EXPLICIT CONSTRUCTION OF LOCAL CLASS FIELD THEORY VIA LUBIN-TATE FORMAL GROUPS

by

Barış Akalın

Submitted to Graduate School of Natural and Applied Sciences
in Partial Fulfillment of the Requirements
for the Degree of Master of Science in
Mathematics

Yeditepe University
2019

EXPLICIT CONSTRUCTION OF LOCAL CLASS FIELD THEORY VIA LUBIN-TATE FORMAL GROUPS

APPROVED BY:

Assist. Prof. Dr. Erol Serbest ....
(Thesis Supervisor)
(Yeditepe University)

Prof. Dr. Kâzım İlhan İkeda İlhan İkeda ....
(Boğaziçi University)

Assist. Prof. Dr. Meltem Özgül ....
(Yeditepe University)

DATE OF APPROVAL: ..../..../2019

To humanity...

ACKNOWLEDGEMENTS

I would wholeheartedly like to express my deepest thanks to my thesis supervisor Asst. Prof. Dr. Erol Serbest. He has always guided me in the Great Forest of Mathematics while encouraging independent work. He was an ideal supervisor.

I would like to thank the Department of Mathematics at Yeditepe University, especially Prof. Dr. Yusuf Ünlü, and also Prof. Dr. İlhan İkeda for their support and guidance.

I would wholeheartedly like to thank my friends Serdar Nair and Mert Tomruk from the deparment. They shared their experience in mathematics and LaTeX without reservation. Thanks to them, now I quitted the habit of drawing boxes for fields.

I also would like to thank my friends and my family, especially my wife Çiğdem Öz Akalın for encouragement and support.

ABSTRACT

EXPLICIT CONSTRUCTION OF LOCAL CLASS FIELD THEORY VIA LUBIN-TATE FORMAL GROUPS

Class field theory constitutes a subsection in algebraic number theory which, in particular, investigates Abelian extensions of global fields. On the other hand, local class field theory was introduced by Helmut Hasse and studies the Abelian extensions of local fields with respect to the objects related to the ground field. It was later developed by various important mathematicians such as Schmidt, Chevalley, Nakayama, Artin, Kato and others. There are several approches to local class field theory: Hasse approach, cohomological approach, the explicit methods of Neukirch and Hazewinkel and others. Similar to the theory of complex multiplication on elliptic curves, in their paper in 1965, Lubin and Tate showed that the main theorems in local class field theory can be proved via formal groups over local fields. Using the Lubin-Tate formal groups, they found an explicit way of generating Abelian extensions of local fields. Here, we will study Lubin-Tate theory in detail.

ÖZET

LUBIN-TATE FORMEL GRUPLARI ARACILIĞIYLA YEREL SINIF CİSİM KURAMININ APAÇIK İNŞASI

Sınıf cisim kuramı, cebirsel sayı kuramının, global cisimlerin Abelyen genişlemelerini de özel olarak inceleyen bir dalıdır. Diğer yandan, yerel sınıf cisim kuramı Helmut Hasse tarafından ortaya atılmıştır ve yerel cisimlerin Abelyen genişlemelerini, taban cisim ile ilişkili nesneler yönünden incelemektedir. Bu kuram daha sonra Schmidt, Chevalley, Nakayama, Artin, Kato gibi çeşitli önemli matematikçiler tarafından geliştirilmiştir ve genelleştirilmiştir. Yerel sınıf cisim kuramının inşası için birçok yaklaşım bulunmaktadır: Hasse yaklaşımı, kohomolojik yaklaşım, Neukirch ve Hazewinkel'in apaçık yöntemleri vb. Eliptik eğrilerdeki karmaşık çarpım teorisine benzer şekilde, 1965'te yayınlanan makalelerinde, Lubin ve Tate, yerel cisimler üzerindeki formel grupların, yerel sınıf cisim kuramındaki temel teoremlerin kanıtlanması için kullanılabileceğini gösterdiler. Lubin-Tate formel gruplarını kullanarak, yerel cisimlerin Abelyen genişlemelerini üretmek için apaçık bir yol buldular. Bu tezde Lubin-Tate kuramını detaylı bir şekilde inceleyeceğiz.

TABLE OF CONTENTS

LIST OF SYMBOLS/ABBREVIATIONS

Art_k	Artin map for a local field k
$e_{k'/k}$	The ramification index of the extension k'/k
$f_{k'/k}$	The residue degree of the extension k'/k
$\mathbb{F}_p$	Finite field with p elements
φ_k	Frobenius automorphism for the extension k_{ur}/k
$F_f(X,Y)$	Lubin-Tate formal group with respect to formal power series f
$\mathrm{Gal}(L/K)$	The Galois group of the extension L/K
$\underset{i\in I}{\varprojlim} G_i$	The inverse limit of the groups G_i's
k	A local field
$\hat{k}$	The completion of k
k^{alg}	A fixed algebraic closure of k
k^{ab}	The maximal Abelian extension of k in k^{alg}
k_{ur}	The maximal unramified extension of k in k^{ab}
κ_k	The residue field of a local field k
$\mathcal{O}_k$	The valuation ring of a local field k
$N_{k'/k}$	The norm function for the extension k'/k
$N(F/k)$	The norm group of the extension F/k
$NU(F/k)$	The unit norm group of the extension F/k
$\mathfrak{p}_k$	The maximal ideal of a valuation ring $\mathcal{O}_k$
$\mathbb{Q}$	The set of rational numbers
$\mathbb{Q}_p$	The set of p-adic numbers
$\mathbb{R}$	The set of real numbers
$T_{k'/k}$	The trace function for the extension k'/k
$\mathcal{U}_k$	The unit group of a valuation ring $\mathcal{O}_k$
$\mathcal{U}_n$	Higher unit groups of the unit group $\mathcal{U}_k$
v	A valuation on a field
$\mathbb{Z}$	The set of integers
$\mathbb{Z}_p$	The set of p-adic integers
$\widehat{\mathbb{Z}}$	The profinite completion of $\mathbb{Z}$

1. INTRODUCTION

Class field theory can be described as one of the most influential achivements of algebraic number theory in the 20th century. The term “class field”, coined by Weber, refers to an Abelian field extension satisfying a technical property that is related to ideal class groups. The aim of class field theory is to describe the Galois groups of Abelian extensions of a global field K based on our knowledge of K itself (more specifically, the arithmetic of K which is the study of the ideals of K, the quotient rings determined by the ideals of K, the ideal class groups etc.). The Kronecker-Weber theorem is an early result stating that, if K is a finite Abelian extension $\mathbb{Q}$, then it is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$ for some m. Artin, Weber, Tagaki and Hilbert were among the mathematicians who developed class field theory [1].

Local class field theory was introduced by Helmut Hasse and studies the abelian extensions of local fields with respect to the objects related to the ground field as in the global case. It was later developed and generalized by various mathematicians such as Schmidt, Chevalley, Nakayama, Artin, Kato and others. In this theory, the Galois group of k^{ab}, the maximal Abelian extension of a local field k can be described via the local Artin map which is an injective homomorphism from $k^\times$ to $\mathrm{Gal}(k^{ab}/k)$. For example, for a finite Abelian extension L of k, the local Artin map induces the isomorphism $k^\times/N_{L/k}(L^\times) \cong \mathrm{Gal}(L/k)$. There are several approches to local class field theory: Hasse approach, the cohomological approach, the explicit methods of Neukirch and Hazewinkel [2] and others.

Suggested by the theory of complex multiplication on elliptic curves, in their paper [3] in 1965, Lubin and Tate showed that, using the so-called Lubin-Tate formal groups over local fields one can construct k^{ab} and the local Artin map explicitly. In this thesis, we will study Lubin-Tate theory in detail.

This thesis consists of five chapters:

After discussing infinite Galois theory and profinite groups in the first chapter, we give basic theory of local fields in the second chapter.

In the third chapter we introduce formal power series over arbitrary rings and study their properties.

The fourth chapter explains the formal groups and particularly Lubin-Tate formal groups.

In the final chapter, we define special (totally ramified) extensions of a local field k via Lubin-Tate formal groups and use these extensions to construct k_π which is actually a maximal totally ramified extension in k^{ab}. Then we define a homomorphism ρ_k: $k^\times \to \mathrm{Gal}(k^{ab}/k)$ and using this homomorphism, we prove that $k^{ab} = k_{ur}k_\pi$, here the field k_{ur} is the maximal unramified extension of k. Also we prove that ρ_k is actually the local Artin map of k.

We claim no originality in this thesis.

2. PRELIMINARIES

In this chapter, we will review Infinite Galois Theory and Profinite Groups very briefly and state the important theorems without proofs, which will be used in the text frequently. The main references for this chapter are Chapter 1 of [4], Chapter 6 of [5], Chapter 3 of [6] and [7].

2.1. INFINITE GALOIS THEORY

Definition 2.1.1. A field extension R/K is called **Galois extension** if it is algebraic, seperable and normal.

Definition 2.1.2. Let R/K be any Galois extension (infinite or finite). We can endow $\mathrm{Gal}(R/K)$ with a so-called **Krull topology**. This makes $\mathrm{Gal}(R/K)$ a topological group. In this topology, for any $\sigma \in \mathrm{Gal}(R/K)$, the cosets $\sigma\mathrm{Gal}(R/E)$ are taken as a basis of neighborhoods of σ, where E/K runs over all (finite) Galois extensions of K contained in R.

Theorem 2.1.1. *Let R/K be a Galois extension. The Galois group* $\mathrm{Gal}(R/K)$ *is Hausdorff and compact in Krull topology.*

There is a fundamental theorem (in Galois theory) which holds for the infinite case via Krull topology and is an extension of the fundamental theorem for the finite case:

Theorem 2.1.2. *Let R/K be a Galois extension. The map*

$$E \mapsto \mathrm{Gal}(R/E) \tag{2.1}$$

is a bijection between

$$\left\{\begin{array}{c}\textit{the subextensions } E \\ \textit{of } R/K\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\textit{the closed subgroups } \mathrm{Gal}(R/E) \\ \textit{of } \mathrm{Gal}(R/K)\end{array}\right\}, \tag{2.2}$$

that restricts to a bijection

$$\left\{\begin{matrix} \textit{the finite subextensions } E \\ \textit{of } R/K \end{matrix}\right\} \leftrightarrow \left\{\begin{matrix} \textit{the open subgroups } \mathrm{Gal}(R/E) \\ \textit{of } \mathrm{Gal}(R/K) \end{matrix}\right\}. \tag{2.3}$$

Also, in Gal(R/K), *assume H is a closed subgroup. Then H is normal iff the corresponding subextension is a Galois extension.*

2.2. PROFINITE GROUPS

Definition 2.2.1. Let P be a set. Denote a relation by the symbol $\leq$ on this set. This relation is called a **partial order** if it satisfies the following for all $e, f, g \in P$: $e \leq e$; this is called reflexivity. $e \leq f$ and $f \leq e$ implies $e = f$; this is called anti-symmetry. $e \leq f$ and $f \leq g$ implies $e \leq g$; this is called transitivity. The set P together with a partial order $\leq$ is often called a **poset**.

Definition 2.2.2. If a poset $(I, \leq)$ has the following property, then it is called a **directed poset**: Take $e, f \in I$. Then $\exists\ g \in I$ satisfying $e \leq g$ and $f \leq g$.

Definition 2.2.3. Let $(I, \leq)$ be a directed poset and assume that there is a group H_i for every $i \in I$ and homomorphisms $t_{ij} : \sigma_j \to \sigma_i$ for all $i, j \in I$ with $i \leq j$ satisfying the conditions below:

(i) t_{ii} is the identity on H_i for all $i \in I$,

(ii) $t_{ik} = t_{ij} \circ t_{jk}$ for all $i \leq j \leq k$.

The maps t_{ij}'s are called **transition maps**. The set $((H_i)_{i \in I}, (t_{ij})_{i \leq j,\ i,j \in I})$ is called an **inverse system of groups**.

The inverse (projective) limit of this inverse system is defined as

$$\varprojlim_{i \in I} H_i = \left\{ (g_i)_{i \in I} \in \prod_{i \in I} H_i \mid t_{ij}(g_j) = g_i,\ i \leq j \text{ and } i, j \in I \right\}, \tag{2.4}$$

if it exists.

Remark. If H_i's are topological groups and t_{ij}'s are continuous homomorphisms, then the inverse limit $\varprojlim_{i\in I} H_i$ can be thought of as a topological group through embedding into $\prod_{i\in I} H_i$.

Example 1. Let $G_n = \mathbb{Z}/n\mathbb{Z}$ for $n \in \mathbb{N}$. Define a partial order $\leq$ on $\mathbb{N}$: $r \leq n$ if $r|n$. Define

$$f_{rn} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}, \tag{2.5}$$

$$a \mapsto a \ (\mathrm{mod}\ r). \tag{2.6}$$

So we have

$$\varprojlim_{n\in\mathbb{N}} G_n = \left\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z} \mid a_n \equiv a_r \ (\mathrm{mod}\ r),\ \ r|n \text{ and } r,n \in \mathbb{N} \right\}. \tag{2.7}$$

An equivalent definition of the inverse limit can be given as follows: Let Y be a topological group and $((X_i)_{i\in I}, (\sigma_{ij})_{i\leq j,\ i,j\in I})$ an inverse system over a directed poset $(I, \leq)$, where X_i's are topological groups, and $\psi_i : Y \to X_i$ continuous group homomorphisms for $i \in I$. The maps ψ_i's are called **compatible** if $\sigma_{ij}\psi_j = \psi_i$, $i \leq j$. A topological group X along with compatible continuous homomorphisms $\sigma_i : X \to X_i$ is called an **inverse limit** (of the inverse system) if the following is satisfied, which is called the universal property:

If Z denotes a topological group and $\{ \psi_i : Z \to X_i \}$ is a set of compatible continuous homomorphisms, there is a unique continuous homomorphism $\psi : Z \to X$ such that $\sigma_i\psi = \psi_i$ for all $i \in I$.

$$\begin{tikzcd} Z \arrow[r, "\psi"] \arrow[dr, "\psi_i"] & X \arrow[d, "\sigma_i"] \\ & X_i \end{tikzcd} \tag{2.8}$$

Theorem 2.2.1. *Let*

$$(I, \leq)$$

be a directed poset and $((X_i)_{i\in I}, (\sigma_{ij})_{i\leq j,\ i,j\in I})$ an inverse system over I, where X_i's are topological groups. Then there is an inverse limit of this inverse system and the limit is unique in the following manner: If (X, σ_i) and (Y, ψ_i) are two inverse limits of the inverse system $((X_i)_{i\in I}, (\sigma_{ij})_{i\leq j,\ i,j\in I})$, then there is a unique homeomorphism $\psi : X \to Y$ such that $\psi_i\psi = \sigma_i$ for $i \in I$.

Definition 2.2.4. A topological group that is Hausdorff, compact and has a neighborhood basis of the identity, which consists of normal subgroups, is called a **profinite group**.

We have the following theorems about the profinite groups:

Theorem 2.2.2. *If G is a profinite group and N runs over the normal open subgroups of G, then*

$$G \cong \varprojlim_{N} G/N, \tag{2.9}$$

the transition maps being natural projections. Conversely, let $((G_i)_{i\in I}, (f_{ij})_{i\leq j,\, i,j\in I})$ be an inverse system, where G_i's are finite groups. Then $\varprojlim_{i\in I} G_i$ is a profinite group.

Theorem 2.2.3. *Let G be a topological compact group and $\{H_i \mid i \in I\}$ a family of normal closed subgroups of finite index such that*
(i) For every finite subset J of I, there exists $i \in I$ such that $H_i \subseteq \bigcap_{j\in J} H_j$,
(ii) $\bigcap_{i\in I} H_i = 1$.
Then $G \cong \varprojlim_{i\in I} G/H_i$ as topological groups.

By using Krull topology, it can be proved that Galois groups are profinite groups and we can write them in the form of inverse limits. Let R/K be a Galois extension. According to Theorem 2.1.2, $\mathrm{Gal}(R/K)$ is a Hausdorff space and compact group and by definition, its basis of open neighbourhoods of $1_{\mathrm{Gal}(R/K)}$ is given by $\mathrm{Gal}(R/E)$, where E runs over the finite Galois subextensions of R/K, all of which are open normal subgroups and they are the only such subgroups. So,

$$\mathrm{Gal}(R/K) \cong \varprojlim_{E/K \text{ is finite Galois}} \mathrm{Gal}(R/K)/\mathrm{Gal}(R/E) \cong \varprojlim_{E/K \text{ is finite Galois}} \mathrm{Gal}(E/K). \tag{2.10}$$

Example 2. We have

$$\mathrm{Gal}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right) \cong \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p). \tag{2.11}$$

3. BASIC THEORY OF LOCAL FIELDS

In this chapter, the theory of local fields will be discussed briefly, which will be necessary in the following chapters and we will not give any proofs here. The main references for this chapter are Chapters 1, 2, and 3 of [8], Chapter 2 of [9], [10], [11], [12], [13] and [14].

3.1. VALUATIONS ON A FIELD

Definition 3.1.1. Let k be a field. A mapping $v : k \to \mathbb{R} \cup \{+\infty\}$ satisfying the following conditions is called a **valuation** on the field k:

(i) If $x \neq 0$, then $v(x) \in \mathbb{R}$. We set $v(0) = +\infty$.

(ii) For $x, y \in k$,

$$v(x + y) \geqslant \min\{v(x), v(y)\}. \tag{3.1}$$

(iii) For $x, y \in k$,

$$v(xy) = v(x) + v(y). \tag{3.2}$$

We denote a field k with the valuation v shortly as (k, v).

Remark. By (iii) above, v defines a homomorphism

$$v : k^{\times} \longrightarrow \mathbb{R}^{+},$$

where $\mathbb{R}^{+}$ denotes the additive group of $\mathbb{R}$.

Remark. Let v be a valuation on a field k. By Definition 3.1.1, the following properties are easy to show:

$$v(\pm 1) = 0, \tag{3.3}$$

$$v(-x) = v(x), \tag{3.4}$$

$$v(x) < v(y) \implies v(x + y) = v(x), \tag{3.5}$$

where $x, y \in k$.

Example 3. The mapping $v : k \to \mathbb{R} \cup \{+\infty\}$ defined as:

$$v(x) = \begin{cases} 0 & \text{if} \quad x \neq 0, \\ +\infty & \text{if} \quad x = 0, \end{cases} \tag{3.6}$$

is a valuation on k and called **trivial valuation**.

Example 4. Take a prime number p. Every non-zero rational number x can be written in a unique way as $x = p^e y$, where e is an integer, y is a rational number whose numerator and denominator are not divisible by p. We define a mapping v_p on $\mathbb{Q}$ by

$$v_p(x) = \begin{cases} +\infty & \text{if } x = 0, \\ e & \text{if } x \neq 0 \text{ and } x = p^e y. \end{cases} \tag{3.7}$$

The mapping can be shown to be a valuation, which is called the **p-adic valuation** of $\mathbb{Q}$.

