respect to the valuation given by a prime p (Subsection 2.3).

Definition 1.1. The function $v_p : \mathbb{Q} \to \mathbb{Z}$, sending 0 to $v_p(0) = \infty$ and an integer a to $v_p(a) = k$, a maximal integer such that $p^k \mid a$, and a rational a/b to

$$v_p(a/b) = v_p(a) - v_p(b)$$

is a valuation on $\mathbb{Q}$. We denote by $|\cdot|_p$ the norm generated by v_p.

We will see from Theorem 2.17 that $\mathbb{Q}_p$ is constructed as the quotient of the ring of Cauchy sequences on $\left(\mathbb{Q}, |\cdot|_p\right)$ by its maximal ideal of sequences converging to 0. The p-adic norm and valuation extend uniquely to $\mathbb{Q}_p$ and endow it with a topological ring structure. Denote by $\mathbb{Z}_p$ the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$. We have

Proposition 1.2.

1. The value group of $\mathbb{Q}_p$ equals to that of $\mathbb{Q}$ and $\mathbb{Q}_p$ is complete.
2. We have $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\} = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\}$.
3. $\mathbb{Z}_p$ is a PID and its ideals are in the form $p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq n\}$ for some $n \in \mathbb{N}$.
4. We have the canonical topological ring isomorphisms $\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ sending $[x] \mapsto [x]$ which induce an isomorphism
$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$$
sending $(a_n)_{n\in\mathbb{N}} \mapsto \lim a_n$.
5. The series $\sum a_n$ in $\mathbb{Q}_p$ converges if and only if $\lim a_n = 0$.
6. Every element $a \in \mathbb{Q}_p$ can be written uniquely as
$$a = p^\alpha \left(\sum_{n=0}^{\infty} b_n p^n \right)$$
where $\alpha = v_p(a)$, $b_i \in \{0, \ldots, p-1\}$ and $b_0 > 0$.

The study of $\mathbb{Q}_p$ and its algebraic extensions fits in the general theory of discretely valued fields and precisely of local fields. Our goal is to understand the smooth characters of absolute Galois group Gal_K of a local field K, i.e. its abelianisation. By Lubin-Tate theory, we define an abelian extension $K^{\mathrm{LT}}|K$, and construct explicitly the Artin map

$$\mathrm{Art}_K : K^\times \longrightarrow \mathrm{Gal}\left(K^{\mathrm{LT}}|K\right)$$

which is an isomorphism onto the Weil group $\mathrm{W}\left(K^{\mathrm{LT}}|K\right)$. It turns out that this Lubin-Tate extension is indeed the maximal abelian extension, hence Art_K extends to the isomorphism from the profinite completion of $K^\times$ to $\mathrm{Gal}\left(K^{\mathrm{ab}}|K\right)$.
The knowledge of Galois theory, finite fields and infinity Galois extension can be found in [1]

2 Valuations and completions

In this section, we generalize the properties of $\mathbb{Q}_p$ presented in the introduction. We mainly follow [2], Chapter 2, Sections 3 and 4.

2.1 Norms and valuations

Definition 2.1. A (multiplicative) norm of a field K is a function $|\cdot| : K \to \mathbb{R}_+$ such that

(i) $|x| = 0$ if and only if $x = 0$,

(ii) For all $x, y \in K$, $|xy| = |x|\,|y|$,

(iii) For all $x, y \in K$, $|x + y| \leq |x| + |y|$,

(iv) $|.|$ is not the trivial function satisfying $|x| = 1$ for all $x \neq 0$.

$(K, |\cdot|)$ is called a *valued field*.

If $|\cdot|$ is a norm of a field K, then K is endowed with a metric by $d(x, y) = |x - y|$.

Definition 2.2. We say that two norms are equivalent if they define the same topology on K.

We have the following criterion for equivalent norms:

Proposition 2.3. Let $|\cdot|_1$ and $|\cdot|_2$ be two norms on a field K. The following are equivalent:

- The two norms $|\cdot|_1$ and $|\cdot|_2$ are equivalent.
- There exists $s > 0$ such that $|\cdot|_1 = |\cdot|_2^s$.
- The open unit ball induced by the first norm is a subset of the open unit ball induced by the second, i.e
$$\{x \in K,\, |x|_1 < 1\} \subseteq \{x \in K,\, |x|_2 < 1\}.$$

Generalising the p-adic norm, we have the following definition.

Definition 2.4. A norm $|\cdot|$ is called nonarchimedean if $\{|n| \mid n \in \mathbb{N}\}$ is bounded in $\mathbb{R}_+$. Otherwise it is called archimedean.

We have the following properties:

Proposition 2.5. Let $(K, |\cdot|)$ be a valued field.

1. The norm $|\cdot|$ is nonarchimedean if and only if it satisfies the strong triangular inequality
$$|x + y| \leq \max\{|x|\,, |y|\}.$$
2. If $|\cdot|$ is nonarchimedean and $|x| < |y|$, then $|x + y| = |y|$.
3. If $|\cdot|$ is nonarchimedean, every point x of a ball $B\,(0,\, 1) = \{y \in K,\, |y| < 1\}$ is the center of this ball, i.e $B(0,\, 1) = B(x,\, 1)$.

We define now the valuation on an arbitrary field K:

Definition 2.6. A valuation on K is a function $v : K \to \mathbb{R} \cup \{\infty\}$ satisfying the following properties:

1. $v(x) = \infty$ if and only if $x = 0$,
2. For all $x, y \in K$, $v(xy) = v(x) + v(y)$,
3. For all $x, y \in K$, $v(x + y) \geq \min\{v(x), v(y)\}$,
4. v is not the trivial function satisfying $v(x) = 0$ for $x \neq 0$ and $v(0) = \infty$.

The set $v\,(K^\times)$ is called the value group of K.

Observe that the notations for nonarchimedean norms can be translated to those of valuation as follow.

Remark 2.7. 1. If $|\cdot|$ is a nonarchimedean norm of the field K and a is a positive real number larger than 1, we can define a valuation

$$v(x) = -\log_a |x|\,,\ x \neq 0, \quad v(0) = \infty.$$

Similarly, by taking the exponential, we can define a nonarchimedean norm by a valuation.

2. Two valuations v_1 and v_2 are called equivalent if $v_1 = sv_2$ for some real number $s > 0$.

Example 2.8. We give some important examples of valuations on $\mathbb{Q}$ and $K(t)$.

1. Let p be a prime number, $(\mathbb{Q},\, v_p)$ in Definition 1.1 is a valuation.
2. Let K be a field. On $K(t)$, we define several nonarchimedean norms as below.
   - If $f(X) \in K[X]$ is irreducible, a map sending g to $v_f(g)$, the exponent of f in the factorisation of g is a valuation.
   - The map sending $g \in K(X)$ to $\deg(g)$ defines a valuation v_∞.

The following proposition classifies all the classes of valuations on $\mathbb{Q}$. Actually, they are $|\cdot|_p$ and $|\cdot|_\infty$.

Proposition 2.9. Every norm of $\mathbb{Q}$ is equivalent to one of the norms $|\cdot|_p$ or $|\cdot|_\infty$, where $|\cdot|_\infty$ is the usual absolute value on $\mathbb{Q}$.

Now, we introduce some notations for valuations and nonarchimedean norms.

Proposition 2.10. Let $(K,\, v)$ be a field with valuation v.

1. The ring of integers (valuation ring) of K is $\mathcal{O} = \{x \in K \,|\, v(x) \geq 0\} = \{x \in K \,|\, |x| \leq 1\}$. The ring $\mathcal{O}$ is an integrally closed domain and $K = \mathrm{Frac}\,(\mathcal{O})$.
2. The set $\mathfrak{p} = \{x \in K \,|\, v(x) > 0\} = \{x \in K \,|\, |x| < 1\} = \{x \in A \,|\, x^{-1} \notin A\}$ is the unique maximal ideal of $\mathcal{O}$ and $\mathcal{O}^\times = \mathcal{O} \setminus \mathfrak{p}$. The quotient $\mathcal{O}/\mathfrak{p}$ is a field called residue class field of K.

2.2 Discrete valuations

Definition 2.11. A valuation is called *discrete* if it admits a smallest positive value s. In this case, $v\,(K^\times) = s\mathbb{Z}$. It is called normalized if $s = 1$.

Remark 2.12. Let v be a discrete valuation on K, and fix $v(K^\times) = s\mathbb{Z}$. Dividing by s, we may always pass to a normalized valuation without changing the invariants $\mathcal{O}, \mathcal{O}^\times$ and $\mathfrak{p}$. Any element π such that $v(\pi) = 1$ is called a uniformizer.

We know that $\mathbb{Q}$ and $\mathbb{Q}_p$ are discretely valued fields, generalising the properties of Proposition 1.2. Let $(K,\, v)$ be a valued field with v a discrete normalized valuation, then

Proposition 2.13. 1. The unit ball $\mathfrak{p} = B(0,\, 1) = \{x \in K \,|\, v(x) \geq 1/2\}$ is closed and open.

2. The quotient topology on $\mathcal{O}/\mathfrak{p}^n$ is discrete, because $\mathfrak{p}^n$ is open and close.
3. The topology on K is totally disconnected.

Example 2.14. All the valuations introduced in Example 2.8 are discrete.

1. For $(\mathbb{Q},\, v_p)$, one has $v_p\,(a/b)$ is an integer, $\mathcal{O} = \{\frac{a}{b} \,|\, v_p(a) \geq v_p(b)\}$ and $\kappa \cong \mathbb{F}_p$.
2. For $(K(X),\, v_\infty)$, the ring of integers is all fractions with non positive degree and the residue class field is isomorphic to K.
3. For $(K(X),\, v_f)$, where f is an irreducible polynomial of $K[X]$, the ring of integers and residue class field are $\mathcal{O} = \left\{ \dfrac{a(X)}{b(X)} \mid \gcd(a,\, b) = \gcd(b,\, f) = 1 \right\}$ and $\kappa \cong K[X]/(f)$ respectively.

We have the following properties for

Proposition 2.15. Let $(K,\, v)$ be a normalized discrete valuation field and π be a uniformizer.

1. Every element $x \in K^\times$ admits a unique representation $x = u\pi^m$ where $u \in \mathcal{O}^\times$ and $m \in \mathbb{Z}$.
2. The ring $\mathcal{O}$ is PID and its ideals are in the form $\mathfrak{p}^n = (\pi^n) = \{x \in \mathcal{O} \,|\, v(x) \geq n\}$.
3. There is a canonical isomorphism $\mathcal{O}/\mathfrak{p} \cong \mathfrak{p}^n/\mathfrak{p}^{n+1}$ sending $[x]$ to $[\pi^n x]$.
4. The chain of ideals $\mathcal{O} \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \ldots$ forms a basis of neighborhoods of 0.
5. Denote by $U^{(n)} = 1 + \mathfrak{p}^n$ for $n \in \mathbb{N}$ then $\mathcal{O}^\times/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^{\mathfrak{n}})^\times$.
6. The chain of subgroups $U^{(0)} \supseteq U^{(1)} \supseteq \ldots$ forms a basis of neighbourhoods of 1.

2.3 Completions

Definition 2.16. A valued field $(K,\, |\cdot|)$ is complete if every Cauchy sequence converges.