Example 5. Let k be a field, $k(X)$ the field of all rational functions in an indeterminate X with coefficients in k. Every $f \in k(X)$ can be written uniquely: $f = X^e g$, here e is an integer and $g \in k(X)$, which is not divisible by X. Now we define a valuation v on $k(X)$ such that $v(X) = 1$ as in the Example 4.

Example 6. Let k be a field, $G \leqslant \mathbb{R}^+$ (the additive group), and $\gamma \in \mathbb{R}^+$. Suppose $v : k \to G \cup \{+\infty\}$ is a surjective valuation. For $f = \sum_{i=0}^{n} a_i X^i \in k[X]$, define the mapping

$$w : k[X] \to \mathbb{R}^+ \cup \{+\infty\},$$

by the rule

$$w(f) = \begin{cases} +\infty & \text{if} \quad f = 0, \\ \min\limits_{0 \leq i \leq n} \{v(a_i) + i\gamma\} & \text{otherwise}. \end{cases} \tag{3.8}$$

Consider the map

$$\widetilde{w} : k(X) \to \mathbb{R}^+ \cup \{+\infty\},$$

defined by

$$\widetilde{w}\left(\frac{f}{g}\right) = w(f) - w(g), \tag{3.9}$$

where $f, g \in k[X] \setminus \{0\}$. Then $\widetilde{w}$ is a valuation that extends v.

Let v be a valuation on a field k. Introduce

$$\mathcal{O}_k = \{x \in k \mid v(x) \geq 0\}, \tag{3.10}$$

$$\mathfrak{p}_k = \{x \in k \mid v(x) > 0\}, \text{ and} \tag{3.11}$$

$$\kappa_k = \mathcal{O}_k/\mathfrak{p}_k. \tag{3.12}$$

Here, $\mathcal{O}_k$ (called the **valuation ring**) and $\mathfrak{p}_k$ (called the **maximal ideal**) become a subring of k and a maximal ideal of $\mathcal{O}_k$, respectively so that κ_k (called the **residue field**) is a field. In addition, define the **unit group** $\mathcal{U}_k$ of the valuation ring $\mathcal{O}_k$ by

$$\mathcal{U}_k = \{x \in \mathcal{O}_k \mid v(x) = 0\}. \tag{3.13}$$

Remark. Note: the maximal ideal $\mathfrak{p}_k$ in $\mathcal{O}_k$ is unique since $\mathfrak{p}_k = \mathcal{O}_k \setminus \mathcal{U}_k$. In other words, $\mathcal{O}_k$ is a local ring.

Definition 3.1.2. Let k be a field. A map on k,

$$|\cdot| : k \mapsto \mathbb{R}, \tag{3.14}$$

is called an **absolute value** if it satisfies the following properties:

(i) $|x| = 0 \iff x = 0$,

(ii) $|x| \geq 0$,

(iii) $|xy| = |x| \cdot |y|$,

(iv) $|x + y| \leq |x| + |y|$,

for all $x, y \in k$.

Definition 3.1.3. Let k be a field and $|\cdot|$ an absolute value on k. If $|\cdot|$ satisfies the condition

$$|x + y| \leq \max\{|x|, |y|\}, \quad \forall x, y \in k, \tag{3.15}$$

then it is called **non-archimedean**.

In the following theorem, a correspondence between the non-archimedean absolute values and valutions is provided. So if we have a valution, we can define a topology on our field just like in the metric spaces.

Theorem 3.1.1. *Let k be field, $|\cdot|$ a non-archimedean absolute value on k, $s \in \mathbb{R}$, $s > 0$. The map*

$$v_s: \quad k \quad \to \quad \mathbb{R} \cup \{+\infty\}, \tag{3.16}$$

$$x \quad \mapsto \quad \begin{cases} -s \log |x| & x \neq 0, \\ +\infty & x = 0, \end{cases} \tag{3.17}$$

is a valuation on k. Also, if s and $s' \in \mathbb{R}$, s, $s' > 0$ and $s \neq s'$, then v_s is equivalent to $v_{s'}$ (refer to definition 3.1.5). Conversely, if v is a valuation on k and $l \in \mathbb{R}$, $l > 1$, then the map

$$|\cdot|_l: \quad k \quad \to \quad \mathbb{R}, \tag{3.18}$$

$$x \quad \mapsto \quad \begin{cases} l^{-v(x)} & x \neq 0, \\ 0 & x = 0, \end{cases} \tag{3.19}$$

is an absolute value on k. Also, if l and $l' \in \mathbb{R}$, l, $l' > 1$ and $l \neq l'$, then $|\cdot|_l$ is equivalent to $|\cdot|_{l'}$.

According to Theorem 3.1.1, we can use valuations and absolute values interchangeably and in this thesis we'll study and describe our theorems in terms of valuations.

Definition 3.1.4. A topological ring k which is a field, where, in addition, the inverse mapping $a \mapsto a^{-1}$ is continuous on $k \backslash \{0\}$, is called a **topological field**.

Now we can define a topology on k. If, for each $x \in k$ and $\alpha \in \mathbb{R}$, we take the family of open balls $B(x, \alpha) = \{y \mid v(x - y) > \alpha \text{ and } y \in k\}$, we define a Hausdorff topology on k. This topology is called **v-topology** on k. Now k is a topological field in that topology. By definition, $\mathcal{O}_k$ is a closed set and $\mathfrak{p}_k$ is an open set in k.

Definition 3.1.5. If two valuations defined on the same field k produce the same topology, they are called **equivalent valutions**.

Remark. Equivalently, two valuations v and μ on k are equivalent if there exist an $\alpha \in \mathbb{R}_{>0}$

such that

$$v(x) = \alpha \cdot \mu(x),\ \forall x \in k. \tag{3.20}$$

In this case, we write $v \sim \mu$.

Remark. The valuation ring, the maximal ideal and the residue field as well as the unit group of equivalent valuations are the same.

In terms of valuations, the limit of a sequence $(x_n) \in k$ can be defined as follows:

$$\lim_{n\to+\infty} x_n = x \Leftrightarrow \lim_{n\to+\infty} v(x_n - x) = +\infty. \tag{3.21}$$

Similarly, a sequence $(x_n) \in k$ is called a Cauchy sequence in the v-topology if,

$$v(x_n - x_m) \to +\infty \text{ as } n,\ m \to +\infty. \tag{3.22}$$

Definition 3.1.6. A valuation v on a field k is called **complete** if every Cauchy sequence in v-topology is convergent.

Since every valuation corresponds to a non-archimedean absolute value, in k:

$$\sum_{n=1}^{\infty} x_n = \lim_{i\to+\infty} \sum_{n=1}^{i} x_n \Leftrightarrow v(x_n) \to +\infty \text{ as } n \to +\infty. \tag{3.23}$$

Definition 3.1.7. Let k be a field. A valuation v on k is called **discrete** if $v(k^\times)$ is a discrete subgroup of $\mathbb{R}^+$. That means, $v(k^\times)$ is equal to $\mathbb{Z}\beta$ for some real number $\beta \geq 0$. When $\beta = 1$, i.e. $v(k^\times) = \mathbb{Z}$, we say the valuation is **normalized**.

Let k' be an extension field of k and v' be a valuation on k'. It can be shown that $v'|_k$ is also a valuation on k and it's called a **restriction** of v' to the subfield k. Conversely, if v is valuation on k, any valuation v' of k' satisfying $v'|_k = v$, is called an **extension** of v to k'.

Let $v'|_k = v$. The following hold:

$$\mathcal{O}_{k'} = \{x' \in k' \mid v'(x') \geq 0\}, \tag{3.24}$$

$$\mathfrak{p}_{k'} = \{x' \in k' \mid v'(x') > 0\}, \tag{3.25}$$

$$\kappa_{k'} = \mathcal{O}_{k'}/\mathfrak{p}_{k'}, \tag{3.26}$$

$$\mathcal{O}_k = \mathcal{O}_{k'} \cap k, \tag{3.27}$$

$$\mathfrak{p}_k = \mathfrak{p}_{k'} \cap k = \mathfrak{p}_{k'} \cap \mathcal{O}_k. \tag{3.28}$$

Since,

$$\kappa_k = \mathcal{O}_k/\mathfrak{p}_k = \mathcal{O}_k/(\mathfrak{p}_{k'} \cap \mathcal{O}_k) \cong (\mathcal{O}_k + \mathfrak{p}_{k'})/\mathfrak{p}_{k'} \subseteq \mathcal{O}_{k'}/\mathfrak{p}_{k'} = \kappa_{k'}, \tag{3.29}$$

we can embed κ_k of v into $\kappa_{k'}$ of v' naturally.

Let

$$e_{k'/k} = [v'(k'^{\times}) : v(k^{\times})] \text{ and } f_{k'/k} = [\kappa_{k'} : \kappa_k]. \tag{3.30}$$

Here $[v'(k'^{\times}) : v(k^{\times})]$ is the group index and $[\kappa_{k'} : \kappa_k]$ is the degree of $\kappa_{k'}/\kappa_k$. Then $e_{k'/k}$ is called the **ramification index** and $f_{k'/k}$ is called the **residue degree** of v'/v.

We have the following central theorem in the valuation theory:

Theorem 3.1.2. *Let v be a complete valuation on k and k' an algebraic extension of k. Then v can be uniquely extended to a valuation v' on k' satisfying $v'|_k = v$. If k'/k is a finite extension, then v' is also complete and we have the following:*

$$v'(x') = \frac{1}{n} \cdot v(N_{k'/k}(x')),\ \forall x' \in k', \tag{3.31}$$

where $n = [k' : k]$ is the extension degree and $N_{k'/k}$ is the norm map of k'/k.

Corollary 3.1.2.1. *Let k'/k, v and v' be as in Theorem 3.1.2 and σ an automorphism of k' over k. Then we have the following:*

$$\begin{gathered} v'(\sigma(x')) = v'(x'),\ \forall x' \in k', \\ \sigma(\mathcal{O}_{k'}) = \mathcal{O}_{k'},\ \sigma(\mathfrak{p}_{k'}) = \mathfrak{p}_{k'}. \end{gathered} \tag{3.32}$$

This implies that σ is a homeomorphism of k' in v'-topology. Also, σ induces an automorphism

σ' of the residue field $\kappa_{k'}$.

Let v be a valuation on k. It can be shown that there is a field k' such that $k \subseteq k'$ and an extension v' of v which is complete and also k is dense in k' with respect to v'-topology of k'. This field k' is called **the completion** of k since it is unique (up to isomorphism). As k is dense in k', any x' in k' can be described as the limit of a sequence (x_n) in k in the v'-topology. So,

$$x' = \lim_{n\to\infty} x_n, \tag{3.33}$$

and then the following hold:

$$v'(x') = \lim_{n\to\infty} v'(x_n) = \lim_{n\to\infty} v(x_n), \tag{3.34}$$

$$v'(k'^{\times}) = v(k^{\times}), \tag{3.35}$$

$$\kappa_{k'} \cong \kappa_k, \tag{3.36}$$

$$e_{k'/k} = f_{k'/k} = 1. \tag{3.37}$$

Example 7. Let k' be an extension field of k and v' an extension of v on k to the extension field $k' : v'|_k = v$. Suppose v' is complete. Denote the topological closure of k in k' in v'-topology by $\bar{k}$. Then, we know from the theory of the topological fields that $\bar{k}$ is a subfield of k' and $(\bar{k}, \bar{v})$ with $\bar{v} = v'|_{k'}$ which is a completion of (k, v).

3.2. COMPLETE FIELDS

Definition 3.2.1. Let v be a valuation on a field k. If v is complete and normalized, then k is called **a complete field**.

Let v be a normalized valuation on a field k and (k', v') the completion of (k, v). Note that $v'(k'^{\times}) = v'(k^{\times}) = \mathbb{Z}$ and (k', v') is a complete field.

Example 8. Let v_p be the p-adic valuation on the field $\mathbb{Q}$. Then v_p is a normalized valuation (that is, $v_p(p) = 1$). The completion of $\mathbb{Q}$ with respect to v_p is the complete field $(\mathbb{Q}_p, v_p)$ of **p-adic numbers**. Its valuation ring $\mathbb{Z}_p$ is called the ring of **p-adic integers** and the maximal ideal of this ring is $p\mathbb{Z}_p$; it can be shown that the residue field of $\mathbb{Q}_p$ is the finite field of $\mathbb{F}_p$ of p elements.

Example 9. Let F be a field and assume T is an indeterminate. Let $F((T))$ be the set of all formal Laurent series:

$$\sum_{n=i}^{+\infty} a_n T^n,\ a_n \in F,\ i \in \mathbb{Z}. \tag{3.38}$$

Define a mapping v by

$$v(x) = \begin{cases} +\infty & \text{if } x = 0, \\ i & \text{if } x \neq 0,\ x = \sum_{n=i}^{+\infty} a_n T^n,\ \ a_i \neq 0. \end{cases} \tag{3.39}$$

It can be shown that $F((T))$ is the completion of the field with the valuation which were described in Example 5. The valuation ring $F[[T]]$ is the all (integral) power series in T over F (i.e. $i \geq 0$ in the Laurent series expansion) and the maximal ideal is $TF[[T]]$. Here, the residue field of the valuation is isomorphic to F.

Let (k, v) be a complete field. As $v(k^\times) = \mathbb{Z}$, there is an element π_k in k satisfying $v(\pi_k) = 1$. Such elements are called **prime elements** or **uniformizers** of k. Since $\mathfrak{p}_k = \{x \in k \mid v(x) \geq 1\}$, we see that $\mathfrak{p}_k = (\pi_k) = \pi_k \mathcal{O}_k$. For any integer $n \geq 0$ define,

$$\mathfrak{p}_k^n = (\pi_k^n) = \pi_k^n \mathcal{O}_k = \{x \in k \mid v(x) \geq n\}. \tag{3.40}$$

These are the all ideals of $\mathcal{O}_k$ and the sequence

$$\{0\} \subset \cdots \subset \mathfrak{p}_k^2 \subset \mathfrak{p}_k \subset \mathfrak{p}_k^0 = \mathcal{O}_k \tag{3.41}$$

describes the ideal structure of $\mathcal{O}_k$. So $\mathcal{O}_k$ is a PID, i.e. a principal ideal domain. In addition to this, $v(x) \geq n$ iff $v(x) > n - 1$ for any $n \in \mathbb{Z}$. So all the ideals are open and closed at the same time and they form a neighborhood base of 0 in the v-topology of k. Generally, let a be an $\mathcal{O}_k$-submodule of k not equal to 0 or k. The set $\{v(x) \mid x \in a, x \neq 0\}$ is bounded below (otherwise we can generate all elements of k since a is an $\mathcal{O}_k$-submodule of k). If n is the minimum of integers in the set, then

$$a = \{x \in k \mid v(x) \geq n\} = \pi_k^n \mathcal{O}_k. \tag{3.42}$$

Such $\mathcal{O}_k$-submodules of k are called **ideals** of k.

Now we consider the multiplicative group $k^\times$ of k. Let $x \in k^\times$. Since $x \neq 0$, $v(x) = n \in \mathbb{Z}$.

We see that $v(x\pi_k^{-n}) = 0$ which implies $x = u\pi_k^n$, for some $u \in \mathcal{U}_k$. Then

$$k^\times = \mathcal{U}_k \times < \pi_k > . \tag{3.43}$$

Define the following subgroups:

$$\mathcal{U}_0 = \mathcal{U}_k,\ \mathcal{U}_n = 1 + \mathfrak{p}_k^n = \{x \in \mathcal{O}_k \mid x \equiv 1 \bmod \mathfrak{p}_k^n\}, \tag{3.44}$$

for $n \geq 1$.
Let κ_k^+ and $\kappa_k^\times$ denote the additive and the multiplicative groups of κ_k. The following sequences of subgroups of $k^\times$ and isomorphisms exist:

$$\{1\} \subset \cdots \subset \mathcal{U}_3 \subset \mathcal{U}_2 \subset \mathcal{U}_1 \subset \mathcal{U}_0 = \mathcal{U}_k, \tag{3.45}$$

$$\mathcal{U}_0/\mathcal{U}_1 \cong \kappa_k^\times,\ \ \mathcal{U}_n/\mathcal{U}_{n+1} \cong \kappa_k^+, \tag{3.46}$$

for $n \geq 1$.
Similarly, the groups U_n's, $n \geq 0$ are open in $k^\times$ and constitute a neighborhood base of 1 in the v-topology of $k^\times$.

We continue assuming that (k, v) is a complete field. Let A be a complete set of representatives of the residue field κ_k. If, for each $n \in \mathbb{Z}$, we fix an element π_n in k such that $v(\pi_n) = n$, then we can express every element of k in the form of a special infinite sum as explained below:

Theorem 3.2.1. *(i) Each x in k can be expressed (uniquely) as follows:*

$$x = \sum_{n=i}^{+\infty} a_n \pi_n, \tag{3.47}$$

with $a_n \in A$. If $x \neq 0$, $a_i \neq 0$, and $a_s = 0$ for all $s < i$, then $v(x) = i$.
(ii) Let

$$x = \sum a_n \pi_n \ \ and\ \ y = \sum b_n \pi_n,\ \ a_n, b_n \in A. \tag{3.48}$$

Then for any integer i, $v(x - y) \geq i$ iff $a_n = b_n$ $\forall n < i$.

Example 10. If we consider $\mathbb{Q}_p$, then we can take $A = \{0, 1, \ldots, p - 1\}$ and $\pi = p$. Then every p-adic integer can be written (uniquely) as follows:

$$x = \sum_{n=0}^{+\infty} a_n p^n, \quad a_n \in A. \tag{3.49}$$

3.3. FINITE EXTENSIONS OF COMPLETE FIELDS

Let (k, v) be a complete field.

Definition 3.3.1. If a complete field (k', v') is an extension of a complete field (k, v) such that $v'|_k \sim v$, then k' is called a **complete extension** of k.

Let $\mu = v'|_k$. Then $e_{k'/k}$ is the **ramification index** of k'/k (an extension of complete fields) an $f_{k'/k}$ denotes the **residue degree** of k'/k, respectively. Since $\mu = \alpha v,\ \alpha > 0$ and $\mu(k^{\times}) = \alpha v(k^{\times}) = \alpha\mathbb{Z}$,

$$e_{k'/k} = [v'(k^{\times}) : \mu(k^{\times})] = [\mathbb{Z} : \alpha\mathbb{Z}] = \alpha. \tag{3.50}$$

Now we see that $v'|_k = e_{k'/k}v$ and $e_{k'/k} < +\infty$. But this may not be true for $f_{k'/k}$. If (k'', v'') is a complete extension of (k', v'), then

$$e_{k''/k} = e_{k''/k'} \cdot e_{k'/k}, \tag{3.51}$$

and

$$f_{k''/k} = f_{k''/k'} \cdot f_{k'/k}. \tag{3.52}$$

Lemma 3.3.1. *Let (k', v') be a complete extension of a complete field (k, v). If $f_{k'/k}$ is finite, then k'/k is a finite extension and the following holds:*

$$[k' : k] = e_{k'/k} \cdot f_{k'/k}. \tag{3.53}$$

We can calculate the value of $v'(x')$ via the following fundamental result:

Theorem 3.3.2. *Let (k, v) be a complete field and k' a finite extension of k. Then there exists a unique normalized valuation v' on k' such that $v'|_k \sim v$, (k', v') is a complete extension* *of* (k, v),

$$[k' : k] = e_{k'/k} \cdot f_{k'/k}, \tag{3.54}$$

and

$$v'(x') = \frac{1}{f_{k'/k}} \cdot v(N_{k'/k}(x')),\ \forall x' \in k'. \tag{3.55}$$

3.4. LOCAL FIELDS

In this section we will discuss local fields and their properties. Local fields are one of the fundamental objects in this thesis.