Similar to the way construct $\mathbb{R}$ from $\mathbb{Q}$, we complete an arbitrary valued field as below.

Theorem 2.17. For every valued field $(K,\, |\cdot|)$, there exists a unique up to isomorphism complete valued field $\left(\widehat{K},\, |\cdot|\right)$ such that K is a dense subspace of $\widehat{K}$.

Proof. Let R be the ring of all Cauchy sequences of $(K, |.|)$ and its maximal ideal $\mathfrak{m}$ of all sequences converging to 0, we define $\widehat{K} = R/\mathfrak{m}$. We have that K embeds into $\widehat{K}$ by sending every $a \in K$ to the class of the Cauchy sequence $(a,\, a,\, a, \ldots)$. The norm of the element $(a_1,\, a_2, \ldots,\, a_n, \ldots)$ is given by

$$|(a_1,\, a_2, \ldots)| = \lim_{n\to\infty} |a_n| \,.$$

The completeness and uniqueness can be proved similar to the case of $\mathbb{Q}$ and $\mathbb{R}$. □

The following theorem, named after Ostrowski, allows us to focus on nonarchimedean norms.

Theorem 2.18 (Ostrowski)**.** Let K be a field which is complete with respect to an archimedean valuation $|\cdot|$. Then there is an isomorphism σ from K onto $\mathbb{R}$ or $\mathbb{C}$ and $s \in (0, 1]$ satisfying $|a| = |\sigma a|^s$ for all $a \in K$.

We have the following properties for the completion of a valued field.

Proposition 2.19. Let $(K,\, v)$ be a valued field with valuation v.

1. The valuation v uniquely extends to $\widehat{v}$ on $\widehat{K}$ and the value group of $\widehat{K}$ equals to that of K. In particular, if v is discrete, so is $\widehat{v}$.
2. Let $(\mathcal{O},\, \mathfrak{p})$ and $\left(\widehat{\mathcal{O}},\, \widehat{\mathfrak{p}}\right)$ be the valuation rings of K and $\widehat{K}$. Thus $\widehat{\mathcal{O}}$ is the closure of $\mathcal{O}$ in $\widehat{K}$ and there is a canonical isomorphism $\mathcal{O}/\mathfrak{p} \to \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$ sending $[x]$ to $[x]$.
3. The series $\sum a_n$ in $\widehat{K}$ converges if and only if $\lim a_n = 0$.

Propositions 2.19 and 2.15 generalize Proposition 1.2. Now, we generalize the $p-$adic expansion to the case of an arbitrary discrete valuation v of a field K.

Proposition 2.20. Let $R \subseteq \mathcal{O}$ be a system of representatives for $\kappa = \mathcal{O}/\mathfrak{p}$ such that $0 \in R$, and let $\pi \in \mathcal{O}$ be a uniformizer. Then every $x \in \widehat{K}^\times$ admits a unique representation as a convergent series

$$x = \pi^m \left(\sum_{n=0}^{+\infty} a_n \pi^n \right)$$

where $a_n \in R$, $a_0 \neq 0$ and $m \in \mathbb{Z}$.

Proof. Let $x = \pi^m u$ with $u \in \widehat{\mathcal{O}}^\times$. By proposition 2.19, we have $\mathcal{O}/\mathfrak{p} \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$, hence the class $[u] \in \mathcal{O}/\mathfrak{p}$ has a unique non zero representative $a_0 \in R$. Write $u = a_0 + \pi b_1$ for some $b_1 \in \widehat{\mathcal{O}}$ (recall that $\widehat{\mathfrak{p}} = \pi\widehat{\mathcal{O}}$). Assume that $a_0, \dots, a_{n-1} \in R$ exist and satisfy

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + b_n\pi^n$$

for some $b_n \in \widehat{\mathcal{O}}$, and that the a_i are uniquely determined by this equation. Let $a_n \in R$ be the representative of $[b_n] \in \mathcal{O}/\mathfrak{p}$, hence a_n is unique and $b_n = a_n + \pi b_{n+1}$ for $b_{n+1} \in \widehat{\mathcal{O}}$. Hence

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n + b_{n+1}\pi^{n+1}.$$

By induction, we constructed an infinite series $\sum_{n=0}^{\infty} a_n\pi^n$ which is uniquely determined by u. It converges to u because the remainder terms $\pi^{n+1}b_{n+1}$ tend to zero. □

Example 2.21. Let $\mathbb{F}_q$ be a finite field. We construct the completion of $\mathbb{F}_q(t)$. Recall Example 2.14.

- The residue class field of $(\mathbb{F}_q(t), v_\infty)$ is $\mathbb{F}_q$, we can choose the system of representative $R = \mathbb{F}_q$. Thus $\widehat{\mathbb{F}_q(t)} = \mathbb{F}_q((t))$ contains all Laurent series with coefficient in $\mathbb{F}_q$ in the form $\sum\limits_{n \geq -M} a_n t^n$.
- Let $f(t) = t - a \in \mathbb{F}_q[t]$. Then the residue class field of $(\mathbb{F}_q(t), v_f)$ is isomorphic to $\mathbb{F}_q[X]/(f) \cong \mathbb{F}_q$. Thus we can again choose the system $R = \mathbb{F}_q$ and the completion is $\widehat{\mathbb{F}_q(t)} = \mathbb{F}_q((t-a))$.

Considering $\mathcal{O}/\mathfrak{p}^{\mathfrak{n}}$ as topological rings for the quotient topology, we get the product topology on the ring $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^{\mathfrak{n}}$, which gives a canonical topological ring structure on

$$\varprojlim \mathcal{O}/\mathfrak{p}^{\mathfrak{n}} = \left\{ (x_n) \in \prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^{\mathfrak{n}} | \lambda_n(x_{n+1}) = x_n \right\}.$$

For every $n \in \mathbb{N}_{\geq 1}$ we have a canonical homomorphism $\mathcal{O} \to \mathcal{O}/\mathfrak{p}^n$, which gives a canonical homomorphism $\mathcal{O} \to \varprojlim \mathcal{O}/\mathfrak{p}^{\mathfrak{n}}$ which is indeed an isomorphism:

Proposition 2.22. The canonical mapping $\mathcal{O} \to \varprojlim \mathcal{O}/\mathfrak{p}^{\mathfrak{n}}$ is an isomorphism and a homeomorphism. The same is true for the mapping $\mathcal{O}^\times \to \varprojlim \mathcal{O}^\times/U^{(n)}$.

Proof. The first map is injective since its kernel is $\bigcap_{n=1}^{\infty} \mathfrak{p}^{\mathfrak{n}} = \{0\}$. To prove surjectivity, let $R \subseteq \mathcal{O}$ be a system of representatives for $\mathcal{O}/\mathfrak{p}$ such that $0 \in R$, we saw in the proof of proposition 2.20 that the element $a \in \mathcal{O}$ can be written uniquely in the form

$$a \equiv a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \pmod{\mathfrak{p}^{\mathfrak{n}}}$$

where $a_i \in R$. Each element $s \in \varprojlim \mathcal{O}/\mathfrak{p}^{\mathfrak{n}}$ is given by a sequence $s_n = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}$ where $n \in \mathbb{N}_{\geq 1}$ and $a_i \in R$ are fixed coefficients. Therefore s is the image of the element

$$x = \lim_{n \to \infty} s_n = \sum_{n=0}^{\infty} a_n\pi^n \in \mathcal{O}.$$

The sets $P_n = \prod_{i>n} \mathcal{O}/\mathfrak{p}^{\mathfrak{i}}$ form a basis of neighbourhoods of the 0 element of $\prod_{n=1}^{\infty} \mathcal{O}/\mathfrak{p}^{\mathfrak{n}}$. Under the bijection $\mathcal{O} \to \varprojlim \mathcal{O}/\mathfrak{p}^{\mathfrak{n}}$ the basis of neighbourhoods $\mathfrak{p}^n$ of 0 in $\mathcal{O}$ is mapped onto the basis of neighbourhoods $P_n \cap \varprojlim \mathcal{O}/\mathfrak{p}^n$ of 0 in $\varprojlim \mathcal{O}/\mathfrak{p}^n$. Thus the bijection is a homeomorphism. It induces an isomorphism and a homeomorphism on the group of units :

$$\mathcal{O}^\times \cong (\varprojlim \mathcal{O}/\mathfrak{p}^{\mathfrak{n}})^\times \cong \varprojlim (\mathcal{O}/\mathfrak{p}^{\mathfrak{n}})^\times \cong \varprojlim \mathcal{O}^\times/U^{(n)}.$$

□

We now state a useful result, Lemma 2.24. The proof, which is not very relevant to the rest of the report, is not be given here, but it can be found in Section 4, Chapter 2 of [2]. But first, let's introduce what a primitive polynomial is:

Definition 2.23. We call a polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathcal{O}[x]$ primitive if $f(x) \neq 0$ in $\mathcal{O}/\mathfrak{p}[X]$, i.e. if $\max\{|a_0|, \ldots, |a_n|\} = 1$.

Lemma 2.24 (Hensel's Lemma)**.** If a primitive polynomial $f(x) \in \mathcal{O}[x]$ admits a modulo $\mathfrak{p}$ factorization $f(x) \equiv \overline{g}(x)\overline{h}(x) \pmod{\mathfrak{p}}$ into relatively prime polynomials $\overline{g}, \overline{h} \in \kappa[x]$, then $f(x)$ admits a factorization $f(x) = g(x)h(x)$ where $g, h \in \mathcal{O}[x]$ such that

$$\deg(g) = \deg(\overline{g}), \quad g(x) \equiv \overline{g}(x) \pmod{\mathfrak{p}}, \text{ and } h(x) \equiv \overline{h}(x) \pmod{\mathfrak{p}}.$$

Corollary 2.25. Let K be complete with respect to the nonarchimedean norm $|\cdot|$. Then for every irreducible polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ such that $a_0a_n \neq 0$ we have

$$\max\{|a_0|, |a_n|\} = \max\{|a_0|, |a_1|, \ldots, |a_n|\}.$$

In particular, $a_n = 1$ and $a_0 \in \mathcal{O}$ imply that $f \in \mathcal{O}[x]$.

The above corollary is a consequence of Hensel's Lemma, and is used in the proof of the following theorem.

Theorem 2.26. Let K be complete with respect to the norm $|\cdot|$. Then $|\cdot|$ may be extended uniquely to a valuation of any given algebraic extension $L|K$. This extension is given by the formula

$$|\alpha|_L = |\alpha| = \sqrt[n]{\left|N_{L|K}(\alpha)\right|} = \sqrt[[K(\alpha):K]]{\left|N_{L|K}(\alpha)\right|}$$

when $L|K$ has finite degree n. In this case L is again complete.

Proof. If $|\cdot|$ is archimedean, then by Ostrowki's theorem we have $K = \mathbb{R}$ or $\mathbb{C}$, hence $N_{\mathbb{C}|\mathbb{R}}(z) = z\overline{z}$ and the theorem is proven. Otherwise, we have $|\cdot|$ is nonarchimedean. We can assume without loss of generality that $[L : K]$ is finite, because every algebraic extension is the union of its finite subextensions.

Existence : Let $\mathfrak{o}$ the valuation ring of K and $\mathcal{O}$ its integral closure in L, we have

$$\mathcal{O} = \{\alpha \in L \mid N_{L|K}(\alpha) \in \mathfrak{o}\}. \tag{1}$$

Indeed, if $\alpha \in \mathcal{O}$, we have $N_{L|K}(\alpha) \in \mathfrak{o}$. Conversely, the case $\alpha = 0$ being clear, let $\alpha \in L^\times$, $N_{L|K}(\alpha) \in \mathfrak{o}$, and $f(x) \in K[x]$ be the minimal polynomial of α over K. Then $N_{L|K}(\alpha) = \pm f(0)^m$, which implies $|f(0)| \leq 1$ thus $a_0 \in \mathfrak{o}$. Corollary 2.25 gives $f(x) \in \mathfrak{o}[x]$, i.e. $\alpha \in \mathcal{O}$.

Now consider the function $|\alpha| = \sqrt[n]{\left|N_{L|K}(\alpha)\right|}$, the only non-trivial condition that we need to check in the definition of a valuation is the strong triangular inequality : $|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$, the case $\alpha = \beta = 0$ being true, we assume without loss of generality that $\beta \neq 0$, and therefore we only need to prove that $|\alpha| \leq 1 \implies |\alpha + 1| \leq 1$ which by (1), is implied by the veracity of $\alpha \in \mathcal{O} \implies \alpha + 1 \in \mathcal{O}$ which is true. Therefore $|\alpha| = \sqrt[n]{\left|N_{L|K}(\alpha)\right|}$ defines a valuation on L of valuation ring $\mathcal{O}$, and restricted to K, gives the valuation $|\cdot|$.

Uniqueness: Let $|\cdot|'$ be another extension with valuation ring $\mathcal{O}'$. Let $\mathfrak{p}$, resp. $\mathfrak{p}'$, be the maximal ideal of $\mathcal{O}$, resp. $\mathcal{O}'$. We show that $\mathcal{O} \subseteq \mathcal{O}'$. Let $\alpha \in \mathcal{O}\backslash\mathcal{O}'$, and let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ be its minimal polynomial of α over K, then we have $a_{d-1}, ..., a_0 \in \mathfrak{o}$ and $\alpha^{-1} \in \mathfrak{p}'$, where the latter is true by the definition of a valuation ring. Hence

$$1 = -a_{d-1}\alpha^{-1} - ... - a_0\alpha^{-d} \in \mathfrak{p}',$$

which is a contradiction. Therefore $\mathcal{O} \subseteq \mathcal{O}'$. In other words, $|\alpha| \leq 1 \implies |\alpha|' \leq 1$, which implies that $|\cdot|$ and $|\cdot|'$ are equivalent. The last implication is true because if $|\cdot|$ and $|\cdot|'$ were not equivalent we would have by Proposition 2.3 some $x \in K$ such that $|x| < 1 = |x|'$. Let $y \in K$ such that $|y|' > 1$. Since $|x^n| = |x|^n \to 0$, then for n large enough we have $|x^n y| < 1 < |x^n y|'$ which contradicts Proposition 2.3. Thus $|\cdot|$ and $|\cdot|'$ are equal because they agree on K.
The fact that L is again complete with respect to the extended valuation is deduced from the more general result in the following lemma. □

Lemma 2.27. Let K be complete with respect to the valuation $|\cdot|$ and let V be an $n-$dimensional normed vector space over K. Then for any basis $v_1, ..., v_n$ of V, the maximal norm

$$\|x_1 v_1 + \cdots + x_n v_n\| = \max\{|x_1|, \ldots, |x_n|\}$$

is equivalent to the given norm on V. In particular, V is complete and the isomorphism

$$K^n \to V, (x_1, ..., x_n) \mapsto x_1 v_1 + \cdots + x_n v_n$$

is a homeomorphism.

Remark 2.28.
1. If $[L : K] = n$ and $\pi \in L$ such that $|\pi| = \sqrt[n]{|\pi_K|}$ for some uniformizer π_K of K, π is a uniformizer of L.
2. If $L|K$ is a Galois extension of complete field $(K, |\cdot|)$ and $|\cdot|$ extends to the norm on L, the Galois action preserves the norm on L. Precisely, if $[L : K] = n$ and $\varphi \in \mathrm{Gal}(L|K)$ and $\alpha \in L$,
$$|\alpha| = \sqrt[n]{\left|N_{L|K}(\alpha)\right|} = \sqrt[n]{\prod \phi(\alpha)} = |\varphi(\alpha)| \quad \text{where } \phi \in \mathrm{Gal}(L|K).$$
3. If $L|K$ is an extension of fields with (K, v) complete, then v extends uniquely to a valuation on L. We denote by $(\mathcal{O}_K, \mathfrak{p}_K, \kappa_K)$ and $(\mathcal{O}_L, \mathfrak{p}_L, \kappa_L)$ the local rings of integers and residue class fields of K and L respectively. Then κ_K is a subfield of κ_L. Indeed, $\mathcal{O}_K \subseteq \mathcal{O}_L$ because $\mathcal{O}_L$ contains all element of norm at most 1 and similarly, $\mathfrak{p}_K \subseteq \mathfrak{p}_L$. If $a, b \in \mathcal{O}_K$ are in the same class modulo $\mathfrak{p}_K$, $|a - b| < 1$ thus $a \equiv b \pmod{\mathfrak{p}_L}$. The converse holds, thus κ_K is a subfield of κ_L.

Definition 2.29. Let $L|K$ be an extension of field with (K, v) is complete. We denote $v(L^\times)$ the value group of L extending uniquely from $v(K^\times)$. The index and degree

$$e(L|K) = \left(v\left(L^\times\right) : v\left(K^\times\right)\right), \quad f(L|K) = [\kappa_L : \kappa_K]$$

are respectively called the *ramification index* and *inertia degree* of the extension $L|K$.

The following proposition is called **fundamental identity**, which gives the relations between these subjects and the degree of $L|K$. The proof can be found in a more general version with henselian fields, in Section 2.6 of [2].

Proposition 2.30. Let $L|K$ be a finite separable extension of complete fields, then

$$[L : K] = e(L|K) f(L|K).$$

3 Local fields

In this section, we give the definition of local fields and classify them up to isomorphism.

Definition 3.1. A local field is a nonarchimedean field with a complete discrete valuation and has a finite residue field.

Proposition 3.2. A local field K is locally compact and its valuation ring $\mathcal{O}_K$ is compact.

Proof. We have an isomorphism of topological rings $\mathcal{O}_K = \varprojlim \mathcal{O}_K/\mathfrak{p}_K^n$ by Proposition 2.22. Hence $\mathcal{O}_K$ is a subspace of

$$X = \prod \mathcal{O}_K/\mathfrak{p}_K^n,$$

which is a product of finite discrete space, thus a Hausdorff compact space. Because $\mathcal{O}_K$ is complete, it is closed in X hence compact. Thus $\mathcal{O}_K$ is a compact neighborhood of 0 because it is open. By translation, $a + \mathcal{O}_K$ is a compact neighborhood of a. □

Before characterising all the local fields, we introduce the following lemma. Its proof can be found in [3], Chapter 4, Theorem 4.12.

Lemma 3.3. Let K be a locally compact valued field. Then

1. If $\operatorname{char} K = 0$, then K is $\mathbb{R}$, $\mathbb{C}$ or a finite extension of $\mathbb{Q}_p$.
2. If $\operatorname{char} K = p > 0$, then K is isomorphic to $\mathbb{F}_q((t))$ for some finite field $\mathbb{F}_q$.

Proposition 3.4. The local fields are precisely the finite extensions of $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$.

Proof. Let k be $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$. A finite extension $K|k$ is complete by Theorem 2.26. To show that the residue field κ of K is finite over $\kappa_k = \mathbb{F}_p$, any $\mathbb{F}_p-$linearly independent set $\{\overline{x_1}, \ldots, \overline{x_n}\} \subseteq \kappa$ lifts to a linearly independent set on $K|k$. Thus $\kappa/\mathbb{F}_p$ is of dimension at most $[K : k]$. Conversely, if K is a local field, it is locally compact by Proposition 3.2. By Lemma 3.3, since K is nonarchimedean, it is a finite extension of $\mathbb{Q}_p$ or it is the field $\mathbb{F}_q((t))$, a finite extension of $\mathbb{F}_p((t))$. □

4 Unramified and totally ramified extensions

4.1 Generalities

We follow Chapter 2, Section 7 of [2]. Throughout this section, (K, v) is a complete field with a discrete nonarchimedean valuation v.

Definition 4.1. A finite extension $L|K$ is called *unramified* if

$$\kappa_L|\kappa_K \text{ is separable}, \quad [\kappa_L : \kappa_K] = [L : K].$$

In general, an extension $L|K$ is unramified if L is the union of finite unramified subextensions of K.

We introduce some basic facts of this terminology.

Proposition 4.2. Let $L|K$ be an algebraic extension where K is a complete field. We have

1. If $L|K$ is unramified, the ramification index $(v(L^\times) : v(K^\times)) = 1$, which explains the notation.
2. If $L|K$ is Galois and unramified, κ_L is also Galois over κ_K and there is an isomorphism of groups $\operatorname{Gal}(L|K) \cong \operatorname{Gal}(\kappa_L|\kappa_K)$ sending φ to $\widetilde{\varphi} : [\alpha] \mapsto [\varphi(\alpha)]$.
3. The union of two unramified subextensions $K_1|K$ and $K_2|K$ is a unramified subextension.

4. The union of all unramified subextensions of $L|K$ is an unramified extension T of K, which is called the **maximal unramified extension** of $L|K$.

5. We have a bijection
$$\left\{ \begin{array}{c} L|K'|K, \\ K' \text{ unramified over } K \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} \kappa_L|k'|\kappa_K, \\ k' \text{ separable over } \kappa_K \end{array} \right\}$$
sending a unramified extension $K'|K$ to its residue field $\kappa_{K'}|\kappa_K$. In particular, the residue field of T is $\kappa_K^{\text{sep}} \cap \kappa_L$. In case $L = \overline{K}$, we call T the maximal unramified extension of K and is denoted by K^{ur}.

Definition 4.3. The extension $L|K$ is called *totally ramified* if $T = K$.

Remark 4.4. If $L|K$ is finite and separable, it is totally ramified if and only if $f(L|K) = 1$.

4.2 Aspects of local fields

We will follow Section 2 of [4] in this subsection. We classify all the unramified extensions of a local field K with the residue field $\mathbb{F}_q$. Let μ_n be the set of roots of unity of order n. From now on, the completion of the maximal unramified extension $K^{\text{ur}}|K$ is denoted by $\widehat{K}$.

Proposition 4.5. 1. All the finite unramified extension of K is Galois given by $K_n = K(\mu_{q^n-1})$, and the residue field of K_n is $\mathbb{F}_{q^n}$, moreover
$$\text{Gal}(K_n|K) \cong \text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}.$$

2. The Galois group $\text{Gal}(K^{\text{ur}}|K) \cong \text{Gal}\left(\overline{\mathbb{F}_q}|\mathbb{F}_q\right) \cong \widehat{\mathbb{Z}}$.