Definition 3.4.1. If a complete field (k, v) has a finite residue field, it is called a **local field**.

Example 11. The p-adic number field $\mathbb{Q}_p$ is a local field since

$$\kappa_{\mathbb{Q}_p} = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p. \tag{3.56}$$

Example 12. Let $\mathbb{F}_q$ be a finite field where $q = p^n$. Let $F((X))$ be the field of formal Laurent series in X with coefficients in $\mathbb{F}_q$, and v be the valuation given in Example 9. Then $F((X))$ is a local field since $\kappa_{F((X))} = \mathbb{F}_q[[X]]/X\mathbb{F}_q[[X]] \cong \mathbb{F}_q$.

Definition 3.4.2. If the residue field κ_k of a local field k is a field of characteristic p, then the local field k is called a **p-field**.

The following therom completely characterizes the topology of local fields.

Theorem 3.4.1. *Let (k, v) be a local field. Then k is a non-discrete, totally disconnected, locally compact field in its v-topology. The valuation ring $\mathcal{O}_k$ and ideals $\mathfrak{p}_k^n$ of $\mathcal{O}_k$, $n \geq 1$, are open, compact subgroups of the additive group of field k and they form a neighborhood base of 0 in k. Furthermore $\mathcal{O}_k$ is the (unique) maximal compact subring in k.*

Take a prime element π_k of a local field (k, v). We know that $\mathfrak{p}_k^n = \pi_k^n \mathcal{O}_k$, $n \geq 0$. So the map

$$x \mapsto \pi_k^n x,\ \ x \in \mathcal{O}_k \tag{3.57}$$

induces an $\mathcal{O}_k$-module isomorphism $\mathcal{O}_k/\mathfrak{p}_k \cong \mathfrak{p}_k^n/\mathfrak{p}_k^{n+1}$ for $n \geq 0$. The index $[\mathcal{O}_k : \mathfrak{p}_k^n] = q^n$,

$n \geq 0$, because $\kappa_k = \mathbb{F}_q$ and $[\mathcal{O}_k : \mathfrak{p}_k] = q$. According to Theorem 3.4.1, $\mathcal{O}_k$ is compact and the intersection of all $\mathfrak{p}_k^n$ for $n \geq 0$ is 0; so we see that by Definition 2.2.4 and Theorem 2.2.3,

$$\mathcal{O}_k \cong \varprojlim \mathcal{O}_k/\mathfrak{p}_k^n. \tag{3.58}$$

That is, the additive group of $\mathcal{O}_k$ constitutes a profinite group (actually a pro-p-group). Here, the transition maps which are used in the inverse limit are $\mathcal{O}_k/\mathfrak{p}_k^m \to \mathcal{O}_k/\mathfrak{p}_k^n$ for all $m \geq n \geq 0$.

Local fields can be classified by the following the theorem:

Theorem 3.4.2. *(Classification theorem) Let k be a local field.*
(i) Case 1 - k has char 0: Then $k \cong L$, where L is a finite extension of $\mathbb{Q}_p$.
(ii) Case 2 - k has char p: Then k is isomorphic to $K((X))$, the field of Laurent series (over a finite field K of characteristic p).

Lemma 3.4.3. *Let k be a local field, $f(X) \in \mathcal{O}_k[X]$ and $\alpha \in \mathcal{O}_k$ satisfying $|f(\alpha)| < |f'(\alpha)|^2$. Then there exists $\beta \in \mathcal{O}_k$ such that $f(\beta) = 0$ and*

$$|\beta - \alpha| \leq \left|\frac{f(\alpha)}{f'(\alpha)}\right|. \tag{3.59}$$

The lemma above is called Hensel's Lemma. There exists a proof, that is based on this lemma, for the existence of **Teichmüller representatives**, i.e. the elements of the set A_k in the theorem below.

Let (k, v) be a local field, $V_k = \{x \in k \mid x^{q-1} = 1\}$ and $A_k = V \cup \{0\} = \{x \in k \mid x^q = x\}$.

Theorem 3.4.4. *A_k is complete set of representatives of κ_k in $\mathcal{O}_k$ and contains 0. V_k is the set of all $(q-1)$th roots of unity in k, and the canonical ring homomorphism $\mathcal{O}_k \to \kappa_k$ induces the isomorphism of multiplicative groups $V_k \cong \kappa_k^\times$. So V_k is a cyclic group and it is of order* $q - 1$.

Teichmüller representatives can be used to show the existence of the following isomorphism:

Theorem 3.4.5. *Let k be a local field. Then $\mathcal{O}_k^\times \cong \kappa_k^\times \times (1 + \mathfrak{p}_k) = \kappa_k^\times \times \mathcal{U}_1$.*

The multiplicative structure of $k^\times$ can be described as below:

Theorem 3.4.6. *Let (k, v) be a local field. The group $k^\times$ is a totally disconnected and locally compact Abelian group, which is also non-discrete, in the v-topology of k. The unit group $\mathcal{U}_k$ $(= \mathcal{U}_0)$ and its subgroups $\mathcal{U}_n = 1 + \mathfrak{p}_k^n, n \geq 1$ are compact, open subgroups of $k^\times$, they form a neighborhood base of 1 in $k^\times$. Furthermore, $\mathcal{U}_k$ is the (unique) maximal compact subgroup of $k^\times$.*

It can be shown that the compact group $\mathcal{U}_1$ is the inverse limit of $\mathcal{U}_1/\mathcal{U}_n$'s (finite Abelian groups) with respect to the transition maps $\mathcal{U}_1/\mathcal{U}_m \to \mathcal{U}_1/\mathcal{U}_n$ for $m \geq n \geq 0$:

$$\mathcal{U}_1 \cong \varprojlim \mathcal{U}_1/\mathcal{U}_n. \tag{3.60}$$

3.5. FINITE EXTENSIONS OF LOCAL FIELDS

Let (k, v) be a local field and $\kappa_k = \mathcal{O}_k/\mathfrak{p}_k = \mathbb{F}_q$ its residue field. Let k' be any finite extension over k. By Theorem 3.1.2, we can extend v to a unique normalized valuation v' on k' s.t. $v'|_k \sim v$. Then (k', v') is a complete extension of (k, v). So, if k'/k a finite extension, we always get a local field (k', v').

Definition 3.5.1. Let k'/k be a finite extnsion of local fields and put $n = [k' : k] = e_{k'/k} \cdot f_{k'/k}$. Then, k'/k is called an **unramified extension** if $e_{k'/k} = 1$ and $f_{k'/k} = n$ and it is called a **totally ramified extension** if $e_{k'/k} = n$ and $f_{k'/k} = 1$.

Take prime elements π_k and $\pi_{k'}$ of k and k', respectively. So $v(\pi_k) = v'(\pi_{k'}) = 1$. We know that,

$$e_{k'/k} = v'(\pi_k), \;\; f_{k'/k} = v(N_{k'/k}(\pi_{k'})). \tag{3.61}$$

Then we see that

- The extension k'/k is unramified iff a prime π_k also becomes a prime in k',
- The extension k'/k is totally ramified iff $N_{k'/k}(\pi_{k'})$ is a prime element of k when $\pi_{k'}$ is a prime element of k'.

Let k'/k be any finite extension of local fields, $n = [k' : k] = e_{k'/k} \cdot f_{k'/k}$ and $\kappa_k = \mathbb{F}_q$,

$\kappa_{k'} = \mathbb{F}_{q'}$ for the residue fields with $q' = q^{f_{k'/k}}$. Let

$$A'_k = \{y \in k' \mid y^{q'} = y\}, \;\; k_0 = k(A'_k), \;\; k \subseteq k_0 \subseteq k'. \tag{3.62}$$

For k_0, we have the following:

Lemma 3.5.1. *The field k_0 is a splitting field of $x^{q'} - x$ over k and k_0/k is an unramified cyclic extension with degree $[k_0 : k] = f_{k'/k}$.*

Using the Lemma 3.5.1 we can show the following isomorphism:

$$\mathrm{Gal}(k_0/k) \cong \mathrm{Gal}(\kappa_{k_0}/\kappa_k). \tag{3.63}$$

We also have the following important result about the unramified extensions of local fields:

Theorem 3.5.2. *Let (k, v) be a local field and $\kappa_k = \mathcal{O}_k/\mathfrak{p}_k = \mathbb{F}_q$ its residue field. For each integer $n \geq 1$, there exits an unramified extension k'/k with degree $[k' : k] = n$. Here k' is unique over k (up to an isomorphism). The extension field k' is a splitting field of $X^{q^n} - X$ over k, and it is also a cyclic extension and of degree n over k. Let $\kappa_{k'}$ be the residue field of the local field (k', v'). Then each element of σ of $\mathrm{Gal}(k'/k)$ induces an automorphism σ' of $\kappa_{k'}/\kappa_k$, and the map $\sigma \mapsto \sigma'$ defines an isomorphism*

$$\mathrm{Gal}(k'/k) \cong \mathrm{Gal}(\kappa_{k'}/\kappa_k). \tag{3.64}$$

The generator φ of the cyclic group $\mathrm{Gal}(k'/k)$ in Theorem 3.5.2, which corresponds to the automorphism $\omega \mapsto \omega^q, \forall \omega \in \kappa_{k'}$, is called the **Frobenius automorphism** of the unramified extension of k'/k and it is uniquely characterized by the following property:

$$\varphi(y) \equiv y^q \bmod \mathfrak{p}_{k'}, \tag{3.65}$$

for all $y \in \mathcal{O}_{k'}$.

Theorem 3.5.3. *The splitting field k_0 of $x^{q'} - x$ over k in Lemma 3.5.1 is the unique maximal unramified extension over k in k'. The extension k'/k_0 is a totally ramified extension and*

$$[k' : k_0] = e_{k'/k}, \;\; [k_0 : k] = f_{k'/k}. \tag{3.66}$$

The field k_0 is called **the inertia field** of k'/k.

3.6. INFINITE EXTENSIONS OF LOCAL FIELDS

In this section the infinite extensions of local fields will be discussed. Let (k, v) be a local field and $\kappa_k = \mathcal{O}_k/\mathfrak{p}_k = \mathbb{F}_q$ its residue field. Denote a fixed algebraic closure of k by k^{alg} and let μ be the unique extension of v to k^{alg}. Denote the completion of (k^{alg}, μ) by $(\widehat{k^{alg}}, \hat{\mu})$. If F is any intermediate field of k and k^{alg}, then we have:

$$k \subseteq F \subseteq k^{alg} \subseteq \widehat{k^{alg}}. \tag{3.67}$$

We have discussed that the closure $\overline{F}$ of F in $\widehat{k^{alg}}$ is a subfield of $\widehat{k^{alg}}$. Let

$$\mu_F = \mu|_F, \ \ \mu_{\overline{F}} = \hat{\mu}|_{\overline{F}}. \tag{3.68}$$

Then μ_F is the uniquely determined extension of v to the algebraic extension F over k. Also $(\overline{F}, \mu_{\overline{F}})$ is the completion of (F, μ_F) as described in Example 7. In case of infinite extensions, similar to finite extensions, we have the following definitions:

$$\mathcal{O}_F \text{ : the valuation ring of } \mu_F, \tag{3.69}$$

$$\mathfrak{p}_F \text{ : the maximal ideal of } \mu_F, \tag{3.70}$$

$$\kappa_F = \mathcal{O}_F/\mathfrak{p}_F \text{ : the residue field of } \mu_F. \tag{3.71}$$

Also let $\mathcal{O}_{\overline{F}}$, $\mathfrak{p}_{\overline{F}}$, and $\kappa_{\overline{F}}$ be defined similarly for $\mu_{\overline{F}}$. Since $f_{\overline{F}/F} = 1$, the injection $\mathcal{O}_F \hookrightarrow \mathcal{O}_{\overline{F}}$ induces:

$$\kappa_F \cong \kappa_{\overline{F}}. \tag{3.72}$$

Lemma 3.6.1. *Let L be an extension of F in k^{alg} (assume the extension is finite) and denote the closure of L in $\widehat{k^{alg}}$ by $\bar{L}$. Then*

$$L\bar{F} = \bar{L}. \tag{3.73}$$

If L/F is seperable, then we have that $L \cap \bar{F} = F$.

3.7. UNRAMIFIED AND TOTALLY RAMIFIED EXTENSIONS

Let $k \subseteq F \subseteq k^{alg}$ be as in Section 3.6

Definition 3.7.1. Then the extension F/k is called an **unramified extension** if every finite extension k' over k in F, $k \subseteq k' \subseteq F$ is unramified; that is $e_{k'/k} = 1$. It is evident that, if F/k is unramified and also we have $k \subseteq F' \subseteq F$, then F'/k is also unramified.

We have the following lemma to characterize the unramified extensions:

Lemma 3.7.1. *Let $k \subseteq F \subseteq k^{alg}$. Then F/k is unramified if and only if $\mu_F(= \mu|_F)$ is a normalized valuation on F; i.e. $\mu(F^{\times}) = \mathbb{Z}$.*

There exists a unique unramified extension k_{ur}^n over k in k^{alg} with degree n for $n \geq 1$. This field is the splitting field of $X^{q^n} - X$ over k in k^{alg}. If we take the union k_{ur} of all k_{ur}^n, $n \geq 1$, then we get a subfield of k^{alg}:

$$k_{ur} = \bigcup_{n\geq 1} k_{ur}^n. \tag{3.74}$$

Let $K = k_{ur}$. It can be shown that K is the **unique maximal unramified extension** over k in k^{alg}. Similar to finite case, the following theorem can be given for the Galois group of the maximal unramified extension.

Theorem 3.7.2. *The field κ_K is an algebraic closure of κ_k of k. Each $\sigma \in \mathrm{Gal}(K/k)$ induces an automorphism σ' of κ_K/κ_k, and the map $\sigma \mapsto \sigma'$ defines a natural isomorphism*

$$\mathrm{Gal}(K/k) \cong \mathrm{Gal}(\kappa_K/\kappa_k). \tag{3.75}$$

Since $\kappa_k = \mathbb{F}_q$, the map $\omega \mapsto \omega^q$, $\omega \in \kappa_K$ defines an automorphism of κ_K over κ_k. Let φ denote the corresponding element in $\mathrm{Gal}(K/k)$ under $\mathrm{Gal}(K/k) \cong \mathrm{Gal}(\kappa_K/\kappa_k)$. This is the unique element in $\mathrm{Gal}(K/k)$ satisfying

$$\varphi(\alpha) \equiv \alpha^q \bmod \mathfrak{p}_K, \text{ for all } \alpha \in \mathcal{O}_K. \tag{3.76}$$

This automorphism is called the **Frobenius automorphism** of K/k. It is usually denoted by φ_k. We see that φ_k induces on each k_{ur}^n, $n \geq 1$, the Frobenius automorphism φ_n of k_{ur}^n/k

(Theorem 3.5.2). We know that $\mathrm{Gal}(k_{ur}^{n}/k)$ is the cyclic group of order n and it is generated by φ_n, so the map a mod $n \mapsto \varphi_n^a, a \in \mathbb{Z}$ defines an isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \mathrm{Gal}(k_{ur}^{n}/k)$.

We know that $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$. It can be shown that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{Z}/m\mathbb{Z} \arrow[r, "\sim"] \arrow[d] & \mathrm{Gal}(k_{ur}^{m}/k) \arrow[d] \\
\mathbb{Z}/n\mathbb{Z} \arrow[r, "\sim"] & \mathrm{Gal}(k_{ur}^{n}/k)
\end{tikzcd} \tag{3.77}$$

Taken together, $\widehat{\mathbb{Z}} \cong \mathrm{Gal}(K/k) \cong \varprojlim \mathrm{Gal}(k_{ur}^{n}/k)$.

Definition 3.7.2. Let F be an algebraic extension of k in k^{alg}: $k \subseteq F \subseteq k^{alg}$. The extension F/k is called a **totally ramified extension** if every k' such that $k \subseteq k' \subseteq F$, $[k' : k] < \infty$, is a totally ramified extension; that is, $f_{k'/k} = 1$. In general F/k is totally ramified if and only if $F \cap k_{ur} = k$.

Let k be a local field. Assume that the cardinality of its residue field is q which is a power of a prime p. Let V_∞ be multipl. group of all roots of unity in k^{alg} with order prime to p. For $n \geq 1$, let V_n denote the subgroup of all $(q^n - 1)$th roots of unity in k^{alg}. Then,

$$V_\infty = \bigcup_{n \geq 1} V_n, \quad k_{ur}^{n} = k(V_n), \quad k_{ur} = k(V_\infty). \tag{3.78}$$

By Theorem 3.4.4, the ring homomorphism $\mathcal{O}_K \to \kappa_K$ induces $V_\infty \cong \kappa_K^{\times}$. So if $\varphi_k(\eta) \equiv \eta^q \mod \mathfrak{p}_K$ then $\varphi_k(\eta) = \eta^q \mod \mathfrak{p}_K$ for $\eta \in V_\infty$.

We conclude this section with the following important lemma about totally ramified extensions:

Lemma 3.7.3. *Let T be Galois over k, containing k_{ur}, ψ an element of* $\mathrm{Gal}(T/k)$ *satisfying $\psi|_{k_{ur}} = \varphi_k$. Denote the fixed field of ψ in T by F. Then*

$$Fk_{ur} = T, \;\; F \cap k_{ur} = k, \;\; \mathrm{Gal}(T/F) \cong \mathrm{Gal}(k_{ur}/k). \tag{3.79}$$

$$\begin{tikzcd}[column sep=small]
 & Fk_{ur} = T \arrow[dl, dash] \arrow[dr, dash] & \\
F \arrow[dr, dash] & & k_{ur} \arrow[dl, dash] \\
 & F \cap k_{ur} = k &
\end{tikzcd} \tag{3.80}$$

Particularly, F is a maximal totally ramified extension over k in T.

3.8. THE NORM GROUPS

Here we will present the norm groups of algebraic extensions. They will be used later on in the text.