Definition 4.6. The arithmetic Frobenius $\varphi \in \text{Gal}(K^{\text{ur}}|K)$ is defined as the element which reduces mod $\mathfrak{p}$ to the q-th power Frobenius map of $\overline{\mathbb{F}_q}$ and denote by Frob_K the inversion of φ.

Definition 4.7. The separable extension $E|K$ is finitely ramified if E is a finite extension of an unramified extension of K.

Lemma 4.8. Let $E \subseteq K^{\text{sep}}$ be finitely ramified over K. Then

1. The ring $\mathcal{O}_E$ is a DVR.
2. If $E'|E$ finite and separable, then $E'\widehat{E} = \widehat{E'}$ and $\widehat{E} \cap E' = E$ where $\widehat{E}$ and $\widehat{E'}$ are respectively the completions of E and E'.
3. $\widehat{E} \cap K^{\text{sep}} = E$.

Proof. 1. Let F be the subfield of E which is unramified over K such that $[E : F] = N < +\infty$, then $v(K) = v(F) = \mathbb{Z}$. Consider $\alpha \in E$, it is algebraic over F with the minimal polynomial
$$p(x) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in F[X] \text{ and } m \mid N.$$
If B is the set of all conjugates of all the a_i then $K(B)$ is a finite Galois extension of K with Galois group G. Consider polynomial $P(X) = \prod_{\varphi \in G} \varphi(p(x))$. Because P is invariant under every $\varphi \in G$, all its coefficients belong to K. Moreover, the action of G does not change the norm of every $a \in K(B)$ thus $|P(0)| = |a_0|^{|G|}$ and hence
$$|\alpha| = \sqrt[\deg P]{|P(0)|} = \sqrt[m]{|a_0|}.$$
This means $v(\alpha) \in \frac{1}{m}\mathbb{Z} \subseteq \frac{1}{N}\mathbb{Z}$, i.e $\mathcal{O}_E$ is a discrete valuation ring.

2. Since E' and $\widehat{E}$ are the subsets of $\widehat{E'}$, we have $E'\widehat{E} \subseteq \widehat{E'}$. Denote by $L = E'\widehat{E}$. To show that $\widehat{E'} \subseteq L$, it suffices to prove that L is complete. Since $E'|E$ is finite and separable, it is generated by an element α, i.e. $E' = E(\alpha)$ and hence $L = \widehat{E}(\alpha)$. In other words, $L/\widehat{E}$ is finite and L is a finite dimensional $\widehat{E}$-vector space. Because $\widehat{E}$ is complete, L is complete by Theorem 2.26. Now we show that $\widehat{E} \cap E' = E$. Suppose the contradiction that there is $\beta \in \widehat{E} \cap E'$ does not belong to E and denoted by $\{\beta_1, \ldots, \beta_m\}$ the set of all conjugates of β. Let H be the Galois group of the extension $K(\beta_1, \ldots, \beta_n)|K$. Since $\beta \in \widehat{E}$, it is the limit of some Cauchy sequence $(a_n) \subseteq E$. Because β is separable over E, there exists an element $\varphi \in H$ such that $\varphi(\beta) \neq \beta$. However, when we extend continuously φ to an element of $\mathrm{Gal}\left(\widehat{E}(\beta_1, \ldots, \beta_n)|\widehat{E}\right)$, thus $\varphi(\beta) = \lim \varphi(a_n) = \lim a_n = \beta$ which is a contradiction.

3. The previous part demonstrates that every β separable over E is an element of $\widehat{E}$ if and only if it belongs to E. Thus $K^{\mathrm{sep}} \cap \widehat{E} = E$.

□

When the extension $E'|K$ is Galois, let E be the maximal unramified extension of $E'|K$. We define its Weil group by

$$\mathrm{W}\left(E'|K\right) = \{\sigma \in \mathrm{Gal}\left(E'|K\right) : \sigma|_E \in \varphi^{\mathbb{Z}}\}.$$

Definition 4.9. The completion L of a finitely ramified extension $E|K$ is called a *complete extension* of K. When $E|K$ is unramified, L is called a *complete unramified extension* of K.

Remark 4.10. We know that L is discrete since E is discrete. As discussed in Lemma 4.8, the complete extensions of K correspond bijectively to finitely ramified extensions $E|K$.

Definition 4.11. 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 $\varphi^i \in \mathrm{Aut}(L|K)$ extends to $[L' : L]$ distinct elements of $\mathrm{Aut}(L'|K)$. In general, we say L' is Galois over K if it is the union of finite extension of L which are Galois over K. We define the *Weil group* of $L'|K$ by

$$\mathrm{W}\left(L'|K\right) = \{\sigma \in \mathrm{Aut}\left(L'|K\right) \mid \sigma|_L \in \mathrm{Frob}_K^{\mathbb{Z}}\}.$$

Remark 4.12.

1. This notation concides with the usual Galois extension in case $L'|K$ is finite.

2. If $E' = L' \cap K^{\mathrm{sep}}$ is Galois over K, by restriction, we can define a surjection $\mathrm{W}(L'|K) \to \mathrm{W}(E'|K)$ which is indeed an isomorphism.

5 Formal groups and Lubin-Tate groups

This section gives the definitions of formal groups and Lubin-Tate groups over the valuation ring $\mathcal{O}_L$ of the complete unramified extension $L|K$. The idea is to define an action of $\mathcal{O}_K$-module on a subset of $\mathfrak{p}_L$, which can be seen as the ideal generated by π in $\mathcal{O}_L = \mathcal{O}_L[[\pi]]$ where π is a uniformizer of L. We mainly follow Section 3 of [4].

Definition 5.1. A formal group law over $\mathcal{O}_L$ is a formal power series of two variables $F(X, Y) \in \mathcal{O}_L[[X, Y]]$ 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) $F(X, Y) = F(Y, X)$.

Remark 5.2. We can equip $(X) \subseteq \mathcal{O}_L[[X]]$ with a structure of abelian group by a formal group F over a ring $\mathcal{O}_L$. Since $F(X, 0) \equiv X \pmod{X^2}$, by induction, we can find a unique $i_F(X) \in (X)$ such that $F(X, i_F(X)) = 0$. We define the addition $+_F$ on the ideal $(X) \subseteq \mathcal{O}_L[[X]]$ by

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

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

Example 5.3. The formal group F converges absolutely on $\mathfrak{p}_L$. Then $(\mathfrak{p}_L, +_F)$ is an abelian group.

Definition 5.4. Let F and G be formal groups over $\mathcal{O}_L$. A power series $f(X) \in (X)$ is called a *homomorphism* from F to G if it satisfies

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

The power series $f \in (X)$ is an *isomorphism* if it is invertible, i.e has the linear term in $\mathcal{O}_L^\times$.

We still define φ as the extension of the Frobenius map of $\mathrm{Gal}(K^{\mathrm{ur}}|K)$ to L and denote by $\theta^\varphi = \varphi(\theta)$.

Definition 5.5. For uniformizers π, π' of L, set $\Theta^L_{\pi,\pi'} = \{\theta \in \mathcal{O}_L : \theta^\varphi/\theta = \pi'/\pi\}$.

Remark 5.6. The set $\Theta^L_{\pi,\pi'}$ is an additive group and if $\theta \in \Theta^L_{\pi,\pi'}$ and $\theta' \in \Theta^L_{\pi',\pi''}$ then $\theta\theta' \in \Theta^L_{\pi,\pi''}$.

Lemma 5.7. Let π be a uniformizer of L and let $f \in \mathcal{O}_L[[X]]$ satisfy

$$f(X) \equiv \pi X \pmod{\deg 2}, \qquad f(X) \equiv X^q \pmod{\mathfrak{p}_L}.$$

Let f' and π' be another such pair. Assume that $\theta_1, \ldots, \theta_t \in \Theta^L_{\pi,\pi'}$. Then there is a unique $F \in \mathcal{O}_L[[X_1, \ldots, X_t]]$ 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 $m \geq 1$, there is a unique polynomial F_m of degree at most m in $\mathcal{O}_L[X_1, \ldots, X_t]$ satisfying

$$F_m \equiv \theta_1 X_1 + \cdots + \theta_t X_t \pmod{\deg 2}, \qquad f' \circ F_m \equiv F_m^\varphi \circ f \pmod{\deg(m+1)}.$$

In case $m = 1$, the polynomial $F_1 = \theta_1 X_1 + \cdots + \theta_t X_t$ works because $\theta_k^\varphi/\theta_k = \pi'/\pi$. Suppose that we have F_m. By taking modulo $\deg(m+1)$, we conclude $F_{m+1} = F_m + H_{m+1}$ for H_{m+1} homogeneous of degree $m+1$. Modulo $\deg(m+2)$, we have

$$\begin{cases} f' \circ (F_m + H_m) \equiv f' \circ F_m + \pi' H_m \pmod{\deg(m+2)}, \\ (F_m + H_m)^\varphi \circ f \equiv F_m^\varphi \circ f + \pi H_m^\varphi \pmod{\deg(m+2)}. \end{cases}$$

Denoted by $G_{m+1} = f' \circ F_m - F_m^\varphi \circ f$. Modulo $\mathfrak{p}_L$ we have

$$G_{m+1} \equiv F_m^q - F_m^\varphi(X_1^q, \ldots, X_t^q) \equiv 0 \pmod{\mathfrak{p}_L}.$$

Finally, to show the existence and uniqueness of H_{m+1}, we need to find the coefficients of each monomial of degree $m+1$. Indeed, it suffices to show that for each $a \in \mathfrak{p}_L$, there exists a unique element $b \in \mathcal{O}_L$ such that $a + \pi' b - \pi^{m+1} b^\varphi = 0$, which means

$$b = -c - \sum_{i=1}^{\infty} \left(\frac{\pi^{m+1}}{\pi'}\right)^{1+\varphi+\cdots+\varphi^{i-1}} c^{\varphi^i}.$$

where $c = a(\pi')^{-1}$. □

Now, we give a technical proposition, which helps us present the Lubin-Tate extension. We will only give the proof of first item, the others can be proved similarly.

Proposition 5.8. Let f and f' as in Lemma 5.7.

1. There exists a unique formal group F_f over $\mathcal{O}_L$ such that $f \in \mathrm{Hom}_{\mathcal{O}_L}\left(F_f,\, F_f^{\varphi}\right)$. We call F_f the Lubin-Tate group associated to f.
2. There is a unique group homomorphism $[\cdot]_{f,\,f'} : \Theta^L_{\pi,\,\pi'} \to \left((X)\,,\, +_{F_{f'}}\right) \subseteq \mathcal{O}_L\,[[X]]$ such that

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

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

Proof. By Lemma 5.7, when $\theta_1 = \theta_2 = 1$, there exists a unique $F_f \in \mathcal{O}_L\,[[X]]$ such that $f \circ F_f = F_f^{\varphi} \circ f$. We need to verify F_f is a formal group. We know that

$$F_f(X,\,Y) \equiv \theta_1 X + \theta_2 Y \equiv X + Y \pmod{\deg 2}.$$

Swapping the role of X and Y, the power series $F_f(Y,\,X)$ also satisfies these conditions, thus the uniqueness implies that F_f is symmetric. Denote by $F_f\left(F_f(X,\,Y),\,Z\right) = G\left(X,\,Y,\,Z\right) \in \mathcal{O}_L\,[[X,\,Y,\,Z]]$. The linear term of G is

$$G\left(X,\,Y,\,Z\right) = F_f\left(F_f(X,\,Y),\,Z\right) \equiv F_f(X,\,Y) + Z \equiv X + Y + Z \pmod{\deg 2}.$$

We verify $f \circ G = G^{\varphi} \circ f$. Let $H = F_f\left(X,\,F_f\left(Y,\,Z\right)\right)$ then $H \equiv X + Y + Z \pmod{\deg 2}$ and $f \circ H = H^{\varphi} \circ f$, thus $G = H$ due to the uniqueness part of Lemma 5.7. □

Corollary 5.9. The map $[\cdot]_f = [\cdot]_{f,\,f} : \mathcal{O} \longrightarrow \mathrm{End}_{\mathcal{O}_L}\left(F_f\right)$ is an injective ring homomorphism and $\mathrm{End}_{\mathcal{O}_L}\left(F_f\right)$ is a formal $\mathcal{O}$-module.

Proof. The image of $\alpha \in \mathcal{O}$ is a power series $[\alpha]_f$ such that

$$[\alpha]_f \equiv \alpha X \pmod{\deg 2}, \qquad f \circ [\alpha]_{f,\,f} = [\alpha]^{\varphi}_{f,\,f} \circ f.$$

Thus $[\alpha]_f$ and $[\alpha']_f$ have the same linear terms if and only if $\alpha = \alpha'$, hence $[\cdot]_f$ is an injective. This map preserves addition and multiplication due to part 2. and 3. of Proposition 5.8. □

Corollary 5.10. If $\theta \in \Theta^L_{\pi,\,\pi'} \cap \mathcal{O}_L^{\times}$, then $[\theta]_{f,\,f'}$ is an isomorphism with the inversion $\left[\theta^{-1}\right]_{f',\,f}$.

Example 5.11. We have $\pi \in \Theta^L_{\pi,\,\pi^{\varphi}}$ and $[\pi]_{f,\,f^{\varphi}} = f$ because of the uniqueness in Lemma 5.7. Note that $F_f^{\varphi} = F_{f^{\varphi}}$ and $[\theta]^{\varphi}_{f,\,f'} = [\theta^{\varphi}]_{f^{\varphi},\,f'^{\varphi}}$.

Definition 5.12. Define $f_m = f^{\varphi^{m-1}} \circ \cdots \circ f^{\varphi} \circ f$. Then we have

$$f_m = \left[\pi^{\varphi^{m-1}}\right]_{f^{\varphi^{m-1}},\,f^{\varphi^m}} \circ \cdots \circ [\pi]_{f,\,f^{\varphi}} = [\pi_m]_{f,\,f^{\varphi^m}}$$

where $\pi_m = \prod_{t=0}^{m-1} \pi^{\varphi^t}$.

6 Lubin-Tate extensions and Artin map

In this section, we construct explicitly the Artin map discussed in the introduction. The aim is to understand the structure of $\mathrm{W}\left(K^{\mathrm{LT}}|K\right)$. We mainly follow Section 4 of [4].

6.1 Lubin-Tate extensions

Let $(\mathcal{O},\, \mathfrak{p},\, \mathbb{F}_q)$ be the valuation ring and residue class field of a local field K and let L be a complete unramified extension of K. Let $(\mathcal{O}_L,\, \mathfrak{p}_L)$ be the integer ring of L. This subsection defines the Lubin-Tate extensions of L and studies their Galois groups by the Lubin-Tate theory. We denote by $v(x) = v_K(x)$.

Definition 6.1. Let $f \in \mathcal{O}_L[X]$ be a monic polynomial satisfying

$$f(X) \equiv \pi X \pmod{X^2}, \qquad f(X) \equiv X^q \pmod{\mathfrak{p}_L} \tag{2}$$

for a uniformizer π of L, we say that f is a *Lubin-Tate polynomial* with linear term π. For $m \geq 1$, let L_f^m be the splitting field of $f_m \in \mathcal{O}_L[X]$ over L (c.f Definition 5.12), and $\mu_{f,\,m}$ be the set of roots of f in L_f^m.

Remark 6.2. When we write f is a Lubin-Tate polynomial in this section, we always assume its linear term is a uniformizer π.

Our goal in this subsection is to prove that L_f^m is Galois over L, and precisely f_m is separable. This helps us view the action of Lubin-Tate group on the set of roots of f_m as the action of the Galois group $\mathrm{Gal}\left(L_f^m|L\right)$, i.e. the Lubin-Tate action is the Galois action "in some interpretation".
The following lemma gives some characteristics of $\mu_{f,\,m}$.

Lemma 6.3. Let $m \geq 1$ and f be a Lubin-Tate polynomial. Denote by $L' = L_f^m$ and $[\cdot] = [\cdot]_f$.

1. We have $\mu_{f,\,m} \subseteq \mathfrak{p}_{L'}$.
2. Let $x \in K^\times$, $v(x) = m$ and $\alpha \in \mathfrak{p}_{L^{sep}}$. We have $\alpha \in \mu_{f,\,m}$ if and only if

$$[x](\alpha) = 0 \Leftrightarrow [a](\alpha) = 0$$

for all $a \in \mathfrak{p}^m$.

Proof. 1. Since $f_m \in \mathcal{O}_L[x]$ is a monic polynomial, then $\mu_{f,m} \subset \mathcal{O}_{L'}$. If $\alpha \in \mathcal{O}_{L'}^\times$, $f_m(\alpha)$ equals to α^{q^m} modulo $\mathfrak{p}_{L'}$, a contradiction.

2. Note that $[x](\alpha)$ is well-defined by the same argument in Example 5.3. Let $a \in K^\times$ with $v(a) = m$. Then $a \cdot (\pi_m)^{-1} \in \mathcal{O}_L^\times$ and because

$$[a] = \left[a \cdot (\pi_m)^{-1}\right]_{f^{\varphi^m},\,f} \circ [\pi_m]_{f,\,f^{\varphi^m}} = \left[a \cdot (\pi_m)^{-1}\right]_{f^{\varphi^m},\,f} \circ f_m.$$

If α is a root of f_m, then $[x](\alpha)$ is obviously 0. On the other hand, assume that $[x](\alpha) = 0$. The law $\left[a \cdot (\pi_m)^{-1}\right]_{f^{\varphi^m},\,f}$ is invertible with the inverse $\left[\pi_m \cdot a^{-1}\right]_{f,\,f^{\varphi^m}}$ thus

$$f_m(\alpha) = \left[\pi_m \cdot a^{-1}\right]_{f,\,f^{\varphi^m}}[x](\alpha) = 0.$$

□

Proposition 6.4. The set $\mu_{f,m}$ is an $\mathcal{O}$-module equipped by operations

1. For all $\alpha_1, \alpha_2 \in \mu_{f,m}$, we define $\alpha_1 +_{F_f} \alpha_2 = F_f(\alpha_1, \alpha_2)$,
2. For all $a \in \mathcal{O}$ and $\alpha \in \mu_{f,m}$, we define $a \circ \alpha = [a](\alpha)$.

Proposition 6.5. Let $m \geq 1$ and $f \in \mathcal{O}_L[X]$ be a Lubin-Tate polynomial.

1. For any $\alpha \in \mu_{f,m}^{\times} \coloneqq \mu_{f,m} \setminus \mu_{f,m-1}$ the following map is an isomorphism of $\mathcal{O}$-modules

$$\psi_a : \mathcal{O}/\mathfrak{p}^m \longrightarrow \mu_{f,m},\ a \bmod \mathfrak{p}^m \overset{\psi_a}{\longmapsto} [a]_f(\alpha).$$

   In addition, every $\mathcal{O}$-map automorphism of $\mu_{f,m}$ is defined by $\alpha \mapsto [b](\alpha)$ for some $b \in \mathcal{O}^{\times}$.

2. If $\alpha \in \mu_{f,m}^{\times}$ 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 extension $L_f^m|L$ is a totally ramified Galois extension of degree $\left|\mu_{f,m}^{\times}\right| = q^{m-1}(q-1)$.

3. We have the canonical isomorphism of abelian groups

$$\rho_{f,m} : \mathrm{Gal}\left(L_f^m|L\right) \overset{\cong}{\longrightarrow} \mathrm{Aut}_{\mathcal{O}}(\mu_{f,m}) \overset{\cong}{\longrightarrow} (\mathcal{O}/\mathfrak{p}^m)^{\times}$$

   sending σ to the action $[a]$ such that $\sigma(\alpha) = [a](\alpha)$.

Proof. 1. Since $a \mapsto [\alpha]_f(\alpha)$ is an $\mathcal{O}$-homomorphism, with kernel $\mathfrak{p}^m$ due to Lemma 6.3, part 2, it suffices to show that this is a surjection. Indeed, since

$$|\mu_{f,m}| \geq |\mathcal{O}/\mathfrak{p}^m| = q^m \geq |\mu_{f,m}|$$

we have $|\mu_{f,m}| = q^m$ and the induced homomorphism $\mathcal{O}/\mathfrak{p}^m \to \mu_{f,m}$ is a surjection hence an isomorphism. Now let ϕ be an $\mathcal{O}$-module automorphism of $\mu_{f,m}$, By composition with ψ_a, we obtain an $\mathcal{O}$-module automorphism $\phi' = \psi_a^{-1}\phi\psi_a$. We know that ϕ' is uniquely determined by $\phi'(1 \bmod \mathfrak{p}^m)$, and it is an automorphism if and only if ϕ' is the left multiplication by $b \in \mathcal{O}^{\times}$. Thus ϕ is also the left multiplication by b.

2. For $\beta \in \mu_{f,m}$, there exists $a \in \mathcal{O}$ such that $\beta = [a]_f(\alpha)$ where $[a]_f \in \mathcal{O}_L[[X]]$ which implies that β is a power series in $L(\alpha)$. Since L is complete and $[L(\alpha) : L] < +\infty$, we have $L(\alpha)$ is also complete. Hence the series $[a]_f(\alpha)$ converges in $\widehat{L(\alpha)} = L(\alpha)$. Thus $\beta \in L(\alpha)$, i.e. $L_f^m = L(\alpha)$. Since $L(\alpha)|L$ is the splitting field of a separable polynomial f_m, we conclude that $L(\alpha)|L$ is a Galois extension. Now we show that f_m/f_{m-1} is irreducible. Firstly,

$$\prod_{\beta \in \mu_{f,m}^{\times}} (-\beta) = \frac{f_m(0)}{f_{m-1}(0)} = \pi^{\varphi^m}.$$

   By taking the valuation of both sides, we have

$$e(L(\alpha)|L) = \sum_{\beta \in \mu_{f,m}^{\times}} v_{L(\alpha)}(-\beta) \geq \left|\mu_{f,m}^{\times}\right| = q^m - q^{m-1}$$

   because $\mu_{f,m} \subseteq \mathfrak{p}_{L(\alpha)}$ thanks to Lemma 6.3 part 1. On the other hand,

$$q^m - q^{m-1} = \deg(f_m) - \deg(f_{m-1}) \geq [L(\alpha) : L] \geq e(L(\alpha)|L)$$

by the fundamental identity in Proposition 2.30. From the two previous inequalities, we conclude that

$$e\left(L\left(\alpha\right)|L\right) = q^m - q^{m-1} = [L(\alpha) : L]$$

thus f_m/f_{m-1} is irreducible. Therefore $\mu_{f,\,m}^{\times}$ is the set of all conjugates of α and the elements of this set have the same valuation. This means $\pi^{\varphi^m} = N_{L(\alpha)|L}(-\alpha)$ and since

$$v_{L(\alpha)}\left(\alpha\right) \cdot \left|\mu_{f,\,m}^{\times}\right| = \left|\mu_{f,\,m}^{\times}\right|,$$

α is the uniformizer of $L\left(\alpha\right)$. Finally, $L(\alpha)|L$ is Galois and $e\left(L\left(\alpha\right)|L\right)$ is equal to the degree of extension, hence $L(\alpha)|L$ is a totally ramified extension.