Let k be a local field. Consider any algebraic extension F/k ($k \subseteq F \subseteq k^{alg}$). Let $\mathcal{U}_F$ denote the unit group of F:

$$\mathcal{U}_F = \mathrm{Ker}(\mu_F : F^{\times} \mapsto \mathbb{R}^{+}). \tag{3.81}$$

Define

$$N(F/k) = \bigcap_{k'} N_{k'/k}(k'^{\times}), \quad NU(F/k) = \bigcap_{k'} N_{k'/k}(\mathcal{U}_{k'}), \tag{3.82}$$

where $k \subseteq k' \subseteq F$, $[k' : k] < +\infty$. The groups $N(F/k)$ and $NU(F/k)$ are called the **norm group** and the **unit norm group** of F/k, respectively. If F/k is finite, we have

$$N(F/k) = N_{F/k}(F^{\times}), \; NU(F/k) = N_{F/k}(\mathcal{U}_F). \tag{3.83}$$

The group $N(F/k)$ is a closed subgroup in $k^{\times}$, $NU(F/k)$ is a compact subgroup of $\mathcal{U}_k$, and

$$NU(F/k) = N(F/k) \cap \mathcal{U}_k. \tag{3.84}$$

Note that, if $k \subseteq F \subseteq F' \subseteq k^{alg}$, then

$$N(F'/k) \subseteq N(F/k), \; NU(F'/k) \subseteq NU(F/k). \tag{3.85}$$

Theorem 3.8.1. *Let F/k be an algebraic extension. Assume also it is unramified. Then we* *have*

$$NU(F/k) = \mathcal{U}_k. \tag{3.86}$$

Also, if the extension F/k is infinite,

$$N(F/k) = \mathcal{U}_k. \tag{3.87}$$

Particularly, if F is k_{ur}, in this case we have the following:

$$N(k_{ur}/k) = NU(k_{ur}/k) = \mathcal{U}_k. \tag{3.88}$$

Theorem 3.8.2. *Let k be a local field and T/k an algebraic extension, where $k \subseteq T \subseteq k^{alg}$. Then T/k is totally ramified iff N(T/k) contains a prime in k.*

3.9. THE DIFFERENT

Consider the finite extension of local fields k'/k and assume also this extension is separable. It is known that the trace map $T_{k'/k} : k' \to k$ is continuous [15] and $T_{k'/k}(\mathcal{O}_{k'}) \subseteq \mathcal{O}_k$. Define:

$$A = \{x' \in k' \mid T_{k'/k}(x'\mathcal{O}_{k'}) \subseteq \mathcal{O}_k\}. \tag{3.89}$$

Since we assumed k'/k is separable so there is an $y \in k'$ such that $T_{k'/k}(y) \neq 0$. This implies $T_{k'/k}(k') = k$, also A is an $\mathcal{O}_{k'}$-submodule of k' which is not equal to k'. The inclucion $T_{k'/k}(\mathcal{O}_{k'}) \subseteq \mathcal{O}_k$ implies that $\mathcal{O}_{k'} \subseteq A$ and $A \neq 0$. So m is an ideal of k' and $\mathcal{D}_{k'/k} = m^{-1}$ is a non-zero ideal of $\mathcal{O}_{k'}$ (recall the definition of an ideal). We call $\mathcal{D}_{k'/k}$ the **different** of the extension k'/k.

Lemma 3.9.1. *There is an element $\xi \in \mathcal{O}_{k'}$ such that $1, \xi, \dots, \xi^{n-1}$ form a free basis of the $\mathcal{O}_k$-module $\mathcal{O}_{k'}$; that is,*

$$\mathcal{O}_{k'} = \mathcal{O}_k \oplus \mathcal{O}_k\xi \oplus \cdots \oplus \mathcal{O}_k\xi^{n-1}. \tag{3.90}$$

Particularly, $\mathcal{O}_{k'} = \mathcal{O}_k[\xi]$.

Theorem 3.9.2. *Let k'/k be a totally ramified finite extension and π' a prime in k'. Then*

$$\mathcal{O}_{k'} = \mathcal{O}_k[\pi']. \tag{3.91}$$

Theorem 3.9.3. *Let $\alpha \in \mathcal{O}_{k'}$ be as in Lemma 3.9.1 and $f(X)$ the minimal polynomial of $\alpha \in k$. Then*

$$\mathcal{D}_{k'/k} = f'(\alpha)\mathcal{O}_{k'}. \tag{3.92}$$

Here $f'(X)$ denotes the formal derivative of $f(X)$.

3.10. THE RAMIFICATION THEORY OF LOCAL FIELDS

Let k'/k be a finite Galois extension of local fields and put $G = \text{Gal}(k'/k)$. Take an element $\xi \in G$. Then by 3.32,

$$\xi(\mathcal{O}_{k'}) = \mathcal{O}_{k'},\ \ \xi(\mathfrak{p}_{k'}) = \mathfrak{p}_{k'},\ n \geq 1. \tag{3.93}$$

This implies ξ induces the following automorphisms:

$$\xi_n : \mathcal{O}_{k'}/\mathfrak{p}_{k'}^{n+1} \cong \mathcal{O}_{k'}/\mathfrak{p}_{k'}^{n+1}. \tag{3.94}$$

The map $\psi : \xi \mapsto \xi_n$ is a homomorphism of G into Aut$(\mathcal{O}_{k'}/\mathfrak{p}_{k'}^{n+1})$, the group of automorphisms of $\mathcal{O}_{k'}/\mathfrak{p}_{k'}^{n+1}$. Denote Ker ψ as G_n; i.e.,

$$G_n = \{\xi \in G \mid \xi(x') \equiv x' \text{ mod } \mathfrak{p}_{k'}^{n+1} \text{ for all } x' \in \mathcal{O}_{k'}\}. \tag{3.95}$$

The subgroup G_n is a normal in G and $G_{n+1} \subseteq G_n$ where $n \geq 0$. If $\xi \neq 1$, then there exists an $x' \in \mathcal{O}_{k'}$ such that $\xi(x') \neq x'$, so $\xi(x') - x' \notin \mathfrak{p}_{k'}^{n+1}$ for sufficiently large n. This means that $G_m = 1$ for $m \geq n$ and we have the following sequence of normal subgroups of G:

$$1 = \ldots = G_m \subseteq \ldots \subseteq G_1 \subseteq G_0 = G. \tag{3.96}$$

These groups are usually called (in lower numbering) **the ramification groups** of the extension k'/k. We will need two theorems about the ramifications groups.

Theorem 3.10.1. *Let k_0 be the inertia field of k'/k. Then the following hold:*

$$G_0 = \mathrm{Gal}(k'/k_0),\ \ G/G_0 = \mathrm{Gal}(k_0/k) \cong \mathrm{Gal}(\kappa_{k'}/\kappa_k). \tag{3.97}$$

By this theorem, G/G_0 is a cyclic, $|G_0| = e_{k'/k}$. Also $[G : G_0] = f_{k'/k}$.

Theorem 3.10.2. *There exists an injective homomorphism*

$$\omega : G_n/G_{n+1} \to \mathcal{U}_n/\mathcal{U}_{n+1}, \tag{3.98}$$

where $n \geq 0$ and $\mathcal{U}_n$ is the subgroups of the unit group of k' as described in 3.45.

Now let k be a p-field. Then by the equations in 3.46,

$$\mathcal{U}_0/\mathcal{U}_1 \cong \kappa_{k'}^{\times}, \tag{3.99}$$

and

$$\mathcal{U}_n/\mathcal{U}_{n+1} \cong \kappa_{k'}^{+},\ \ n \geq 1. \tag{3.100}$$

So, if we consider the theorem above, the following easily follow:

(i) G_0/G_1 is cyclic and $[G_0 : G_1] \mid (q' - 1)$,

(ii) G_n/G_{n+1} is Abelian of type $(p, \dots, p)$, $[G_n : G_{n+1}] \mid q'$,

(iii) $[G_0 : G_1]$ is prime to p and $\mid G_1 \mid$ is a power of p.

4. FORMAL POWER SERIES

In this chapter, we will discuss formal power series and then we will introduce power series over $\mathcal{O}_{\hat{R}}$. The main references for this chapter are [8], [15], [16] and [17].

4.1. BASIC DEFINITIONS

Let R be a commutative ring with identity $1 \neq 0$. In this chapter,

$$S = R[[X_1, \dots, X_n]] \tag{4.1}$$

denotes the commutative ring of all power series

$$f = f(X_1, X_2, \dots, X_{n-1}, X_n) = \sum_i a_{i_1,\, i_2,\, \dots\, ,i_{n-1}, i_n} X_1^{i_1} X_2^{i_2}\, \cdots\, X_{n-1}^{i_{n-1}} X_n^{i_n},\ \ a_{i_1,\, i_2,\, \dots\, ,i_{n-1}, i_n} \in R, \tag{4.2}$$

where $X_1, X_2, \dots, X_{n-1}, X_n$ are indeterminates and $i = (i_1, i_2, \dots, i_{n-1}, i_n)$ ranges over all n-tuples of non-negative integers.

Let $f,\ g \in S$ and $d \geq 0$ an integer. Then, if the power series $f - g$ does not have any terms of total degree $\leq d$, we write

$$f \equiv g \bmod \deg d. \tag{4.3}$$

Let $g_1, \dots, g_n$ be power series in $R[[Y_1, \dots, Y_m]]$ such that $g_i \equiv 0 \bmod \deg 1$ for $1 \leq i \leq n$. For any $f(X_1, \dots, X_n)$ in S, we can substitute g_i for X_i, $1 \leq i \leq n$ and we get a well-defined power series

$$f(g_1(Y_1, \dots, Y_m), \dots, g_n(Y_1, \dots, Y_m)), \tag{4.4}$$

in $T = R[[Y_1, \dots, Y_m]]$. This is because we take '0 mod deg 1' power series, so we do not encounter such power series that contain constant terms and the problem of convergence does not come up. We denote such a power series by $f \circ (g_1, \dots, g_n)$.

We can get interesting algebraic structures by using formal power series. As an example, let X be an indeterminate. Consider the ideal M of $R[[X]]$, generated by X; i.e., $M = (X) = X \cdot R[[X]]$. The set M consists of all $f \equiv 0 \bmod \deg 1$. Consider the preceeding discussion and take $n = m = 1$; then the power series $f \circ g$ is well-defined and it belongs to M. In particular we get a monoid with the multiplication defined by $f \circ g$. The power series $e(X) = X$ is the identity element of this monoid: $X \circ f = f \circ X = f$.

If there exist $f,\ g \in M$ such that $f \circ g = g \circ f = X$, then we can define the inverses and write

$$f = g^{-1},\ g = f^{-1}. \tag{4.5}$$

The following lemma is a well-known fact about formal power series:

Lemma 4.1.1. *Let* $f(X) = \sum_{n=1}^{\infty} a_n X^n,\ \ a_n \in R$. *Then* f *is invertible in M iff* a_1 *is invertible in R.*

Let k be a local field, k^{alg} a fixed algebraic closure of k, $\widehat{k^{alg}}$ the completion of k^{alg} and $\kappa_{\widehat{k^{alg}}}$ the residue field of $\widehat{k^{alg}}$. Take

$$f = \sum_{i} a_{i_1,\,\dots\,,i_n} X_1^{i_1} \cdots X_n^{i_n},\ \ a_{i_1,\,\dots\,,i_n} \in \mathcal{O}_{\widehat{k^{alg}}}, \tag{4.6}$$

and let $g_1, \dots, g_n$ be power series in $\mathcal{O}_{\widehat{k^{alg}}}[[Y_1, \dots, Y_m]]$ satisfying that the constant terms of $g_1, \dots, g_n$ are contained in $\mathfrak{p}_{\widehat{k^{alg}}}$. Consider

$$f \circ (g_1, \dots, g_n) = \sum_{i} a_{i_1,\dots,i_n} g_i(Y_1, \dots, Y_m)^{i_1} \cdots g_n(Y_1, \dots, Y_m)^{i_n}. \tag{4.7}$$

We see that the formal power series converges in $\mathcal{O}_{\widehat{k^{alg}}}[[Y_1, \dots, Y_m]]$ since the constant term in it constitute a convergent series (because its terms belong to $\mathfrak{p}_{\widehat{k^{alg}}}$, the powers of the terms increase as n goes to infinity, so the valuation of the difference between the consecutive partial sums increases indefinitely, which proves that it is a Cauchy sequence). Particularly if we took any $\alpha_1, \dots, \alpha_n \in \mathfrak{p}_{\widehat{k^{alg}}}$, then $f(\alpha_1, \dots, \alpha_n)$ would be well-defined.

4.2. POWER SERIES OVER $\mathcal{O}_{\hat{K}}$

Let k be a local field and K denote k_{ur}, i.e. the maximal unramified extension of the local field k in k^{alg}. Also denote the Frobenius automorphism of k by φ_k: $\varphi_k \in \mathrm{Gal}(K/k)$ and let

$\widehat{\varphi}_k$ be the natural extension of φ_k to $\widehat{K}$. In this section we will call both of them φ if there is no risk of confusion. Recall that φ induces the automorphism $\omega \mapsto \omega^q$ on the residue field $\kappa_K \cong \kappa_{\widehat{K}} = \mathcal{O}_{\widehat{K}}/\mathfrak{p}_{\widehat{K}}$,

$$\alpha^{\varphi} := \varphi(\alpha) \equiv \alpha^q \bmod \mathfrak{p}_{\widehat{K}} \text{ for all } \alpha \in \mathcal{O}_{\widehat{K}}. \tag{4.8}$$

We will prove a lemma for the endomorphisms below:

$$\varphi - 1 : \mathcal{O}_{\widehat{K}} \to \mathcal{O}_{\widehat{K}}, \tag{4.9}$$

$$\alpha \mapsto (\varphi - 1)(\alpha) = \varphi(\alpha) - \alpha, \tag{4.10}$$

$$\varphi - 1 : U_{\widehat{K}} \to U_{\widehat{K}}, \tag{4.11}$$

$$\xi \mapsto \xi^{\varphi-1} = \varphi(\xi)/\xi. \tag{4.12}$$

Lemma 4.2.1. *Let $O_{\widehat{K}}$ be the additive group of $\mathcal{O}_{\widehat{K}}$, $U_{\widehat{K}}$ the group of units in $\widehat{K}$. The sequences below are exact:*

$$1 \to U_k \to U_{\widehat{K}} \xrightarrow{\varphi-1} U_{\widehat{K}} \to 1 \tag{4.13}$$

$$0 \to \mathcal{O}_k \to \mathcal{O}_{\widehat{K}} \xrightarrow{\varphi-1} \mathcal{O}_{\widehat{K}} \to 0 \tag{4.14}$$

Proof. The exactness of the first sequence will be proved. The proof of the other case is similar. Recall that $\kappa_K \cong \kappa_{\widehat{K}}$ is algebraically closed. So the maps $\kappa_{\widehat{K}} \to \kappa_{\widehat{K}}$ defined by $\omega \mapsto \omega^q - \omega$ and $\omega \mapsto \omega^{q-1}$ are both surjective. So

$$(\varphi - 1)\mathcal{O}_{\widehat{K}} + \mathfrak{p}_{\widehat{K}} = \mathcal{O}_{\widehat{K}}, \quad U_{\widehat{K}}^{\varphi-1}(1 + \mathfrak{p}_{\widehat{K}}) = U_{\widehat{K}}. \tag{4.15}$$

Let $\xi \in U_{\widehat{K}}$. We will use the induction to define a sequence of elements $\{\eta_n\}_{n\geq 0} \in U_{\widehat{K}}$ satisfying

$$\xi \equiv \eta_n^{\varphi-1} \bmod \mathfrak{p}_{\widehat{K}}^{n+1}, \quad \eta_n \equiv \eta_{n+1} \bmod \mathfrak{p}_{\widehat{K}}^{n+1}, \quad \text{for all } n \geq 0. \tag{4.16}$$

There exists $\eta_0 \in U_{\widehat{K}}$ such that $\xi \equiv \eta_0^{\varphi-1} \bmod \mathfrak{p}_{\widehat{K}}$ by the equation 4.15. Now we suppose that we found a sequence of elements, $\eta_0, \eta_1, \dots, \eta_n$, $n \geq 0$ satisfying the congruences in 4.16. Take a prime π_k in k. As K/k is unramified, π_k is also a prime in K and $\widehat{K}$. So, we can write $\mathfrak{p}_{\widehat{K}} = \pi_k \mathcal{O}_{\widehat{K}}$. By the congruence in 4.16,

$$\xi \eta_n^{1-\varphi} = 1 + \alpha \pi_k^{n+1}, \quad \alpha \in \mathcal{O}_{\widehat{K}}. \tag{4.17}$$

We know by 4.16, there exists an element $\beta \in \mathcal{O}_{\widehat{K}}$ such that $\alpha \equiv (\varphi - 1)(\beta) \bmod \mathfrak{p}_{\widehat{K}}$.
Let

$$\eta_{n+1} = \eta_n(1 + \beta\pi^{n+1}). \tag{4.18}$$

We see that $\eta_{n+1} \in U_{\widehat{K}}$ and $\eta_n \equiv \eta_{n+1} \bmod \mathfrak{p}_{\widehat{K}}^{n+1}$. We also know that $\varphi(\pi_k) = \pi_k$, then the following holds:

$$\eta_{n+1}^{\varphi-1} = \eta_n^{\varphi-1}(1 + \varphi(\beta)\pi_k^{n+1})\left(1 + \frac{-\beta\pi_k^{n+1}}{1 + \beta\pi_k^{n+1}}\right) \tag{4.19}$$

$$= \eta_n^{\varphi-1}(1 + \varphi(\beta)\pi_k^{n+1})\{1 + [(-\beta\pi_k^{n+1})(1 + \gamma\pi_k^{n+1})]\} \tag{4.20}$$

$$\equiv \eta_n^{\varphi-1}(1 + (\varphi(\beta) - \beta)\pi_k^{n+1}) \bmod \mathfrak{p}_{\widehat{K}}^{n+2} \tag{4.21}$$

$$\equiv \eta_n^{\varphi-1}(1 + \alpha\pi_k^{n+1}) \bmod \mathfrak{p}_{\widehat{K}}^{n+2} \tag{4.22}$$

$$\equiv \xi \bmod \mathfrak{p}_{\widehat{K}}^{n+2}. \tag{4.23}$$

where $\gamma \in \mathcal{O}_{\widehat{K}}$ (we used the fact that $1 + \mathfrak{p}_{\widehat{K}}^{n+1}$ is a multiplicative group). Now we showed the existence of the sequence $\{\eta_n\}_{n\geq 0}$. Since $\widehat{K}$ is complete, then $\eta = \lim_{n\to\infty} \eta_n$ exits in $U_{\widehat{K}}$ and satisfies $\eta^{\varphi-1} = \xi$. Hence we proved that $U_{\widehat{K}} \xrightarrow{\varphi-1} U_{\widehat{K}}$ is surjective.