3. The action of $\mathrm{Gal}\left(L_f^m|L\right)$ on $\mu_{f,\,m}$ is compatible with the action of $\mathcal{O}$-module on this set. The action by σ is an automorphism with inverse element σ^{-1}. These gives a group homomorphism $\rho_{f,\,m} : \mathrm{Gal}\left(L_f^m|L\right) \to \mathrm{Aut}_{\mathcal{O}}\left(\mu_{f,\,m}\right)$ and it is injective because every σ is uniquely determined by the image of $\alpha \in \mu_{f,\,m}^{\times}$. It suffices to show that these groups have the same cardinality. Let $Q = \left|\mathrm{Aut}_{\mathcal{O}}\left(\mu_{f,\,m}\right)\right| = \left|\left(\mathcal{O}/\mathfrak{p}^m\right)^{\times}\right| = \left|\left(\mathcal{O}/\mathfrak{p}^m\right)^{\times}\right|$. Since $\rho_{f,\,m}$ is injective, Q is a multiple of $q^{m-1}(q-1)$. On the other hand

$$Q \leq \left|\mathcal{O}/\mathfrak{p}^m\right| - 1 = q^m - 1$$

thus $Q = q^{m-1}(q-1)$ and $\rho_{f,\,m}$ is an isomorphism.

□

6.2 Artin map

The following lemma shows a link between L_f^m and $L_{f'}^m$ via the map $[\theta]_{f,\,f'}$, where f and f' are Lubin-Tate polynomials with linear term π and π' . Actually, they are defined almost independently from f and f'. We denote by $\Theta_{\pi,\,\pi'}^{L,\,\times} = \Theta_{\pi,\,\pi'}^{L} \cap \mathcal{O}_L$.

Lemma 6.6. If there exists $\theta \in \Theta_{\pi,\,\pi'}^{L,\,\times}$, $[\theta]_{f,\,f'}$ is an $\mathcal{O}_L$-isomorphism $\mu_{f,\,m} \to \mu_{f',\,m}$ and $L_f^m = L_{f'}^m$.

Proof. By the definition, if α is a root of $f_m = f^{\varphi^{m-1}} \circ \cdots \circ f$, we have

$$\begin{aligned} f'_m\left([\theta]_{f,\,f'}\left(\alpha\right)\right) &= \left(f'\right)^{\varphi^{m-1}} \circ \cdots \circ f'\left([\theta]_{f,\,f'}\left(\alpha\right)\right) \\ &= \left(f'\right)^{\varphi^{m-1}} \circ \cdots \circ \left(f'\right)^{\varphi}\left[\theta\right]_{f,\,f'}^{\varphi}\left(f(\alpha)\right) \\ &= \ldots = \left[\theta\right]_{f,\,f'}^{\varphi^m}\left(f_m\left(\alpha\right)\right) = \left[\theta\right]_{f,\,f'}^{\varphi^m}\left(0\right) = 0. \end{aligned}$$

Note that $[\theta]_{f,\,f'}$ is an $\mathcal{O}_L$-map which has inverse $\left[\theta^{-1}\right]_{f',\,f}$ and thus $[\theta]_{f,\,f'}$ is an $\mathcal{O}_L$-automorphism. Moreover, since $[\theta]_{f,\,f'} \in \mathcal{O}_L\left[[X]\right]$, we have $\mu_{f',\,m} = [\theta]_{f,\,f'}\left(\mu_{f,\,m}\right) \subseteq L_f^m$, i.e. $L_{f'}^m \subseteq L_f^m$. Similarly, we have $L_f^m \subseteq L_{f'}^m$, which concludes the lemma. □

Remark 6.7. Note that $\Theta_{\pi,\pi}^{K,\times} = \mathcal{O}_K^{\times}$ is non-empty, thus L_f^m is defined by the linear term π of f. We denote by $L_f^m = L_\pi^m$.

To construct the Artin map, for $j < 0$, we denote by

$$\pi_j = \left(\pi_{-j}^{-1}\right)^{\varphi^j}$$

then $\pi_{j+j'} = \pi_{j'}^{\varphi^j}\pi_j$ for all $j,\, j' \in \mathbb{Z}$ and hence $v_L\left(\pi_j\right) = j$ for all $j \in \mathbb{Z}$. We have the following lemma.

Lemma 6.8. For each $\alpha \in \mu_{f,m}^{\times}$, we have a surjection

$$\Psi : K^{\times} \to \bigcup_{j \in \mathbb{Z}} \mu_{f^{\varphi^j},m}^{\times}$$

sending x to $[x\pi_j]_{f,f^{\varphi^j}}(\alpha)$, where $j = -v(x)$.

Proof. Since $v(x) = -j = -v(\pi_j)$, we have $x\pi_j \in \Theta_{\pi,\varphi^j(\pi)}^{L,\times}$ because

$$\frac{\varphi(x\pi_j)}{x\pi_j} = \frac{\varphi(\pi_j)}{\pi_j} = \frac{\varphi^j(\pi)}{\pi}.$$

thus $[x\pi_j]_{f,f^{\varphi^j}}$ is defined and invertible. By the proof of Lemma 6.6, $[x\pi_j]_{f,f^{\varphi^j}} : \mu_{f,m} \to \mu_{f^{\varphi^j},m}$ is an isomorphism. Fix $\beta_0 = [x\pi_j]_{f,f^{\varphi^j}}(\alpha)$ and consider $\beta \in \mu_{f^{\varphi^j},m}^{\times}$. From the proof of Proposition 6.5, we know that $L(\beta_0) = L_f^m = L(\beta)$, thus there exists a unique permutation $\phi \in \mathrm{Gal}\left(L_f^m|L\right)$ such that $\phi(\beta_0) = \beta$. Through the isomorphism

$$\mathrm{Gal}\left(L_f^m|L\right) \cong \mathcal{O}^{\times}/\mathfrak{p}^m,$$

let the left multiplication by $b \in \mathcal{O}^{\times}$ be the image of ϕ. Thus we have

$$[bx\pi_j]_{f,f^{\varphi^j}}(\alpha) = [b](\beta_0) = \beta.$$

This means $\mu_{f^{\varphi^j},m}^{\times}$ is a subset of the image of Ψ. □

The aim of the next proposition is to construct the Artin map. Firstly, we prove that L_f^m is Galois over K, i.e. to extend each exponent of the Frobenius map $\varphi^j : L \to L$ to exactly $q^{m-1}(q-1)$ automorphism of L_f^m. This fact will help us discuss the Weil group of the extension $\widehat{K}_f^m|\widehat{K}$, here $\widehat{K}$ is the completion of K^{ur}.

Proposition 6.9. Let $m \geq 1$ and $f \in \mathcal{O}_L[X]$ be a Lubin-Tate polynomial.

1. The extension $L_f^m|K$ is Galois.
2. In case $L = \widehat{K}$, the isomorphism $\rho_{f,m}$ in Proposition 6.5 extends to an isomorphism

   $$\rho_{f,m} : \mathrm{W}\left(L_f^m|K\right) \xrightarrow{\cong} K^{\times}/(1+\mathfrak{p}^m)$$

   with the inverse sending $\overline{x} \in K^{\times}/(1+\mathrm{p}^m)$ to ϕ such that $\phi|_{\widehat{K}} = \varphi^{-v(x)}$ and $\phi(\alpha) = [x\pi_j]_{f,f^{\varphi^j}}(\alpha)$ for $\alpha \in \mu_{f,m}^{\times}$.
3. Let $\widehat{K}_f^{\mathrm{LT}} = \bigcup_{m\geq 1} \widehat{K}_f^m$, we have a canonical isomorphism $\rho_f : \mathrm{W}\left(\widehat{K}_f^{\mathrm{LT}}|K\right) \xrightarrow{\cong} K^{\times}$ with the inverse sending x to ϕ such that

   $$\phi|_{\widehat{K}} = \varphi^{-v(x)}, \quad \alpha \in \mu_{f,m} \mapsto \left[x\pi_{-v(x)}\right]_{f,f^{\varphi^j}}(\alpha)$$

   for all positive integer m.

Proof. 1. Fixing $j \in \mathbb{Z}$, we will prove that for $\alpha \in \mu_{f,m}^{\times}$ and $\beta \in \mu_{f^{\varphi^j},m}^{\times}$, and for all $j \in \mathbb{Z}$, there exists a unique isomorphism $\phi : L(\alpha) = L_f^m \to L_f^m = L(\beta)$ extending φ^j such that $\phi(\alpha) = \beta$. Since every $x \in L_f^m$ is written in the form $p(\alpha)$ for some $p \in \mathcal{O}_L[X]$, it suffices to show that ϕ is well defined, i.e. for all polynomial p and q such that $p(\alpha) = q(\alpha)$, then $p^{\varphi^j}(\beta) = q^{\varphi^j}(\beta)$. By the proof of Proposition 6.5, the minimal polynomials of α and β over $\mathcal{O}_L$ are f_m/f_{m-1} and $f_m^{\varphi^j}/f_{m-1}^{\varphi^j}$ respectively. Since $p - q$ is a multiple of f_m/f_{m-1}, we have $p^{\varphi^j} - q^{\varphi^j}$ is a multiple of $(f_m/f_{m-1})^{\varphi^j} = f_m^{\varphi^j}/f_{m-1}^{\varphi^j}$, thus ϕ is well-defined. Since $\mu_{f^{\varphi^j},m}^{\times}$ has $q^{m-1}(q-1)$ elements, there are at least $q^{m-1}(q-1)$ maps extending φ^j. On the other hand, if φ^j extends to ϕ, which sends a root of f_m to a root of $f_m^{\varphi^j}$ hence ϕ is uniquely determined by the equation $\phi(\alpha) = \beta$.