Consider the kernel of $U_{\widehat{K}} \xrightarrow{\varphi-1} U_{\widehat{K}}$ and observe that U_k is in the kernel. Suppose $\xi \in \ker \varphi - 1,\ \xi^{\varphi-1} = 1$. We know that the set $A_{\widehat{K}} = \{0\} \cup V_\infty$ is a complete set of representatives for $\kappa_{\widehat{K}}$ in $\mathcal{O}_{\widehat{K}}$. Take a prime element π_k as above. Then ξ can be expressed (in a unique way) as follows:

$$\xi = \sum_{n=0}^{\infty} a_n\pi_k^n, \quad a_n \in A = \{0\} \cup V_\infty. \tag{4.24}$$

Now we apply φ to ξ and we get $\xi = \varphi(\xi) = \sum_{n=0}^{\infty} \varphi(a_n)\pi_k^n$. But by the uniqueness of the representation, $a_n = \varphi(a_n) = a_n^q$, for all $n \geq 0$. So $a_n = 0$ or a_n is an element of the cyclic group V_k of order $q - 1$. Now we see that $\xi \in k \cap U_{\widehat{K}} = U_k$ and the exactness is proved. □

From now on, for the power series

$$f(X_1, \ldots, X_n) = \sum_i a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}, \quad a_{i_1,\ldots,i_n} \in \mathcal{O}_{\widehat{K}}, \tag{4.25}$$

f^φ will mean

$$f^\varphi(X_1, \ldots, X_n) = \sum_i \varphi(a_{i_1,\ldots,i_n}) X_1^{i_1} \cdots X_n^{i_n}. \tag{4.26}$$

Now we will prove a fundamental theorem in this section.

Theorem 4.2.2. *Let π_1 and π_2 be primes in $\widehat{K}$, f_1 and f_2 power series in $\mathcal{O}_{\widehat{K}}[[X]]$ satisfying the following conditions:*

$$f_1(X) \equiv \pi_1 X,\ \ f_2(X) \equiv \pi_2 X \ \bmod\ \deg\ 2,\ \ \ f_1(X) \equiv f_2(X) \equiv X^q \ \bmod\ \mathfrak{p}_{\widehat{K}}, \tag{4.27}$$

where q is the order of κ_k. Let

$$L(X_1, \dots, X_m) = \alpha_1 X_1 + \cdots + \alpha_m X_m,\ \ \alpha_i \in \mathcal{O}_{\widehat{K}}, \tag{4.28}$$

be a linear form in $X_1, \dots, X_m$ satisfying

$$\pi_1 L(X_1, X_2, \dots, X_{m-1}, X_m) = \pi_2 L^{\varphi}(X_1, X_2, \dots, X_{m-1}, X_m). \tag{4.29}$$

Then there is a unique $F = F(X_1, \dots, X_m)$ in $\mathcal{O}_{\widehat{K}}[[X_1, \dots, X_m]]$ such that

$$F \equiv L \ \text{mod deg}\ 2,\ \ f_1 \circ F = F^{\varphi} \circ f_2. \tag{4.30}$$

Proof. We proceed by induction on n. We inductively construct a sequence (F_n) satisfying the following conditions:

$$f_1 \circ F_n \equiv F_n^{\varphi} \circ f_2,\ \ F_{n+1} \equiv F_n \ \text{mod deg}\ n+1 \ \ \text{for all}\ n \geq 1. \tag{4.31}$$

Let $F_1 = L$. Because of our assumptions on f_1, f_2 and L,

$$f_1 \circ F_1 \equiv F_1^{\varphi} \circ f_2 \ \text{mod deg}\ \ 2. \tag{4.32}$$

Assume that $n \geq 1$ and we have found a polynomial F_n ot total degree $\leq n$ in $\mathcal{O}_{\widehat{K}}[X_1, \dots, X_m]$ satisfying

$$f_1 \circ F_n \equiv F_n^{\varphi} \circ f_2 \ \text{mod deg}\ \ n+1. \tag{4.33}$$

Let H_{n+1} be a homogeneous polynomial, which is of degree $n+1$ and also a member of $\mathcal{O}_{\widehat{K}}[[X_1, \dots, X_m]]$ and let

$$F_{n+1} = F_n + H_{n+1}. \tag{4.34}$$

So F_{n+1} is a polynomial of total degree $\leq n+1$ in $\mathcal{O}_{\hat{K}}[X_1, \dots, X_m]$ satisfying

$$F_{n+1} \equiv F_n \text{ mod deg } n+1. \tag{4.35}$$

The existence of F depends on the existence a particular unique H_{n+1} such that F_{n+1} above satisfies

$$f_1 \circ F_{n+1} \equiv F_{n+1}^{\varphi} \circ f_2 \text{ mod deg } n+2. \tag{4.36}$$

Let $G_{n+1} = f_1 \circ F_n - F_n^{\varphi} \circ f_2$. By the congruence 4.33, $G_{n+1} \equiv 0$ mod deg $n+1$. Since $f_1 \equiv \pi_1 X$ and also $f_2 \equiv \pi_2 X$ mod deg 2,

$$f_1 \circ F_{n+1} = f_1(F_n + H_{n+1}) \equiv f_1 \circ F_n + \pi_1 H_{n+1} \text{ mod deg } n+2, \tag{4.37}$$

$$F_{n+1}^{\varphi} \circ f_2 = F_n^{\varphi} \circ f_2 + H_{n+1}^{\varphi} \circ f_2 \equiv F_n^{\varphi} \circ f_2 + \pi_2^{n+1} H_{n+1}^{\varphi} \text{ mod deg } n+2. \tag{4.38}$$

So the congruence 4.36 is equivalent to the following congruence:

$$G_{n+1} + \pi_1 H_{n+1} - \pi_2^{n+1} H_{n+1}^{\varphi} \equiv 0 \text{ mod deg } n+2. \tag{4.39}$$

But, since $f_1 \equiv f_2 \equiv X^q$ mod $\mathfrak{p}_{\hat{K}}$ and $\alpha^{\varphi} \equiv \alpha^q$ mod $\mathfrak{p}_{\hat{K}}$ for $\alpha \in \mathcal{O}_{\hat{K}}$, if we consider the definition of G_{n+1}, we will see that

$$G_{n+1} \equiv F_n(X_1, \dots, X_m)^q - F_n^{\varphi}(X_1^q, \dots, X_m^q) \equiv 0 \text{ mod } \mathfrak{p}_{\hat{K}}. \tag{4.40}$$

Now consider a monomial $X^i = X_1^{i_1} \cdots X_m^{i_m}$ of degree $n+1$ in $\mathcal{O}_{\hat{K}}[X_1, \dots, X_m]$. The coefficient of X^i in G_{n+1} should be an element of the form $-\pi_1 \beta$, $\beta \in \mathcal{O}_{\hat{K}}$. Let α be the coefficient of X^i in H_{n+1}. Then the coefficient of the same X^i in $\pi_1 H_{n+1} - \pi_2^{n+1} H_{n+1}^{\varphi}$ is $\pi_1 \alpha - \pi_2^{n+1} \alpha^{\varphi}$. Since $G_{n+1} \equiv 0$ mod deg $n+1$, the congruence 4.39 holds if and only if α satisfy the following:

$$-\pi_1 \beta + \pi_1 \alpha - \pi_2^{n+1} \alpha^{\varphi} = 0, \tag{4.41}$$

for every monomial X^i of degree $n+1$. Let $\gamma = \pi_1^{-1} \pi_2^{n+1}$. We see that $\mu_{\hat{K}}(\gamma) = n \geq 1$. Then the equation above for α can be written as

$$\alpha - \gamma \alpha^{\varphi} = \beta, \tag{4.42}$$

where β and γ are known quantities. Since $\mu_{\hat{K}}(\gamma) \geq 1$, this implies that the following series is convergent in $\mathcal{O}_{\hat{K}}$ and satisfies the equality 4.42:

$$\alpha = \beta + \gamma\beta^{\varphi} + \gamma^{1+\varphi}\beta^{\varphi^2} + \dots \tag{4.43}$$

To prove the uniqueness of the solution, assume that α_1 and α_2 are two solutions, then

$$\alpha_1 - \alpha_2 = \gamma(\alpha_1^{\varphi} - \alpha_2^{\varphi}). \tag{4.44}$$

On the other hand,

$$\mu_{\hat{K}}(\alpha_1 - \alpha_2) = \mu_{\hat{K}}(\varphi(\alpha_1 - \alpha_2)) = \mu_{\hat{K}}(\alpha_1^{\varphi} - \alpha_2^{\varphi}), \tag{4.45}$$

so that $\mu_{\hat{K}}(\alpha_1 - \alpha_2) = +\infty$. That means $\alpha_1 = \alpha_2$. So we proved there exists a unique H_{n+1} satisfying the congruence 4.39 and F_{n+1} satisfying the congruence 4.36. Starting from $F_1 = L$, we can construct a sequence of polynomials F_n in $\mathcal{O}_{\hat{K}}[[X_1, \dots, X_m]]$ such that deg $F_n \leq n$ and

$$f_1 \circ F_n \equiv F_n^{\varphi} \circ f_2,\ \ F_{n+1} \equiv F_n \text{ mod deg } n+1 \text{ for all } n \geq 1. \tag{4.46}$$

The second congruence tells us that F_n converges to a power series F in $\mathcal{O}_{\hat{K}}[[X_1, \dots, X_m]]$ such that $F \equiv F_n$ mod deg $n + 1$ for all $n \geq 1$. So we see that this power series F satisfies the following:

$$F \equiv F_1 = L \text{ mod deg } 2,\ \ f_1 \circ F = F^{\varphi} \circ f_2. \tag{4.47}$$

Now we prove the uniqueness of F. Let F' be any power series satisfying the above-mentioned conditions. Then, for $n \geq 1$, let F_n' represent the the sum which is composed of the terms of degree $\leq n$ in the power series F' and let $F_{n+1}' = F_n' + H_{n+1}'$. Since $F' \equiv L$ mod deg 2, we see $F_1' = L = F_1$. But we proved that H_{n+1} is unique so $F_n' = F_n$ for all $n \leq 1$. Then $F' = F$. □

Remark. In the proof above, we implicitly used the continuity property of formal power series composition. For the proof, refer to [17].

5. FORMAL GROUPS

In this chapter, we will discuss formal groups and then we will introduce the Lubin-Tate formal groups which will be the main tool in the following chapters. The main references for this chapter are [8], [15], [6] and [3].

5.1. BASIC DEFINITIONS

Definition 5.1.1. Let R be a commutative ring with $1 \neq 0$ and $X, Y,$ and Z indeterminates. A power series $F(X,Y)$ in $R[[X,Y]]$ is called a **formal group** over R if it satisfies the following conditions:

F1. $F(X,Y) \equiv X + Y \text{ mod deg } 2,$

F2. $F(F(X,Y),Z) = F(X,F(Y,Z)),$

F3. $F(X,Y) = F(Y,X).$

By F1, $F(0,0) = 0$, so we do not encounter any convergence issues in F2.
Let $Y = Z = 0$ in F1 and F2. So we see that

$$F(X,0) \equiv X \text{ mod deg } 2, \;\; F(F(X,0),0) = F(X,0). \tag{5.1}$$

First equivalence in 5.1 tells us that $f(X) := F(X,0)$ has an inverse f^{-1} in $M = XR[[X]]$ (consider the first coefficient: $1 \cdot X$). So if we apply f^{-1} to the second equality in 5.1, we get $F(X,0) = X$. Similarly, we also get $F(0,Y) = Y$. Then,

$$F(X,Y) = X + Y + \sum_{i,j\ \geq 1}^{\infty} c_{ij} X^i Y^j, \;\; c_{ij} \in R. \tag{5.2}$$

Note that this implies $F(X,Y)$ has no terms like X^3 or Y^2, etc.

There exists a unique power series

$$i_F(X) = -X + \sum_{i=2}^{\infty} b_i X^i, \;\; b_i \in R, \tag{5.3}$$

such that

$$F(X, i_F(X)) = 0. \tag{5.4}$$

For $f, g \in M = XR[[X]]$ define a binary operation $+_F$ on M:

$$f +_F g = F(f(X), g(X)). \tag{5.5}$$

Note that the addition $f +_F g$ belongs to M and the following proposition easily follows from the formal group axioms and the equation 5.4.

Proposition 5.1.1. *The set M becomes an Abelian group with respect to the addition $f +_F g$ and the inverse of f is $i_F(f)$.*

We denote this group by M_F.

Let $G(X, Y)$ be another formal group over R and let $f(X)$ be a power series in $M = XR[[X]]$ such that

$$f(F(X, Y)) = G(f(X), f(Y)). \tag{5.6}$$

We call such f a **homomorphism** from F to G and write $f : F \to G$. In particular, if f has an inverse f^{-1} in M, then we can easily see that f^{-1} is a homomorphism from G to F. In this case we say f is an **isomorphism** and we write $f : F \cong G$. From now on, we will write $f \circ F = G \circ f$ instead of the equation 5.6.

Let $F(X_1, \dots, X_m)$ be any power series in $R[[X_1, \dots, X_m]]$ and $f \in M = XR[[X]]$ invertible in M. We define a power series $F^f(X_1, \dots, X_m)$ in $R[[X_1, \dots, X_m]]$ by

$$F^f(X_1, \dots, X_m) = f \circ F \circ f^{-1} = f(F(f^{-1}(X_1), \dots, f^{-1}(X_m))). \tag{5.7}$$

We see that if $F(X, Y)$ is a formal group over R, then $G = F^f$ is also a formal group and $f : F \cong G$.

We put

$$\mathrm{Hom}_R(F, G) := \{f \mid f \text{ is a homomorphism from } F \text{ to } G\}. \tag{5.8}$$

and in particular we set

$$\mathrm{End}_R(F) := \mathrm{Hom}_R(F, F). \tag{5.9}$$

Example 13. If $F(X, Y) = X + Y + XY$, then $f(T) = (1 + T)^p - 1$ is an endomorphism where p is a prime number.

Concerning the set $\mathrm{Hom}_R(F,G)$, we have the followng lemma:

Lemma 5.1.2. $\mathrm{Hom}_R(F,G)$ *is a subgroup of the Abelian group* M_G *and* $\mathrm{End}_R(F)$ *is a ring with respect to the addition* $f +_F g$ *and the multiplication* $f \circ g$ *defined by the power series composition where* $f, g \in \mathrm{Hom}_R(F,G)$.

Proof. Let $f, g \in \mathrm{Hom}_R(F,G)$ and $h = f +_G g$. Then,

$$h \circ F = f \circ F +_G g \circ F = G \circ f +_G G \circ g = G(G \circ f, G \circ g). \tag{5.10}$$

Using the formal group axioms, we get

$$\begin{aligned} G(G \circ f, G \circ g) &= G(G(f(X), g(X)), G(f(Y), g(Y))) \qquad (5.11) \\ &= G((f +_G g)(X), (f +_G g)(Y)) \qquad (5.12) \\ &= G \circ h. \qquad (5.13) \end{aligned}$$

So $\mathrm{Hom}_R(F,G)$ is closed under addition. Consider the following equality:

$$G(G(X,Y), G(i_G(X), i_G(Y)) = G(G(X, i_G(X)), G(Y, i_G(Y)) = G(0,0) = 0. \tag{5.14}$$

This tells us that $G \circ i_G = i_G \circ G$ (by the formal group axioms). So,

$$i_G(f) \circ F = i_G \circ f \circ F = i_G \circ G \circ f = G \circ i_G \circ f = G \circ i_G(f). \tag{5.15}$$

Now it has been shown that $i_G(f) \in \mathrm{Hom}_R(F,G)$. Clearly $0 \in \mathrm{Hom}_R(F,G)$. We have proved that $\mathrm{Hom}_R(F,G)$ is a subgroup of M_G.

For the second part of the lemma, we will show that the distributive law holds in $\mathrm{End}_R(F)$, since the rest easily follows from the axioms and the definitions.
Let $f \in \mathrm{End}_R(F)$ and $g, h \in M_F$. Then,

$$f \circ (g +_F h) = f(F(g(X), h(X))) = F(f(g(X), f(h(X))) = f \circ g +_F f \circ h. \tag{5.16}$$

□

5.2. LUBIN-TATE FORMAL GROUPS $F_f(X,Y)$

Let k be a local field, $\kappa_k = \mathcal{O}_k/\mathfrak{p}_k = \mathbb{F}_q$ its residue field. Here, the same notation will be used as in the section 4.2. For a prime $\pi_{\widehat{K}}$ of $\widehat{K}$, $\mathcal{F}_{\pi_{\widehat{K}}}$ denotes the family of all power series $f(X)$ in $R[[X]]$ satisfying

$$f(X) \equiv \pi_{\widehat{K}} X \text{ mod deg } 2, \;\; f(X) \equiv X^q \text{ mod } \mathfrak{p}_{\widehat{K}}. \tag{5.17}$$

For example, the polynomial $\pi_{\widehat{K}} X + X^q$ belongs to $\mathcal{F}_{\pi_{\widehat{K}}}$. Also, we see that if $f \in \mathcal{F}_{\pi_{\widehat{K}}}$, then $f^\varphi \in \mathcal{F}_{\varphi(\pi_{\widehat{K}})}$. The union of the sets $\mathcal{F}_{\pi_{\widehat{K}}}$ for all prime $\pi_{\widehat{K}}$'s of $\widehat{K}$ is denoted by

$$\mathcal{F} = \bigcup_{\pi_{\widehat{K}} \text{ is a prime in } \widehat{K}} \mathcal{F}_{\pi_{\widehat{K}}}. \tag{5.18}$$

Theorem 5.2.1. *For each $f \in \mathcal{F}_\pi$, there exists a unique formal group $F_f(X,Y)$ over R such that $f \in \mathrm{Hom}_R(F_f, F_f^\varphi)$: $f \circ F_f = F_f^\varphi \circ f$. Here, F_f's are called* ***Lubin-Tate formal groups****.*

Proof. Take $\pi_1 = \pi_2 = \pi$, $f_1 = f_2 = f$, $L(X,Y) = X + Y$ and $m = 2$ in Theorem 4.2.2. Then there exists a unique power series $F(X,Y)$ in $R[[X,Y]]$ such that

$$F(X,Y) \equiv X + Y \text{ mod deg } 2, \tag{5.19}$$

$$f \circ F = F^\varphi \circ f. \tag{5.20}$$

We verify that F_f satisfies the formal group axioms F2 and F3.

Associativity:

Let

$$F_1(X,Y,Z) = F(F(X,Y),Z), \tag{5.21}$$

$$F_2(X,Y,Z) = F(X,F(Y,Z)). \tag{5.22}$$

By the equations 5.19 and 5.20, we get

$$F_1(X,Y,Z) \equiv F(X,Y) + Z \equiv X + Y + Z \text{ mod deg } 2, \tag{5.23}$$

$$f \circ F_1 = F^{\varphi}(f(F(X,Y)), f(Z)) = F^{\varphi}(F^{\varphi}(f(X), f(Y)), f(Z)) = F_1^{\varphi} \circ f. \tag{5.24}$$

By the similar argument,

$$F_2(X,Y,Z) \equiv X + Y + Z \text{ mod deg } 2, \;\; f \circ F_2 = F_2^{\varphi} \circ f. \tag{5.25}$$

Now, if we take $L(X,Y,Z) = X + Y + Z$, the uniqueness part of Theorem 4.2.2 implies $F_1 = F_2$; that is the associative property for formal groups holds:

$$F(F(X,Y),Z) = F(X, F(Y,Z)). \tag{5.26}$$

Commutativity:

To prove the commutativity, let $G(X,Y) = F(Y,X)$. Then we see,

$$G(X,Y) \equiv X + Y \text{ mod deg } 2, \;\; f \circ G = G^{\varphi} \circ f. \tag{5.27}$$

Since $F(X,Y)$ is unique by the Theorem 4.2.2, we obtain $F = G$; that is $F(X,Y) = F(Y,X)$. We have proved that $F(X,Y)$ is a formal grup (over R). It can be easily shown that F^{φ} is a formal group (over R). Write F_f for F. So F_f is the unique formal group over R satisfying $f \circ F_f = F_f^{\varphi} \circ f$, meaning that $f \in \text{Hom}_R(F_f, F_f^{\varphi})$. □

Remark. Observe that the equality $f \circ F_f = F_f^{\varphi} \circ f$ implies $f^{\varphi} \circ F_f^{\varphi} = (F_f^{\varphi})^{\varphi} \circ f^{\varphi}$. But it means that

$$F_f^{\varphi} = F_{f^{\varphi}}, \;\; \text{where } f^{\varphi} \in \mathcal{F}_{\varphi(\pi)}. \tag{5.28}$$

Let $f \in \mathcal{F}$ and $a \in \mathcal{O}_k$ of k. If we apply Theorem 4.2.2 for $L(X) = aX$, we see there is a unique power series $\psi(X)$ in $R[[X]]$, which satisfies the following conditions:

$$\psi(X) \equiv aX \text{ mod deg } 2, \;\; f \circ \psi = \psi^{\varphi} \circ f. \tag{5.29}$$

We denote this power series $\psi(X)$ by $[a]_f$.

Theorem 5.2.2. *For each $a \in \mathcal{O}_k$, $[a]_f \in \text{End}_R(F_f)$. Moreover the map $a \mapsto [a]_f$ is injective* *and it is a ring homomorphism:*

$$\xi_f : \mathcal{O}_k \to \mathrm{End}_R(F_f). \tag{5.30}$$

Proof. Let $\psi := [a]_f$. Consider the following equations:

$$f \circ \psi \circ F_f = \psi^{\varphi} \circ f \circ F_f = \psi^{\varphi} \circ F_f^{\varphi} \circ f = (\psi \circ F_f)^{\varphi} \circ f, \tag{5.31}$$

$$f \circ F_f \circ \psi = F_f^{\varphi} \circ f \circ \psi = F_f^{\varphi} \circ \psi^{\varphi} \circ f = (F_f \circ \psi)^{\varphi} \circ f, \tag{5.32}$$

$$\psi \circ F_f \equiv F_f \circ \psi \equiv a(X+Y) \text{ mod deg } 2. \tag{5.33}$$

So, by 5.31, 5.32 and 5.33 together with the uniqueness in Theorem 4.2.2,

$$\psi \circ F_f = F_f \circ \psi, \text{ that is, } \psi = [a]_f \in \mathrm{End}_R(F_f). \tag{5.34}$$

Let $a, b \in \mathcal{O}_k$. Along the similar lines,

$$f \circ ([a]_f +_F [b]_f) = f \circ F_f([a]_f, [b]_f) \tag{5.35}$$

$$= F_f^{\varphi}(f \circ [a]_f, f \circ [b]_f) \tag{5.36}$$

$$= F^{\varphi}([a]_f^{\varphi} \circ f, [b]_f^{\varphi} \circ f) \tag{5.37}$$

$$= ([a]_f +_F [b]_f)^{\varphi} \circ f. \tag{5.38}$$

Also we have

$$[a]_f +_F [b]_f \equiv [a+b]_f \equiv (a+b)X \text{ mod deg } 2. \tag{5.39}$$

Hence we see $[a]_f +_F [b]_f = [a+b]_f$. Similarly we get $[a]_f \circ [b]_f = [ab]_f$. So we have proved that $a \mapsto [a]_f$ defines a ring homomorphism $\xi_f : \mathcal{O}_k \to \mathrm{End}_R(F_f)$. This homomorphism is injective because a depends on $[a]_f \equiv aX$ mod deg 2. □

Take two primes π and π' in $\widehat{K}$ and let $f \in \mathcal{F}_{\pi}, f' \in \mathcal{F}_{\pi'}$. Recall that $\pi' = \pi\xi,\ \xi \in U(\widehat{K})$. By Lemma 4.2.1, $\exists \eta \in U(\widehat{K})$ satisfying $\xi = \eta^{\varphi - 1}$. Let $L(X) = \eta X$. Then $\pi' L(X) = \pi L^{\varphi}(X)$. So, applying Theorem 4.2.2 for $f_1 = f',\ f_2 = f,\ \pi_1 = \pi',\ \pi_2 = \pi,\ L(X) = \eta X$, we can conclude that, in $\mathcal{O}_{\hat{K}}[[X]]$, $\exists!\theta(X)$ such that

$$\theta(X) \equiv \eta X \text{ mod deg } 2, \;\; f' \circ \theta = \theta^{\varphi} \circ f. \tag{5.40}$$

Also, since $\eta \in U(\widehat{K})$, $\theta(X)$ is invertible in $M = X\mathcal{O}_{\hat{K}}[[X]]$.

Theorem 5.2.3. *The power series $\theta(X)$ has the following properties:*

(i) $\theta : F_f \cong F_{f'}$, *i.e.,* $F_f^{\theta} = F_{f'}$,

(ii) $[a]_f^{\theta} = [a]_{f'}$ *for* $a \in \mathcal{O}_k$.

Proof. To prove (i) consider the following relationships:

$$f' \circ \theta \circ F_f = \theta^{\varphi} \circ f \circ F_f = \theta^{\varphi} \circ F_f^{\varphi} \circ f = (\theta \circ F_f)^{\varphi} \circ f, \tag{5.41}$$

$$f' \circ F_{f'} \circ \theta = F_{f'}^{\varphi} \circ f' \circ \theta = F_{f'}^{\varphi} \circ \theta^{\varphi} \circ f = (F_{f'} \circ \theta)^{\varphi} \circ f, \tag{5.42}$$

$$\theta \circ F_f \equiv F_f \circ \theta \equiv \eta(X+Y) \text{ mod deg } 2. \tag{5.43}$$

If we use the uniqueness property in Theorem 4.2.2 with $L(X,Y) = \eta(X+Y)$, we see that

$$\theta \circ F_f = F_{f'} \circ \theta, \text{ i.e., } F_f^{\theta} = F_{f'}. \tag{5.44}$$

This concludes the proof for (i). The proof for (ii) is similar. □

Theorem 5.2.3 tells us that formal groups F_f's over $\mathcal{O}_{\hat{K}}$ are isomorphic to each other for all power series f in the family $\mathcal{F}$.

Example 14. Let $k = \mathbb{Q}_p$ and $\pi = p$. Then, $f(X) = (1+X)^p - 1 \in \mathcal{F}_p$. One can directly show that $F(X,Y) = F_f = X + Y + XY$. For any $a \in \mathbb{Z}_p$ define

$$(1+X)^a = \sum_{m \geq 0} \binom{a}{m} X^m, \;\; \binom{a}{m} = \frac{a(a-1)\cdots(a-m+1)}{m(m-1)\cdots 1}. \tag{5.45}$$

It can be shown $\binom{a}{m} \in \mathbb{Z}_p$. We claim that

$$[a]_f = (1+X)^a - 1. \tag{5.46}$$

To prove this, note that $(1+X)^a - 1 = aX + \dots$ and recall that $\varphi|_k = \mathrm{id}_k$. Also,

$$f \circ ((1+X)^a - 1) = (1+X)^{ap} - 1 = ((1+X)^a - 1) \circ f \tag{5.47}$$

holds when a is an integer, which (by continuity) implies that it holds for all $a \in \mathbb{Z}_p$.

6. THE MAIN THEOREMS

The main references for this chapter are [8], [15], [9] and [2].

Let k be a local field. Fix an algebraic closure k^{alg} of k. Let k^{ab} denote the maximal Abelian subextension in k^{alg} over k, which is the compositum of all finite Abelian extension over k. Abelian local class field theory for k [2] states that a unique group homomorphism exists:

$$Art_k : k^\times \to \mathrm{Gal}(k^{ab}/k), \tag{6.1}$$

which is called the **local Artin map** of k characterized by two properties below:

(i) For a prime $\pi \in k$, $Art_k(\pi)|_{k_{ur}} = \varphi_k$, where φ_k is the Frobenius automorphism of k_{ur}.

(ii) For each finite Abelian extension k' over k, $\mathrm{Art}_k(N(k'/k)) \mid_{k'} = 1$.

In this chapter, we have three objectives:

(i) For a fixed prime element $\pi \in k$, we will construct a maximal totally ramified extension k_π/k in k^{ab}.

(ii) We will define a map $\rho_k : k^\times \to \mathrm{Gal}(k^{ab}/k)$.

(iii) We will show that this map ρ_k is the **local Artin map** and we will prove $k^{ab} = k_\pi k_{ur}$ using the local Artin map .

6.1. $\mathcal{O}_k$-MODULES W_f^n

In this section, we keep the same terminology and assumptions as in the section 3.6 and as in the sections of the Chapter 5. For a local field k, we will define an $\mathcal{O}_k$-module structure on $\mathfrak{m} := \mathfrak{p}_{\widehat{k^{alg}}}$ and using these modules, we will construct certain finite Galois extensions of k.

As before, let $\widehat{K}$ denote the completion of $k_{ur}(= K)$ and let $F_f(X, Y)$ be the formal group over $R = \mathcal{O}_{\widehat{K}}$ for an $f \in \mathcal{F}$. For $\alpha, \beta \in \mathfrak{p}_{\widehat{k^{alg}}}$ and for any $a \in \mathcal{O}_k$, define

$$\alpha +_f \beta = F_f(\alpha, \beta), \;\; a \cdot_f \alpha = [a]_f(\alpha). \tag{6.2}$$

Here we see that $F_f(\alpha,\beta)$ and $[a]_f(\alpha) \in \mathcal{O}_{\hat{K}}$. Also, since $F_f(X,Y) \equiv 0$ mod deg 1 and $[a]_f(X) \equiv 0$ mod deg 1 by definition, we get

$$\alpha +_f \beta,\ \ a \cdot_f \alpha \in \mathfrak{p}_{\widehat{k^{alg}}} \tag{6.3}$$

for $\alpha, \beta \in \mathfrak{p}_{\widehat{k^{alg}}}$, $a \in \mathcal{O}_k$.

The set $\mathfrak{p}_{\widehat{k^{alg}}}$ can be seen to be an Abelian group, the operation of which is the adition $+_f$ defined above. In this group, the inverse of an element α is $i_F(\alpha)$ (consider the equation 5.4). It can be shown that the operations in 6.2 defines an $\mathcal{O}_k$-module structure on $\mathfrak{p}_{\widehat{k^{alg}}}$. For example:

Since we know that $[a]_f \circ F_f = F_f \circ [a]_f$ (the equality 5.34),

$$a \cdot_f (\alpha +_f \beta) = [a]_f(F_f(\alpha,\beta)) = F_f([a]_f(\alpha), [a]_f(\beta)) = (a \cdot_f \alpha) +_f (a \cdot_f \beta). \tag{6.4}$$

The other module axioms can be proved similarly. If we define this $\mathcal{O}_k$-module structure on $\mathfrak{p}_{\widehat{k^{alg}}}$, we denote $\mathfrak{p}_{\widehat{k^{alg}}}$ by $\mathfrak{m}_f$.

Now, for any integer $n \geq 1$, a fixed f and $\alpha \in \mathfrak{m}_f$ we define:

$$\mathfrak{p}^{n+1} \cdot_f \alpha = \{a \cdot_f \alpha \mid a \in \mathfrak{p}^{n+1}\}, \tag{6.5}$$

$$W_f^n = \{\alpha \in \mathfrak{m}_f \mid \mathfrak{p}^{n+1} \cdot_f \alpha = 0\}. \tag{6.6}$$

For $n \geq -1$, W_f^n's constitute a nested sequence of $\mathcal{O}_k$-submodules of $\mathfrak{m}_f$:

$$\{0\} = W_f^{-1} \subseteq W_f^0 \subseteq \cdots \subseteq W_f^n \subseteq \cdots \subseteq W_f, \tag{6.7}$$

where

$$W_f = \bigcup_{n\geq -1}^{\infty} W_f^n. \tag{6.8}$$

Now take f' in $\mathcal{F}$. By Theorem 5.2.3, we know that there exists an invertible $\theta(X) \in XR[[X]]$ satisfying $F_f^\theta = F_{f'}$ and $[a]_f^\theta = [a]_{f'}$ $(a \in \mathcal{O}_k)$. We can show that θ defines an $\mathcal{O}_k$-module isomorphism:

$$\theta : \mathfrak{m}_f \cong \mathfrak{m}_{f'}. \tag{6.9}$$

It is clear that $\theta(\alpha) \in \mathfrak{m}_{f'}$ where $\alpha \in \mathfrak{m}$, since $\theta \equiv 0$ mod deg 1. Also observe that

$$\theta(\alpha +_f \beta) = \theta(F_f(\alpha, \beta)) = F_{f'}(\theta(\alpha), \theta(\beta)) = \theta(\alpha) +_{f'} \theta(\beta) \tag{6.10}$$

The other properties of the isomorphism can be proved similarly. The power series θ also induces the following $\mathcal{O}_k$-module isomorphisms:

$$\theta' : W_f^n \cong W_{f'}^n, \quad \theta'' : W_f \cong W_{f'}, \quad n \geq -1. \tag{6.11}$$

Now we will explicitly describe the elements of W_f^n's.

Lemma 6.1.1. *Define*

$$f_i \coloneqq f^{\varphi^i}, \quad g_i \coloneqq f_i \circ f_{i-1} \circ \cdots \circ f_0, \quad g_{-1}(X) = X \tag{6.12}$$

for $f \in \mathcal{F}$ *and* $i \geq 0$. *Then*

$$W_f^n = \{\alpha \in \mathfrak{m} \mid g_n(\alpha) = 0\}, \quad \textit{for} \ \ n \geq -1. \tag{6.13}$$

Proof. The lemma is true for $n = -1$ since $W_f^{-1} = \{0\}$ and $g_{-1}(X) = X$. Now let $n \geq 0$ and take f' and θ as above. Then we know that $f' \circ \theta = \theta^{\varphi} \circ f$. We have the following:

$$f_i' \circ \theta^{\varphi^i} = \theta^{\varphi^{i+1}} \circ f_i, \quad f_i' = \theta^{\varphi^{i+1}} \circ f_i \circ \theta^{-\varphi^i}, \ \ i \geq 0, \tag{6.14}$$

$$g_n' = f_n' \circ f_{n-1}' \circ \cdots \circ f_0' = \theta^{\varphi^{i+1}} \circ g_n \circ \theta^{-1}, \ \ n \geq 0. \tag{6.15}$$

The last two equations imply that if the lemma is true for f, then it also true for f'. To see this, let $\beta \in W_{f'}^n$ and consider $\theta^{-1}(\beta) = \alpha$. Then

$$g_n'(\beta) = \theta^{\varphi^{i+1}} \circ g_n \circ \theta^{-1}(\beta) = \theta^{\varphi^{i+1}} \circ g_n(\alpha) = 0. \tag{6.16}$$

Let $\pi_k \in k$. We know that K/k is an unramified extension so $\pi_k \in \widehat{K}$. Hence

$$f(X) = \pi_k X + X^q \in \mathcal{F}. \tag{6.17}$$

Observe that $\pi_k \in \mathcal{O}_k, f \equiv \pi_k X$ mod deg 2 and $f \circ f = f^{\varphi} \circ f$. By the equation in 5.29, this implies

$$f = [\pi_k]_f, \quad f_i = f, \quad g_n = \underbrace{f \circ \cdots \circ f}_{\text{n+1 many}} = [\pi_k^{n+1}]_f. \tag{6.18}$$

Since $\mathfrak{p}_k^{n+1} = \mathcal{O}_k \pi_k^{n+1}$, we have the following:

$$W_f^n = \{\alpha \in \mathfrak{m}_f \mid \mathfrak{p}_k^{n+1} \cdot_f \alpha = 0\} = \{\alpha \in \mathfrak{m} \mid g_n(\alpha) = 0\}. \tag{6.19}$$

Now we have proved that the lemma is valid for $f(X)$. So it is valid for any $f \in \mathcal{F}$. □

Take an integer $m \geq 1$ and consider $k' := k_{ur}^m$ (the unique unramified extension of degree m over k in k^{alg}).

Take a prime $\pi_{k'}$ in k'. Then the polynomial $f(X) = \pi_{k'} X + X^q \in \mathcal{O}_{k'}[[X]]$ and it is also a member of $\mathcal{F}$. Since k'/k is a complete extension, the following hold:

$$F(X,Y) \in \mathcal{O}_{k'}[[X,Y]], \quad [a]_f(X) \in \mathcal{O}_{k'}[[X]], \quad \text{for } a \in \mathcal{O}_k. \tag{6.20}$$

For $n \geq 0$, define

$$h_n(X) = \pi_{k'}^{\varphi^n} + [g_{n-1}(X)]^{q-1}. \tag{6.21}$$

Then we see that

$$g_n = f_n \circ g_{n-1} = f^{\varphi^n} \circ g_{n-1} = h_n(X) g_{n-1}(X) \tag{6.22}$$

and

$$g_n(X) = h_n(X) h_{n-1}(X) \cdots h_0(X) X. \tag{6.23}$$

Now we will study the properties of $h_n(X)$ and $g_n(X)$.

Lemma 6.1.2. *The following hold for $h_n(X)$ and $g_n(X)$:*

(i) The polynomial $h_n(X)$ is a monic separable irreducible polynomial of degree $(q-1)q^n$

in $\mathcal{O}_{k'}[X]$ and it is also irreducible in $\widehat{K}[X]$.

(ii) The polynomial $g_n(X)$ is a monic separable polynomial of degree q^{n+1} in $\mathcal{O}_{k'}[X]$. The set W_f^n consists of all roots of $g_n(X)$ in k^{alg}. The order of W_f^n is equal to q^{n+1} and hence the extension $k'(W_f^n)/k'$ is a finite Galois extension over k'.

(iii) For $n \geq 0$, let $h_n(\alpha_0) = 0$, where $\alpha_0 \in k^{alg}$. Then following hold:

- $\alpha_0 \in W_f^n$, $\alpha_0 \notin W_f^{n-1}$, $(q-1)q^n = [k'(\alpha_0) : k']$ *and*
- $\pi_{k'}^{\varphi^n} = N(-\alpha_0) \in N(k'(\alpha_0)/k')$.