2. If $L = \widehat{K}$, consider the homomorphism

$$K^{\times} \xrightarrow{\Psi_{f,m}} \mathrm{W}\left(\widehat{K}_f^m | K\right)$$

which sends $x \in K^{\times}$ of valuation $-j$ to ϕ defined by $\phi|_{\widehat{K}} = \varphi^j$ and $\phi(\alpha) = [x\pi_j]_{f,f^{\varphi^j}}(\alpha)$. It is a group homomorphism because $\varphi^{j+j'} = \varphi^j \circ \varphi^{j'}$ and

$$\left[xx'\pi_j\pi_{j'}\right]_{f,f^{\varphi^{j+j'}}} = [x\pi_j]^{\varphi^{j'}}_{f^{\varphi^{j'}},f^{\varphi^{j+j'}}} \circ \left[x'\pi_{j'}\right]_{f,f^{\varphi^{j'}}} = [x\pi_j]_{f,f^{\varphi^j}} \circ \left[x'\pi_{j'}\right]_{f,f^{\varphi^{j'}}}.$$

As proven in Lemma 6.8, $\rho_{f,m}$ is a surjection. We now show that $\operatorname{Ker}\Psi_{f,m}$ is the subgroup $1 + \mathfrak{p}^m$ of $K^{\times}$. Indeed, if the image of x is $\mathrm{Id}_{\widehat{K}_f^m}$, its restriction on $\widehat{K}$ is also identity thus $j = 0$. Hence $[x] = [1]$, and by Lemma 6.3, we have $[x-1](\alpha) = 0$, i.e. $x - 1$ is an element of $\mathfrak{p}^m$. Therefore, $\operatorname{Ker}\Psi_{f,m} \subseteq 1 + \mathfrak{p}^m$. On the other hand, if $x \in 1 + \mathfrak{p}^m$, we know that $v(x) = 0$ and $[x] = [1]$, which concludes that the image of x is the identity.

3. By passing to the limit, this item follows by the previous part.

□

Proposition 6.10. The map $\psi : \widehat{\mathcal{O}}^{\times} \to \widehat{\mathcal{O}}^{\times}, \theta \mapsto \theta^{\varphi}/\theta$ is surjective. In particular, for any pair of uniformizers π, π' of $\widehat{K}$, we have $\Theta_{\pi,\pi'}^{\widehat{K},\times} \neq \emptyset$.

Proof. For $x \in \widehat{\mathcal{O}}^{\times}$, we will construct by induction a sequence $(\theta_m)_{m\in\mathbb{N}} \in \mathcal{O}_{K^{\mathrm{ur}}}$ such that

$$\theta_m \equiv \theta_{m+1} \pmod{\mathfrak{p}^m} \text{ and } \varphi(\theta_m) \equiv \theta_m \pmod{\mathfrak{p}^m}.$$

Then the existence of θ is guaranteed by taking the limit of this sequence. In case $m = 1$, take θ_1 such that $\overline{\theta_1}^{q-1} = \overline{x}$ in $\kappa_{\widehat{K}} \cong \kappa_{K^{\mathrm{ur}}} \cong \overline{\mathbb{F}_q}$. We find θ_{m+1} in the form $\theta_m + a\pi^m$ for $a \in \mathcal{O}_{K^{\mathrm{ur}}}$. Indeed, by the definition and the induction hypothesis,

$$\varphi(\theta_{m+1}) = \varphi(\theta_m) + \varphi(a)\pi^m = x\theta_m + \alpha_m\pi^m + \varphi(a)\pi^m, \text{ and } x\theta_{m+1} = x\theta_m + xa\pi^m$$

for some $\alpha_m \in \mathcal{O}_{K^{\mathrm{ur}}}$. Thus, it suffices to show that there exists a such that $\varphi(a) + \alpha_m \equiv xa \pmod{\pi}$, which is obvious because $\overline{\mathbb{F}_q}$ is algebraically closed. □

Corollary 6.11. The $\widehat{K}_f^m$ and $\rho_{f,m}$, hence also $\widehat{K}_f^{\mathrm{LT}}$ and ρ_f, of Proposition 6.9 do not depend on f. (We drop the subscript f and write $\widehat{K}^m$, ρ_m, $\widehat{K}^{\mathrm{LT}}$ and ρ.)

Proof. For f and f' with linear terms π and π', there exists $\theta \in \Theta_{\pi,\pi'}^{\widehat{K},\times}$ by Proposition 6.10. The Lemma 6.6 proved that $\widehat{K}_f^m = \widehat{K}_{f'}^m$. We show that the map $\Psi_{f,m}$ in the proof of Proposition 6.9 does not depend on f and f'. Indeed,

$$\Psi_{f,m}(x)|_{\widehat{K}} = \varphi^{-v(x)} = \Psi_{f',m}(x)|_{\widehat{K}}.$$

Finally, we show that for $\alpha' = [\theta]_{f,f'}(\alpha)$ and $\sigma = \Psi_{f,m}(x)$ we have $\sigma(\alpha') = \left[x\pi'_j\right]_{f',(f')^{\varphi^j}} [\theta]_{f,f'}(\alpha)$. Indeed,

$$\sigma\left([\theta]_{f,f'}(\alpha)\right) = [\theta]_{f,f'}^{\varphi^j}[x\pi_j]_{f,f^{\varphi^j}}(\alpha) = \left[x\pi'_j\right]_{f',(f')^{\varphi^j}}[\theta]_{f,f'}(\alpha).$$

□

Now, we are able to define the maximal Lubin-Tate extension K^{LT}. Let $L|K$ be a finite extension and $f \in \mathcal{O}_L[X]$ be a Lubin-Tate polynomial, set $K^m = K^{\mathrm{ur}}L_f^m$. Then $K^m|K$ is Galois by Proposition 6.9, part 1. By Lemma 4.8, 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

$$K^{\mathrm{LT}} = \bigcup_{m\geq 1} K^m = \widehat{K}^{\mathrm{LT}} \cap K^{\mathrm{sep}}.$$

We have $\mathrm{W}\left(K^{\mathrm{LT}}|K\right) \cong \mathrm{W}\left(\widehat{K}^{\mathrm{LT}}|K\right)$ by Remark 4.12. We call any subextension of $K^{\mathrm{LT}}|K$ a Lubin-Tate extension.

Definition 6.12. We call the inverse of ρ the *Artin map* of K and write $\mathrm{Art}_K : K^\times \longrightarrow \mathrm{Gal}\left(K^{\mathrm{LT}}|K\right)$.

7 Local class field theory

This section discusses the interactions between the Artin map of a local field and of its finite separable extension and introduces some classical results in local class field theory without the local Kronecker-Weber theorem. Throughout this section, for $K'|K$ a finite separable extension, we denote $N(K'|K)$ the image of the norm map from K' to K sending α to

$$N_{K'|K}(\alpha) = \det(\cdot\,\alpha)$$

where $\cdot\,\alpha : K' \to K'$ is the multiplication by α, which is viewed as a K-linear map. If $K'|K$ is infinite and separable, $N_{K'|K}$ is the union of all $N_{L|K}$ where $K \subseteq L \subseteq K'$ a finite extension of K. We will follow Section 5 of [4].

7.1 Galois group

Let $L = K(\mu_{q^n-1})$ be the finite unramified extension of degree n.

Lemma 7.1. 1. For $n \geq 1$, the fixed field of φ^n in $\widehat{K}$ is L.

2. We have $N(L|K) = v^{-1}(n\mathbb{Z}) \subseteq K^\times$.

3. Let $\theta \in \Theta_{\pi,\pi'}^{\widehat{K},\times}$ for $\pi, \pi' \in L$ uniformizers. Then $\theta \in \mathcal{O}_L^\times$ if and only if $N_{L|K}(\pi) = N_{L|K}(\pi')$.

Proof. 1. It is trivial that $\varphi^n(L) = L$. Let y be an element stable under φ^n and π_K be a uniformizer of K, which is also a uniformizer of $\widehat{K}$. Note that $C = \bigcup_{i=0}^{+\infty} \mu_{q^n-1} \cup \{0\}$ is a system of

representatives of $\kappa_{\widehat{K}}$ in $\widehat{K}$. We have $y \in \widehat{K}$ admits a unique presentation

$$y = \pi_K^{v(y)} \sum_{i=0}^{+\infty} a_i \pi_K^i \implies \varphi^n(y) = \pi_K^{v(y)} \sum_{i=0}^{+\infty} a_i^{q^n} \pi_K^i.$$

This means $y = \varphi^n(y)$ if and only if $a_i = a_i^{q^n}$, i.e. $a_i \in \mu_{q^n-1}$ thus $y \in L$.

2. The norm of π_K is π_K^n and for $\alpha \in L$ of valuation j, $v\left(N_{L|K}(\alpha)\right) = nj$ thus $N_{L|K}$ is a subset of $\mathfrak{p}_K^n$. It remains to show that $N_{L|K}\left(\mathcal{O}_L^\times\right) = \mathcal{O}_K^\times$. For $x \in \mathcal{O}_K^\times$, we will show by induction that there exists a sequence $(\theta_m)_{m\in\mathbb{N}} \subseteq \mathcal{O}_L^\times$ such that

$$N_{L|K}(\theta_m) \equiv x \pmod{\mathfrak{p}_L^m} \text{ and } \theta_m \equiv \theta_{m+1} \pmod{\mathfrak{p}_L^m}.$$

By the same method used in Proposition 6.10, we write

$$N_{L|K}(\theta_m) \equiv x + \beta\pi_K^m \pmod{\pi_K^{m+1}} \text{ and } \theta_{m+1} = \theta_m + \alpha\pi_K^m$$

where $\beta \in \mathcal{O}_K$. We need to verify that for $\gamma \in \mathcal{O}_K$, there exists $\alpha \in \mathcal{O}_L$ such that

$$\sum_{k=0}^{n-1} \varphi^k\left(\frac{\alpha}{\theta_m}\right) \equiv \gamma \pmod{\mathfrak{p}},$$

which is equivalent to prove that the polynomial $\sum_{k=0}^{n-1} X^{q^k} - \overline{\gamma}$ has a root in $\mathbb{F}_{q^n}$. The map $\psi : \mathbb{F}_{q^n} \to \mathbb{F}_q$ sending x to $x + x^q + \cdots + x^{q^{n-1}}$ is a group homomorphism with respect to the addition. The kernel of ψ contains at most q^{n-1} elements and the image of ψ contains at most q elements, thus

$$q^n = |\mathrm{Ker}\psi| \cdot |\mathrm{Im}\psi| \geq q^n,$$

hence ψ is surjective which concludes this point.

3. Since $\varphi(\theta)/\theta = \pi'/\pi$, by applying φ and taking the product, we deduce that

$$\frac{\varphi^n(\theta)}{\theta} = \prod_{i=0}^{n-1} \frac{\varphi(\pi')}{\varphi(\pi)} = \frac{N_{L|K}(\pi')}{N_{L|K}(\pi)}.$$

Since $\theta \in \mathcal{O}_L^\times$ if and only if it is stable under φ^n, the proof of this item is complete.

□

Remark 7.2. For $x \in K^\times$ with $v(x) = n > 0$, take a uniformizer $\pi \in L$ with $N_{L|K}(\pi) = x$ and a Lubin-Tate polynomial $f \in \mathcal{O}_L[X]$ with linear term π. The fields $L_f^m = L_\pi^m$ depend only on π, thus only on x by the previous lemma. We denote by $K_x^m = L_f^m$ and

$$K_x^{\mathrm{ram}} = \bigcup_{m\geq 1} K_x^m$$

which are totally ramified over L. By discussion after Corollary 6.11, we have $K^{\mathrm{LT}} = K^{\mathrm{ur}} K_x^{\mathrm{ram}}$.