Proof. By definition, $g_n = f_n \circ f_{n-1} \circ \cdots \circ f_0$. So,

$$g_n(X) = a_n X + \cdots + X^{q^{n+1}} \equiv X^{q^{n+1}} \bmod \mathfrak{p}', \text{ where } a_n = \pi^{1+\varphi+\cdots+\varphi^n}, \tag{6.24}$$

$$h_n(X) = \pi^{\varphi^n} + (a_{n-1}X + \cdots + X^{q^n})^{q-1} \equiv X^{(q-1)q^n} \bmod \mathfrak{p}'. \tag{6.25}$$

From the equations above, we see that $g_n(X)$ and $h_n(X)$ are monic polynomials in $\mathcal{O}_{k'}[X]$ of degrees q^{n+1} and $(q-1)q^n$, respectively. Since π^{φ^n} is a prime in $\widehat{K}$ (remember that automorphisms do not change the valution of an element), the polynomial $h_n(X)$ is Eisenstein in $\mathcal{O}_{\widehat{K}}[X]$. This implies that $h_n(X)$ is irreducible in $\widehat{K}[X]$. Now suppose that k has char p so that q is a power of p. Note that

$$\frac{dh_n}{dX} = (q-1)a_{n-1}^{q-1}X^{q-2} + \cdots, \quad a_{n-1} = \pi^{1+\varphi+\cdots+\varphi^{n-1}}. \tag{6.26}$$

Here $\frac{dh_n}{dX}$ denotes formal derivative. Since $(q-1)a_{n-1}^{q-1} \neq 0$, $h_n(X)$ is separable. Also, since $h_n(X)$ is irreducible, $h_i(X) \neq h_j(X)$ for $i \neq j$. Hence $g_n(X) = h_n(X)h_{n-1}\cdots h_0(X)X$ is a separable polynomial. We know that if $\alpha \in W_f^n$, then $g_n(\alpha) = 0$ (clearly $\alpha \in k^{alg}$. Conversely, assume that $g_n(\alpha) = 0$, where $\alpha \in k^{alg}$. Then by the equation 6.24, $\hat{\mu}(\alpha) > 0$, so $\alpha \in \mathfrak{m} \cap k^{alg}$. This means that W_f^n consists of the set of all roots of $g_n(X)$, which is a separable polynomial, in k^{alg}. The order of W_f^n is q^{n+1} and $k'(W_f^n)/k'$ is a finite Galois extension. Now we have proved (i) and (ii). For the first part of (iii), consider $h_i(X) \neq h_j(X)$ for $i \neq j$. If $\alpha_0 \in W_f^{n-1}$, then it would be a root of some $h_i(X)$, $0 \leq i \leq n-1$ or 0 which is a contradiction. The second part of (iii) is the consequence of the fact that the constant term in $h_n(X)$ is $\pi_{k'}^{\varphi^n}$. □

Lemma 6.1.3. *Let $f \in \mathcal{F} \subseteq \mathcal{O}_{\bar{k}}[[X]]$. Then the following hold:*

(i) Fix an element $\alpha_0 \in W_f^n \setminus W_f^{n-1}$ for $n \geq 0$. Then $W_f^n = \mathcal{O}_k \cdot_f \alpha_0$ and the map

$$\xi_f : a \mapsto a \cdot_f \alpha_0 \tag{6.27}$$

induces the following isomorphism:

$$\mathcal{O}_k / \mathfrak{p}_k^{n+1} \cong W_f^n. \tag{6.28}$$

(ii) $\mathfrak{p}_k^i \cdot_f W_f^n = W_f^{n-i}$ for $0 \leq i \leq n$.

Proof. Since $|W_f^n|$ is q^{n+1} and $|W_f^{n-1}|$ is q^n, there exists an α_0 such that $\alpha_0 \in W_f^n \setminus W_f^{n-1}$. It is clear that ξ_f is an $\mathcal{O}_k$-module homomorphism. Also, by definition, $\mathfrak{p}_k^{n+1} \cdot_f \alpha_0 = 0$ and $\mathfrak{p}_k^n \cdot_f \alpha_0 \neq 0$. The kernel contains $\mathfrak{p}_k^{n+1}$ but not $\mathfrak{p}_k^n$; i.e., it is equal to $\mathfrak{p}_k^{n+1}$ for every $n \geq 0$. Since we know that $[\mathcal{O}_k : \mathfrak{p}_k^{n+1}] = q^{n+1}$,

$$\mathcal{O}_k / \mathfrak{p}_k^{n+1} \cong W_f^n \text{ and } W_f^n = \mathcal{O}_k \cdot_f \alpha_0. \tag{6.29}$$

Now we have proved (i). For (ii), let π be a prime in k. So

$$\alpha_0 \in W_f^n \setminus W_f^{n-1} \implies \pi^i \cdot_f \alpha_0 \in W_f^{n-i}, \pi^i \cdot_f \alpha_0 \notin W_f^{n-i-1}. \tag{6.30}$$

So if we apply (i),

$$\mathfrak{p}_k^i \cdot_f W_f^n = \pi^i \cdot_f \mathcal{O}_k \cdot_f \alpha_0 = \mathcal{O}_k \cdot_f \pi^i \cdot_f \alpha_0 = W_f^{n-i}. \tag{6.31}$$

Hence the proof is complete. □

Let $f \in \mathcal{F}$. We define

$\mathrm{End}(W_f^n) :=$ the endomorphisms ring of the $\mathcal{O}_k$-module W_f^n,

$\mathrm{Aut}(W_f^n) :=$ the group of all automorphisms of the $\mathcal{O}_k$-module W_f^n.

Consider the following map:

$$\xi_a : W_f^n \to W_f^n, \tag{6.32}$$

$$\beta \mapsto a \cdot_f \beta = [a]_f(\beta), \tag{6.33}$$

where $a \in \mathcal{O}_k$. Since W_f^n is and $\mathcal{O}_k$-submodule, ξ_a is an endomorphism. If we take $b \in U_k$, then ξ_b becomoes invertible since $[b^{-1}]_f = [b]_f^{-1}$. So the map $a \mapsto \xi_a$ defines the following homomorphisms for the ring $\mathrm{End}(W_f^n)$ and the group $\mathrm{Aut}(W_f^n)$:

$$\alpha : \mathcal{O}_k \to \mathrm{End}(W_f^n), \tag{6.34}$$

$$\beta : \mathcal{U}_k \to \mathrm{Aut}(W_f^n). \tag{6.35}$$

Theorem 6.1.4. *The homomorphisms α and β induce the following isomoprhisms:*

$$\mathcal{O}_k/\mathfrak{p}^{n+1} \cong \mathrm{End}(W_f^n), \tag{6.36}$$

$$\mathcal{U}_k/\mathcal{U}_{n+1} \cong \mathrm{Aut}(W_f^n), \tag{6.37}$$

where $n \geq 0$.

Proof. Take $a \in W_f^n \setminus W_f^{n-1}$. Then we know that $W_f^n = \mathcal{O}_k \cdot_f a$ by Lemma 6.1.3. We show that the homomorphism α is surjective. Take $\xi \in \mathrm{End}(W_f^n)$. So $\xi(a) = b \cdot_f a$ for some $b \in \mathcal{O}_k$. Let $c \in W_f^n$. By the module axioms,

$$\xi(c) = \xi(d \cdot_f a) = d \cdot_f \xi(a) = d \cdot_f (b \cdot_f a) = b \cdot_f (d \cdot_f a) = b \cdot_f c. \tag{6.38}$$

That means $\xi = \xi_b$. So the homomorphism α is surjective. Since $\mathfrak{p}^{n+1} \cdot_f W_f^n = 0$ and $\mathfrak{p}^n \cdot_f W_f^n = W_f^0 \neq 0$, the kernel of α is $\mathfrak{p}^{n+1}$; hence we proved that $\mathcal{O}_k/\mathfrak{p}^{n+1} \cong \mathrm{End}(W_f^n)$. Since the unit group of $\mathcal{O}_k/\mathfrak{p}^{n+1}$ is isomorphic to $\mathcal{U}_0/\mathcal{U}_{n+1}$, it follows that $\mathcal{U}_0/\mathcal{U}_{n+1} \cong \mathrm{Aut}(W_f^n)$. □

6.2. EXTENSIONS $\widehat{L}^n/\widehat{K}$

In this section, we will study the extension $\widehat{K}(W_f^n)/\widehat{K}$ and define a natural homomorphism from $\mathcal{U}_k$ to $\mathrm{Gal}(\widehat{K}(W_f^n)/\widehat{K})$.

Lemma 6.2.1. *The extension $\widehat{K}(W_f^n)/\widehat{K}$ is a finite Galois extension over $\widehat{K}$ and independent of f in the family $\mathcal{F}$.*

Proof. Take $f(X) = \pi X + X^q$, where π is a prime in $k' = k_{ur}^m$. By Lemma 6.1.2, $k'(W_f^n)/k'$ is a finite Galois extension. As $k' \subseteq \widehat{K}$, $\widehat{K}(W_f^n)/\widehat{K}$ is also a finite Galois. Since $\widehat{K}$ is complete by definition and $\widehat{K}(W_f^n)/\widehat{K}$ is a finite extension, $\widehat{K}(W_f^n)$ is also complete in $\widehat{k^{alg}}$. Take any power series $f' \in \mathcal{F}$ and let $\theta(X)$ be the power series as in Theorem 5.2.3. Then,

$$\theta(W_f^n) = W_{f'}^n, \quad \theta^{-1}(W_{f'}^n) = W_f^n. \tag{6.39}$$

The power series $\theta(X) \in \mathcal{O}_{\widehat{K}}[[X]]$ and $\widehat{K}(W_f^n)$ is complete, so

$$W_{f'}^n = \theta(W_f^n) \subseteq \widehat{K}(W_f^n). \tag{6.40}$$

This implies that

$$\widehat{K} \subseteq \widehat{K}(W_{f'}^n) \subseteq \widehat{K}(W_f^n). \tag{6.41}$$

Since $\theta(X)$ is invertible and $\theta^{-1}(W_{f'}^n) = W_f^n$, similarly we get $\widehat{K}(W_f^n) \subseteq \widehat{K}(W_{f'}^n)$. So

$$\widehat{K}(W_f^n) = \widehat{K}(W_{f'}^n). \tag{6.42}$$

□

We denote the field $\widehat{K}(W_f^n)$ by $\widehat{L}^n$.

Theorem 6.2.2. *There exists a homomorphism*

$$\gamma^n : \mathcal{U}_k \to \mathrm{Gal}(\widehat{L}^n/\widehat{K}) \tag{6.43}$$

where $n \geq 0$, *satisfying that for* $u \in \mathcal{U}_k$,

$$\gamma^n(u)(\alpha) = u \cdot_f \alpha \tag{6.44}$$

$$= [u]_f(\alpha) \tag{6.45}$$

for every $f \in \mathcal{F}$ *and for every* $\alpha \in W_f^n$. *The homomorphism* γ^n *induces the following isomorphism:*

$$\mathcal{U}_k/\mathcal{U}_{n+1} \cong \mathrm{Gal}(\hat{L}^n/\hat{K}). \tag{6.46}$$

So, $\hat{L}^n/\hat{K}$ *is an Abelian extension with degree* $(q-1)q$.

Proof. Let $f(X) = \pi X + X^q$ and take $h_n(X)$ and α_0 as in the Lemma 6.1.2. We know that $h_n(X)$ is irreducible in $\hat{K}[X]$. Also its degree is $(q-1)q^n$. So,

$$(q-1)q^n = [\hat{K}(\alpha_0) : \hat{K}] \leq [\hat{L}^n : \hat{K}]. \tag{6.47}$$

Take any σ in $\mathrm{Gal}(\hat{L}^n/\hat{K})$. Recall that σ is continuous and $F_f(X,Y)$ and $[a]_f(X)$ are power series in $\mathcal{O}_{\hat{K}}[[X]]$ for $a \in \mathcal{O}_k$. Then the following hold:

$$\sigma(F_f(\alpha,\beta)) = F_f(\sigma(\alpha),\sigma(\beta)) = \sigma(\alpha) +_f \sigma(\beta), \tag{6.48}$$

$$\sigma(a \cdot_f \alpha) = \sigma([a]_f(\alpha)) = [a]_f(\sigma(\alpha)) = a \cdot_f \sigma(\alpha) \tag{6.49}$$

for α, $\beta \in W_f^n$ and $a \in \mathcal{O}_k$. Observe that, by the equation 6.49, $\sigma(\alpha) \in W_f^n$ for $\alpha \in W_f^n$, since $W_f^n = \{\alpha \in \mathfrak{m}_f \mid \mathfrak{p}^{n+1} \cdot_f \alpha = 0\}$. So σ induces an automorphism σ' of W_f^n and the following homomorphism can be defined:

$$\mathrm{Gal}(\hat{L}^n/\hat{K}) \to \mathrm{Aut}(W_f^n), \tag{6.50}$$

$$\sigma \mapsto \sigma'. \tag{6.51}$$

This homomorphism is injective because any element of $\mathrm{Gal}(\hat{L}^n/\hat{K})$ is defined by its actions on the elements of W_f^n. By Theorem 6.1.4, $|\mathrm{Aut}(W_f^n)| = [\mathcal{U}_0 : \mathcal{U}_{n+1}] = (q-1)q^n$, so

$$[\hat{L}^n : \hat{K}] \leq (q-1)q^n. \tag{6.52}$$

Combining this with the equation 4.93, we get

$$\hat{L}^n = \hat{K}(\alpha_0),\ \ [\hat{L}^n : \hat{K}] = (q-1)q^n,\ \ \mathrm{Gal}(\hat{L}^n/\hat{K}) \cong \mathrm{Aut}(W_f^n). \tag{6.53}$$

Set γ^n to be the composition of the mappings below:

$$\mathcal{U}_k \to \mathcal{U}_k/\mathcal{U}_{n+1} \cong \mathrm{Aut}(W_f^n) \cong \mathrm{Gal}(\hat{L}^n/\hat{K}). \tag{6.54}$$

Note that $\gamma^n(u)(\alpha) = [u]_f(\alpha) = u \cdot_f \alpha$ for all $u \in \mathcal{U}_k,\ \alpha \in W_f^n$.

Now, let f' be another power series in $\mathcal{F}$ and $\theta(X)$ the power series as in Theorem 5.2.3. Recall that $W_{f'}^n = \theta(W_f^n)$. Let $\alpha' \in W_{f'}^n$ and $\alpha' = \theta(\alpha)$, where $\alpha \in W_f^n$. Then the following holds:

$$u \cdot_{f'} \alpha' = [u]_{f'}(\alpha') = \theta \circ [u]_f \circ \theta^{-1}(\theta(\alpha)) = \theta([u]_f(\alpha)) = \theta(\gamma^n(u)(\alpha)). \tag{6.55}$$

where $u \in \mathcal{U}_k$. On the other hand, recall that $\theta(X) \in \mathcal{O}_{\hat{K}}[[X]]$ and $\gamma^n(u) \in \mathrm{Gal}(\hat{L}^n/\hat{K})$. So, by the continuity of automorphisms, we have the following for $f' \in \mathcal{F}$, $\alpha' \in W_{f'}^n$:

$$u \cdot_{f'} \alpha' = \theta(\gamma^n(u)(\alpha)) = \gamma^n(u)(\theta(\alpha)) = \gamma^n(u)(\alpha'). \tag{6.56}$$

□

Let $\hat{L}$ be the union of $\hat{L}^n$'s for $n \geq -1$. So $\hat{L} = \hat{K}(W_f)$ for any $f \in \mathcal{F}$.

Theorem 6.2.3. *$\hat{L}/\hat{K}$ is an Abelian extension and there exists a homoemorphism*

$$\gamma : \mathcal{U}_k \cong \mathrm{Gal}(\hat{L}/\hat{K}). \tag{6.57}$$

Moreover, this homeomorphism induces $\gamma^n : \mathcal{U}_k \to \mathrm{Gal}(\hat{L}^n/\hat{K})$ for every $n \geq 0$.

Proof. The following diagram commutes:

$$\begin{tikzcd}
\mathcal{U}/\mathcal{U}_{n+2} \arrow[r, "\sim"] \arrow[d, "\text{natural projection}"] & \mathrm{Gal}(\hat{L}^{n+1}/\hat{K}) \arrow[d, "\text{restriction}"] \\
\mathcal{U}/\mathcal{U}_{n+1} \arrow[r, "\sim"] & \mathrm{Gal}(\hat{L}^n/\hat{K})
\end{tikzcd} \tag{6.58}$$

So, we see that

$$\gamma : \mathcal{U}_k = \varprojlim \mathcal{U}_k/\mathcal{U}_{n+1} \cong \varprojlim \operatorname{Gal}(\hat{L}^n/\hat{K}) = \operatorname{Gal}(\hat{L}/\hat{K}), \tag{6.59}$$

for $n \geq 0$. □

6.3. THE EXTENSIONS L^n AND $k_\pi^{m,n}$

In this section, we will construct certain Abelian extensions of a local field k (and its finite unramified extension fields) and then study the properties of those Abelian extensions.

Denote the valuation ring of the unramified extension k_{ur}^m of degree m over k by $\mathcal{O}_k^m$ for $m \geq 1$. If we take a prime element $\pi \in k_{ur}^m$, we know that it is also prime in $K = k_{ur}$ and $\hat{K}$. Let $\mathcal{F}_\pi$ be the set of power series in $\mathcal{O}_{\hat{K}}[[X]]$ as defined in 5.17. We define

$$\mathcal{F}_\pi^m = \mathcal{F}_\pi \cap \mathcal{O}_k^m[[X]]. \tag{6.60}$$

Then $f(X) = \pi X + X^q \in \mathcal{F}_\pi^m$. We put

$$\mathcal{F}^m := \text{the union of } \mathcal{F}_\pi^m \text{ for } \pi \in k_{ur}^m, \tag{6.61}$$

$$\mathcal{F}^\infty = \text{the union of } \mathcal{F}^m \text{ for } m \geq 1. \tag{6.62}$$

Lemma 6.3.1. *For $m \geq 1$ and $n \geq 0$:*

(i) If $f \in \mathcal{F}_\pi^m$, then $k_{ur}^m(W_f^n)$ is independent of f in $\mathcal{F}_\pi^m$.

(ii) If $f \in \mathcal{F}^\infty$, then $K(W_f^n)$ is independent of f in $\mathcal{F}^\infty$.