Proposition 7.3. Let $x \in K^\times$ with $v(x) = n > 0$. The element $\sigma = \mathrm{Art}_K(x)$ satisfies $\sigma|_{K_x^{\mathrm{ram}}} = \mathrm{id}$ and is characterized by this property. Moreover, for all $m \geq 1$, the Artin map induces the isomorphism

$$K^\times / \left((1+\mathfrak{p}^m) \times \langle x \rangle\right) \xrightarrow{\cong} \mathrm{Gal}\left(K_x^m | K\right)$$

sending a class of an element y to γ such that $\gamma|_L = \varphi^{-v(y)}|_L$ and $\gamma(\alpha) = \left[y\pi_{-v(y)}\right]_{f,f}(\alpha)$ where $f \in \mathcal{O}_L[X]$ is a Lubin-Tate polynomial and $\alpha \in \mu_{f,m}^\times$.

Proof. Firstly, σ acts on L as φ^{-n} thus preserves L due to the second part of Lemma 7.1. Moreover, $x = N_{L|K}(\pi) = \pi_n$ thus $[x\pi_{-n}]_{f,\,f^{\varphi^{-n}}} = \mathrm{id}$ on the set $\mu_{f,\,m}$ hence σ fixes K_x^{ram}. Since $K^{\mathrm{LT}} = K^{\mathrm{ur}}K_x^{\mathrm{ram}}$, x is characterised by this property. To verify the isomorphism, consider the restriction

$$\mathrm{Res}_{x,\,m} : \mathrm{W}\left(K^{\mathrm{LT}}|K\right) \longrightarrow \mathrm{Gal}\left(K_x^m|K\right)$$

sending γ to $\gamma|_{K_x^m}$. We show that $\mathrm{Res}_{x,\,m}$ is surjective. Indeed, if $\phi \in \mathrm{Gal}\left(K_x^m|K\right)$, then ϕ is uniquely determined by $\phi|_L$ and $\phi(\alpha)$ for $\alpha \in \mu_{f,\,m}^{\times}$, and from Proposition 6.9, $\mathrm{Res}_{x,\,m}$ is surjective. The composition

$$\mathrm{Res}_{x,\,m} \circ \mathrm{Art}_K : K^{\times} \longrightarrow \mathrm{Gal}\left(K_x^m|K\right)$$

is surjective, and the kernel contains all y such that

$$\mathrm{Art}_K(y)|_L = \mathrm{id}_L \text{ and } \left[y\pi_{-v(y)}\right]_{f,\,f^{\varphi^{-v(y)}}} = [1]_{f,\,f^{\varphi^{-v(y)}}}.$$

Thus $v(y)$ is a multiple of n and $y\pi_{-v(y)} \in (1+\mathfrak{p}^m)$, hence the kernel is $\left((1+\mathfrak{p}^m) \times \langle x\rangle\right)$. □

7.2 Norm groups and base change

Proposition 7.4. If $E|L$ is totally ramified and E contains K_x^{ram}, then $N(E|K) = \langle x\rangle$.

Proposition 7.5. For $\sigma \in \mathrm{W}(K^{\mathrm{sep}}|K)$ 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 7.3, we have $K_x^{\mathrm{ram}} \subset E_\sigma$, and $E_\sigma \cap K^{ur}$ is the unramified extension of K of degree $v(\sigma) = v(x)$. We conclude by proposition 7.4. □

Definition 7.6. For a local field K, denote by $w_K : \mathrm{W}\left(K^{\mathrm{LT}}|K\right) \longrightarrow \mathbb{N}$ the map sending σ to the natural number n such that $\sigma|_{K^{\mathrm{ur}}} = \varphi^{-n} = \mathrm{Frob}_K^n$. Note that $w_K \circ \mathrm{Art}_K = v_K$.

Theorem 7.7 (Base change)**.** For a finite separable $K'|K$, we have $K^{\mathrm{LT}} \subset K'^{\mathrm{LT}}$ and for all $x' \in K'^{\times}$ we have $\mathrm{Art}_{K'}(x')|_{K^{\mathrm{LT}}} = \mathrm{Art}_K(N_{K'|K}(x'))$, i.e. the following diagram commutes

$$\begin{array}{ccc} K'^{\times} & \xrightarrow{\mathrm{Art}_{K'}} & \mathrm{Gal}\left(K'^{\mathrm{LT}}|K'\right) \\ {\scriptstyle N_{K'|K}}\downarrow & & \downarrow{\scriptstyle \text{restriction}} \\ K^{\times} & \xrightarrow{\mathrm{Art}_K} & \mathrm{Gal}\left(K^{\mathrm{LT}}|K\right) \end{array}$$

Proof. For $x \in \mathfrak{p}_{K'} \cap K'^{\times}$, by Zorn's lemma, we can extend $\mathrm{Art}_{K'}(x)$ to an element $\sigma \in \mathrm{W}\left(K^{\mathrm{sep}}|K'\right)$. By Proposition 7.5, we have

$$\langle N_{K'|K}(x)\rangle = N_{K'|K}\left(\langle x\rangle\right) = N_{K'|K}\left(N\left(E_\sigma|K\right)\right) = \langle \mathrm{Art}_K^{-1}\left(\sigma|_{K^{\mathrm{LT}}}\right)\rangle.$$

Let $K' \cap K^{\mathrm{ur}} = K_n$ for some positive integer n, thus $w_{K_n}\left(\sigma|_{K^{\mathrm{LT}}}\right) = w_{K'}(\sigma)$. Indeed, the residue class fields of K_n and K' are both $\mathbb{F}_{q^n}$ and σ acts the same on both κ_{K_n} and $\kappa_{K'}$. Let ζ_1 be a primitive root of unity in K^{ur} and $\zeta_2 = \sigma(\zeta_1)$, thus

$$\zeta_2^{q^{w_K(\sigma)}} = \zeta_1 = \zeta_2^{q^{n\cdot w_{K_n}(\sigma)}}.$$

Note that this equation holds for all root of unity ζ_2, thus

$$w_K\left(\sigma|_{K^{\mathrm{LT}}}\right) = n w_{K_n}(\sigma) = f\left(K'|K\right) w_{K'}(\sigma) = f\left(K'|K\right) v_{K'}(x) = v_K\left(N_{K'|K}(x)\right).$$

We obtain that $N_{K'|K}(x) = \mathrm{Art}_K^{-1}\left(\sigma|_{K^{\mathrm{LT}}}\right)$ because they generate the same subgroup of $K^{\times}$ and they have the same valuations. Therefore, $\sigma|_{K^{\mathrm{LT}}}$ is uniquely determined by x, thus $K^{\mathrm{LT}} \subseteq K'^{\mathrm{LT}}$ and the diagram commutes because $\mathfrak{p}_{K'} \setminus \{0\}$ generates $K'^{\times}$. □

7.3 Local class field theory

Theorem 7.8 (Local class field theory minus local Kronecker-Weber)**.** Let K be a local field.

1. 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 $\mathrm{Art}_K(\pi)|_{K^{ur}} = \mathrm{Frob}_K$, and
   (b) if $K'|K$ is a Lubin-Tate extension, then $\mathrm{Art}_K\left(N\left(K'|K\right)\right)|_{K'} = \mathrm{id}$.

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

2. If $K'|K$ is finite separable, then $K^{\mathrm{LT}} \subseteq K'^{\mathrm{LT}}$ and $\mathrm{Art}_{K'}(x)|_{K^{\mathrm{LT}}} = \mathrm{Art}_K\left(N_{K'|K}(x)\right)$ for all $x \in K'^\times$. The Art_K induces $K^\times/N(K'|K) \xrightarrow{\cong} \mathrm{Gal}\left(K' \cap K^{\mathrm{LT}}|K\right)$, i.e. the following diagram commutes

$$\begin{array}{ccc} K^\times & \xrightarrow{\quad\mathrm{Art}_K\quad} & \mathrm{Gal}\left(K^{\mathrm{LT}}|K\right) \\ {\scriptstyle \mathrm{pr}_{K'}}\downarrow & & \downarrow{\scriptstyle \text{restriction}} \\ K^\times/N\left(K'|K\right) & \xrightarrow{\cong} & \mathrm{Gal}\left(\left(K^{\mathrm{LT}} \cap K'\right)|K\right). \end{array}$$

Proof. 1. The map Art_K satisfies (a) by definition, and (b) by theorem 7.7. Conversely, if Art'_K satisfies (a) and (b), then for any uniformizer π of K, we have by (b) and 6.5 that $\mathrm{Art}'_K(\pi)|_{K_\pi^{ram}} = \mathrm{id}$. This, proposition 7.3 and (a) show that $\mathrm{Art}_K(\pi) = \mathrm{Art}'_K(\pi)$. Since $K^\times$ is generated by the uniformizers, we get $\mathrm{Art}_K = \mathrm{Art}'_K$. The last claim was seen in 6.12 and the paragraph before it.

2. The first part is theorem 7.7, and Art_K induces an isomorphism

$$K^\times/N\left(K'|K\right) \cong \mathrm{W}(K^{\mathrm{LT}}|K)/\mathrm{Im}\left(\mathrm{W}\left(K'^{\mathrm{LT}}|K'\right)\right).$$

   This is isomorphic to $\mathrm{Gal}\left(\left(K' \cap K^{\mathrm{LT}}\right)|K\right)$, because $\mathrm{W}(K^{\mathrm{LT}}|K)$ surjects onto $\mathrm{Gal}\left(\left(K' \cap K^{\mathrm{LT}}\right)|K\right)$ and $\mathrm{W}(K'^{\mathrm{LT}}|K')$ is the inverse image of $\mathrm{W}(K^{\mathrm{LT}}|K)$ under $\mathrm{Gal}(K'^{\mathrm{LT}}|K') \to \mathrm{Gal}(K^{\mathrm{LT}}|K)$. □

The proof of Theorem 7.8.1 shows that we only need totally ramified Lubin-Tate extensions for the characterization of Art_K. By local Kronecker-Weber theorem (see [4], Section 6), it turns out that $K^{\mathrm{LT}} = K^{\mathrm{ab}}$. We state without proof the following remarkable theorem as a consequence of 7.8 and we will use them to discuss $\mathrm{Gal}\left(K^{\mathrm{ab}}|K\right)$.

Theorem 7.9 (existence theorem)**.** Let K be a local field. 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 $N(K'|K) = H$.

Let $\widehat{K^\times}$ be the profinite completion of $K^\times$. By taking the limit over the subgroups of finite index of $K^\times$, and by the result of Theorem 7.8 part 2, we conclude the following description for $\mathrm{Gal}\left(K^{\mathrm{ab}}|K\right)$.

Theorem 7.10. The Artin map Art_K extends to an isomorphism $\widehat{K^\times} \cong \mathrm{Gal}\left(K^{\mathrm{LT}}|K\right)$.

References

[1] JS Milne. Fields and galois theory. 2018.

[2] J. Neukirch and N. Schappacher. *Algebraic Number Theory.* Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[3] D. Ramakrishnan and R.J. Valenza. *Fourier Analysis on Number Fields.* Graduate Texts in Mathematics. Springer New York, 2013.

[4] Teruyoshi Yoshida. Local Class Field Theory via Lubin-Tate Theory. *Annales de la Faculté des sciences de Toulouse : Mathématiques*, Ser. 6, 17(2):411–438, 2008.