Proof. (i) Let $f(X) = \pi X + X^q$, where $\pi \in k_{ur}^m$ and $f' \in \mathcal{F}_\pi^m$. If we put $\pi_1 = \pi$ and $\eta = \xi = 1$ as in 5.40, then $\theta(X) \in \mathcal{O}_k^m[[X]]$. Recall that $k_{ur}^m(W_f^n)$ is finite Galois by 6.1.2. So, it is complete. Then, similar to Lemma 6.2.1,

$$W_{f'}^n = \theta(W_f^n) \subseteq k_{ur}^m(W_f^n). \tag{6.63}$$

This implies

$$k_{ur}^{m}(W_{f'}^{n}) \subseteq k_{ur}^{m}(W_{f}^{n}). \tag{6.64}$$

Since $\theta(X)^{-1} \in \mathcal{O}_k^m[[X]]$, we also have $k_{ur}^{m}(W_{f}^{n}) \subseteq k_{ur}^{m}(W_{f'}^{n})$. So $k_{ur}^{m}(W_{f}^{n}) = k_{ur}^{m}(W_{f'}^{n})$ for any $f' \in \mathcal{F}_{\pi}^{m}$.

(ii) Let $f \in \mathcal{F}^{\infty}$. So $f \in \mathcal{F}_{\pi}^{m}$ for some $m \geq 1$ and $\pi \in k_{ur}^{m}$. Put $E = K(W_f^n) = Kk_{ur}^{m}(W_f^n)$. Recall that $k_{ur}^{m}(W_f^n)/k_{ur}^{m}$ is finite Galois. Then E/K is a finite Galois. By Lemma 3.6.1,

$$\widehat{E} = E\widehat{K} = \widehat{K}(W_f^n) = \widehat{L}^n, \;\; K = E \cap \widehat{K}. \tag{6.65}$$

Now we take another power series $f' \in \mathcal{F}^{\infty}$. Put $E' = K(W_{f'}^{n})$. Then E'/K is also a finite Galois extension and $\widehat{E}' = \widehat{L}^n$ since $\widehat{K}(W_f^n) = \widehat{K}(W_{f'}^n)$. Let $M = EE'$. Then again by Lemma 3.6.1,

$$K(W_{f'}^{n}) = E' = M \cap \widehat{E}' = M \cap \widehat{L}^n = M \cap \widehat{E} = E = K(W_f^n). \tag{6.66}$$

So we proved the theorem. □

Since $k_{ur}^{m}(W_f^n)$ and $K(W_f^n)$ are independnt of f, the following extensions are well-defined:

$$k_{\pi}^{m,n} = k_{ur}^{m}(W_f^n), \;\; f \in \mathcal{F}_{\pi}^{m}, \;\; n \geq -1, \tag{6.67}$$

$$L^n = K(W_f^n), \;\; f \in \mathcal{F}^{\infty}, \;\; n \geq -1. \tag{6.68}$$

Theorem 6.3.2. *Let $m \geq 1$, $n \geq 0$, and π a prime element in k_{ur}^{m}. Then the following hold: The field $\widehat{L}^n$ is the closure of L^n in k^{alg}. Also,*

$$\widehat{L}^n = \widehat{K}L^n, \;\; K = \widehat{K} \cap L^n, \;\; \mathrm{Gal}(\widehat{L}^n/\widehat{K}) \cong \mathrm{Gal}(L^n/K). \tag{6.69}$$

The field L^n is equal to $Kk_{\pi}^{m,n}$, $k_{ur}^{m} = K \cap k_{\pi}^{m,n}$ and $k_{\pi}^{m,n}$ is a maximal totally ramified extension over k_{ur}^{m} in L^n and

$$\mathrm{Gal}(L^n/k_{ur}^{m}) = \mathrm{Gal}(L^n/k_{\pi}^{m,n}) \times \mathrm{Gal}(L^n/K) \cong \mathrm{Gal}(K/k_{ur}^{m}) \times \mathrm{Gal}(k_{\pi}^{m,n}/k_{ur}^{m}). \tag{6.70}$$

$$\begin{tikzcd}
& Kk_{\pi}^{m,n} = L^n \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & k_{\pi}^{m,n} \arrow[dl, dash] \\
& K \cap k_{\pi}^{m,n} = k_{ur}^{m} &
\end{tikzcd} \tag{6.71}$$

The field extensions L^n/k, L^n/K, $k_{\pi}^{m,n}/k$ and $k_{\pi}^{m,n}/k_{ur}^{m}$ are Abelian and

$$[L^n : K] = [k_{\pi}^{m,n} : k_{ur}^{m}] = (q-1)q^n, \;\; [k_{\pi}^{m,n} : k] = m(q-1)q^n. \tag{6.72}$$

Proof. We know that L^n/K and $k_{\pi}^{m,n}/k_{ur}^{m}$ are finite Galois extensions, $\widehat{L}^n = \widehat{K}L^n$ and $K = \widehat{K} \cap L^n$ by Lemma 6.3.1. This implies $\mathrm{Gal}(\widehat{L}^n/\widehat{K}) \cong \mathrm{Gal}(L^n/K)$. Since we know $[\widehat{L}^n : \widehat{K}] = (q-1)q^n$ by the equation 6.53, $[L^n : K] = (q-1)q^n$.

Since $L^n = Kk_{\pi}^{m,n}$ and $k_{ur}^{m} \subseteq K \cap k_{\pi}^{m,n} \subseteq k_{\pi}^{m,n}$, we see that

$$(q-1)q^n = [L^n : K] = [k_{\pi}^{m,n} : K \cap k_{\pi}^{m,n}] \leq [k_{\pi}^{m,n} : k_{ur}^{m}]. \tag{6.73}$$

Let $f(X) = \pi X + X^q$, where π a prime element of k_{ur}^{m}, h_n and α_0 as in Lemma 6.1.2. So,

$$W_f^n = \mathcal{O}_k \cdot_f \alpha_0 = \{[a]_f(\alpha_0) | a \in \mathcal{O}_k\}. \tag{6.74}$$

Since $f(X) \in \mathcal{O}_k^m[[X]]$, then so is $[a]_f$. Hence

$$W_f^n \subseteq k_{ur}^{m}(\alpha_0). \tag{6.75}$$

We know $\alpha_0 \in W_f^n$. This implies that

$$k_{\pi}^{m,n} = k_{ur}^{m}(W_f^n) = k_{ur}^{m}(\alpha_0). \tag{6.76}$$

By Lemma 6.1.3:

$$(q-1)q^n = [k_{\pi}^{m,n} : k_{ur}^{m}] = [k_{ur}^{m}(\alpha_0) : k_{ur}^{m}]. \tag{6.77}$$

In the view of the inequality 6.73, we get $k_{ur}^{m} = K \cap k_{\pi}^{m,n}$ and this means that $k_{\pi}^{m,n}$ is a maximal totally ramified extension over k_{ur}^{m} in L^n (recall Definition 3.7.2). Now we have

$$\mathrm{Gal}(\widehat{L}^n/\widehat{K}) \cong \mathrm{Gal}(L^n/K) \cong \mathrm{Gal}(k_{\pi}^{m,n}/k_{ur}^{m}), \tag{6.78}$$

the extensions L^n/K and $k_\pi^{m,n}/k_{ur}^m$ are Abelian. Take $m = 1$ as a special case. We know that $k_\pi^{1,n}/k$ is Abelian. Since L^n is the compositum of K and $k_\pi^{1,n}$ and K/k is Abelian, L^n/k is also Abelian. Then it immediately follows that $k_\pi^{m,n}/k$ is Abelian. The claims about the extension degrees are obvious. □

Consider the isomorphism in 6.78. The maps between Galois groups are obtained using restrictions (e.g., we restrict $\hat{L}^n$ to L^n). So in the view of Theorem 6.2.2, we can define the following maps similarly:

$$\gamma^n : \mathcal{U}_k \to \mathrm{Gal}(L^n/K) \tag{6.79}$$

for $n \geq 0$. For each $f \in \mathcal{F}^\infty$, $u \in \mathcal{U}_k$ and $\alpha \in W_f^n$, this map has the following form:

$$\gamma^n(u)(\alpha) = [u]_f(\alpha), \tag{6.80}$$

and also it induces the following isomorphism:

$$\mathcal{U}_k/\mathcal{U}_{n+1} \cong \mathrm{Gal}(L^n/K). \tag{6.81}$$

Take a prime element $\pi \in k_{ur}^m$. Then we can define the following map:

$$\gamma_\pi^n : \mathcal{U}_k \to \mathrm{Gal}(k_\pi^{m,n}/k_{ur}^m) \tag{6.82}$$

for $m \geq 1$. Similarly, for each $f \in \mathcal{F}_\pi^m$, $u \in \mathcal{U}_k$ and $\alpha \in W_f^n$, this map has the following form:

$$\gamma_\pi^n(u)(\alpha) = [u]_f(\alpha), \tag{6.83}$$

and also it induces the following isomorphism:

$$\mathcal{U}_k/\mathcal{U}_{n+1} \cong \mathrm{Gal}(k_\pi^{m,n}/k_{ur}^m). \tag{6.84}$$

Corollary 6.3.2.1. *Let $0 \leq t \leq n$. The isomorphism $\mathcal{U}_k/\mathcal{U}_{n+1} \cong \mathrm{Gal}(k_\pi^{m,n}/k_{ur}^m)$ induces the following map:*

$$\mathcal{U}_{t+1}/\mathcal{U}_{n+1} \cong \gamma_\pi^n(\mathcal{U}_{t+1}) = \mathrm{Gal}(k_\pi^{m,n}/k_\pi^{m,t}). \tag{6.85}$$

Proof. For $u \in \mathcal{U}_k$, $\gamma_\pi^n(u)|_{k_\pi^{m,t}} = \gamma_\pi^t(u)$ (Recall that $k_\pi^{m,t} \subseteq k_\pi^{m,n}$). So, we have the following equivalences:

$$u \in \mathcal{U}_{t+1} \iff \gamma_\pi^t(u) = 1 \iff \gamma_\pi^n(u)|_{k_\pi^{m,t}} = 1 \iff \gamma_\pi^n(u) \in \mathrm{Gal}(k_\pi^{m,n}/k_\pi^{m,t}). \qquad (6.86)$$

So we see that $\mathcal{U}_{t+1}/\mathcal{U}_{n+1} \cong \gamma_\pi^n(\mathcal{U}_{t+1}) = \mathrm{Gal}(k_\pi^{m,n}/k_\pi^{m,t})$. □

Theorem 6.3.3. *Let π be a prime in k_{ur}^m, $m \geq 1$ and $n \geq 0$. Then the following hold:*

(i) The extension $k_\pi^{m,n}/k_{ur}^m$ is a finite Abelian extension and also totally ramified. In additon, $\pi \in N(k_\pi^{m,n}/k_{ur}^m)$.

(ii) Let $f \in \mathcal{F}_\pi^m$ and $\alpha_0 \in W_f^n$, $\alpha_0 \notin W_f^{n-1}$. Then α_0 is a prime in $k_\pi^{m,n}$ and also $k_\pi^{m,n} = k_{ur}^m(\alpha_0)$ and $\mathcal{O}^{m,n} = \mathcal{O}^m[\alpha_0]$, where $\mathcal{O}^{m,n}$ and $\mathcal{O}^m$ are the valuation rings of $k_\pi^{m,n}$ and k_{ur}^m, respectively.

Proof. (i) We know that $K \cap k_\pi^{m,n} = k_{ur}^m$, so $k_\pi^{m,n}/k_{ur}^m$ is totally ramified. Previously we proved that $\varphi^n(\pi) \in N(k_\pi^{m,n}/k_{ur}^m)$ and $k_\pi^{m,n}/k$ is Abelian. Since it is Abelian, we can extend the automorphism φ to an automorphism $\widehat{\varphi}$ in $k_\pi^{m,n}/k$. Consider the following equalities:

$$\widehat{\varphi}(\sigma_1(x) \cdots \sigma_{(q-1)q^n}(x)) = \sigma_1(\widehat{\varphi}(x)) \cdots \sigma_{(q-1)q^n}(\widehat{\varphi}(x)). \qquad (6.87)$$

where $x \in k_\pi^{m,n}$. This implies that $\widehat{\varphi}(N(k_\pi^{m,n}/k_{ur}^m)) = \varphi(N(k_\pi^{m,n}/k_{ur}^m)) = N(k_\pi^{m,n}/k_{ur}^m)$. So $\pi \in N(k_\pi^{m,n}/k_{ur}^m)$.

(ii) Let $f(X) = \pi X + X^q$ and f' any power series in $\mathcal{F}_\pi^m$. Take $\alpha' \in W_{f'}^n \backslash W_{f'}^{n-1}$. Put $\alpha_0 = \theta^{-1}(\alpha')$, where $\theta(X)$ is as in 5.40. Since $\theta(X)$ induces an isomorphism between $W_{f'}^n$ and W_f^n, we see that $\alpha_0 \in W_f^n \backslash W_f^{n-1}$. So, by Lemma 6.1.2, $h_n(\alpha_0) = 0$ and also $\varphi^n(\pi) = N(-\alpha_0)$. Since $\varphi^n(\pi)$ is a prime in k_{ur}^m and $k_\pi^{m,n}/k_{ur}^m$ is a totally ramified extension, α_0 is a prime in $k_\pi^{m,n}$ (recall the equation 3.55). We know that $\theta(X) \in \mathcal{O}_K^m[[X]]$ and $\theta(X) \equiv X \bmod \deg 2$. So $\theta(\alpha_0) = \alpha'$ is a prime in $k_\pi^{m,n}$ (consider the expansion of $\theta(\alpha_0)$). Then by Theorem 3.9.2, $\mathcal{O}^{m,n} = \mathcal{O}^m[\alpha']$ and $k_\pi^{m,n} = k_{ur}^m(\alpha')$. □

Corollary 6.3.3.1. *Let $f \in \mathcal{F}_\pi^m$ and $\alpha \in W_f^n \backslash W_f^{n-1}$. Then the following hold:*

(i) The complete set of conjugates of α over k_{ur}^m is

$$C = \{\beta \mid \beta \in W_f^n \backslash W_f^{n-1}\}. \qquad (6.88)$$

(ii) If $0 \le i \le n$*, then the complete set of conjugates of* α *over* $k_\pi^{m,i}$ *is*

$$\alpha +_f W_f^{n-i-1} = \{\alpha +_f \beta \mid \beta \in W_f^{n-i-1}\}. \tag{6.89}$$

Proof. (i) We know $k_\pi^{m,n} = k_{ur}^{m}(\alpha)$ by Theorem 6.3.3. By the isomorphism in 6.84, all conjugates of α are given by the elements $u \cdot_f \alpha$, where $u \in \mathcal{U}_k$. In the view of the fact that $W_f^n = \mathcal{O}_k \cdot_f \alpha$ and $W_f^{n-1} = \mathfrak{p}_k \cdot_f \alpha$, hence the corollary is proved (recall that $\mathcal{U}_k = \mathcal{O}_k \backslash \mathfrak{p}_k$).
(ii) Consider the isomorphism in 6.85. By this isomorphism, the complete set of conjugates of α over $k_\pi^{m,i}$ is given by the set

$$\{u \cdot_f \alpha \mid u \in \mathcal{U}_{i+1}\}, \tag{6.90}$$

which is also equal to

$$(1 + \mathfrak{p}^{i+1}) \cdot_f \alpha = \alpha +_f (\mathfrak{p}^{i+1} \cdot_f \alpha). \tag{6.91}$$

As $\mathfrak{p}^{i+1} \cdot_f \alpha = W_f^{n-i-1}$, the result follows. □

Example 15. Consider the Example 14. Let:

$$k = \mathbb{Q}_p,\ \pi = p,\ f(X) = (1+X)^p - 1 \in \mathcal{F}_p^1,\ F_f(X,Y) = (1+X)(1+Y) - 1. \tag{6.92}$$

We also showed that $[a]_f = (1+X)^a - 1, a \in \mathbb{Z}_p$. Since $[p^{n+1}]_f(X) = (1+X)^{p^{n+1}} - 1$,

$$W_f^n = \{\alpha - 1 \mid \alpha^{p^{n+1}} = 1\}. \tag{6.93}$$

So $k_p^{1,n} = \mathbb{Q}_p(W_f^n)$ is the cyclotomic field of p^{n+1}th roots of unity over $\mathbb{Q}_p = k_{ur}^1$. Let $u \in \mathcal{U}_{\mathbb{Q}_p}$ and $\beta = \alpha - 1 \in W_f^n$. Then,

$$\gamma_p^n(u)(\beta) = [u]_f(\beta) = (1+\beta)^u - 1. \tag{6.94}$$

We also have the following isomorphisms:

$$\mathcal{U}_{\mathbb{Q}_p}/\mathcal{U}_{n+1} \cong \mathbb{Z}_p^\times/(1 + p^{n+1}\mathbb{Z}_p) \cong \mathrm{Gal}(\mathbb{Q}_p(W_f^n)/\mathbb{Q}_p). \tag{6.95}$$

6.4. ABELIAN EXTENSIONS L AND k_{π} OVER k

Recall that $W_f^{n-1} \subseteq W_f^n$, $f \in \mathcal{F}$. So for a prime $\pi \in k_{ur}^m$ and $m \geq 1$, we have the following:

$$k_{ur}^{m} = k_{ur}^{m,-1} \subseteq k_{ur}^{m,0} \subseteq \cdots \subseteq k_{ur}^{m,n} \subseteq k^{alg}, \tag{6.96}$$

$$k_{ur} = K = L^{-1} \subseteq L^{0} \subseteq L^{1} \subseteq \cdots \subseteq L^{n} \subseteq k^{alg}. \tag{6.97}$$

Define

$$k_{\pi}^{m,\infty} := \bigcup_{n \geq -1} k_{\pi}^{m,n}, \tag{6.98}$$

$$L := \bigcup_{n \geq -1}^{\infty} L^{n}. \tag{6.99}$$

Then we have

$$k_{\pi}^{m,\infty} = k_{ur}^{m}(W_f^n) \tag{6.100}$$

for $f \in \mathcal{F}_{\pi}^{m}$,

$$L = k_{ur}(W_f) \tag{6.101}$$

for $f \in \mathcal{F}^{\infty}$. In the view of the previous theorems in this chapter, we can make the following series of observations:

(i) Since L^n/k is Abelian for $n \geq -1$, so is L/k.

(ii) According to Theorem 6.3.2), we have:

$$L = k_{ur} k_{\pi}^{m,\infty}, \;\; k_{ur}^{m} = k_{ur} \cap k_{\pi}^{m,\infty}. \tag{6.102}$$

(iii) The extension $k_{\pi}^{m,\infty}/k_{ur}^{m}$ is a maximal totally ramified extension over k_{ur}^{m} in L.

(iv) If we consider (ii),

$$\mathrm{Gal}(L/k_{ur}^{m}) = \mathrm{Gal}(L/k_{\pi}^{m,\infty}) \times \mathrm{Gal}(L/k_{ur}) \cong \mathrm{Gal}(k_{ur}/k_{ur}^{m}) \times \mathrm{Gal}(k_{\pi}^{m,\infty}/k_{ur}^{m}). \tag{6.103}$$

We state the following theorem (its proof is very similar to Theorem 6.2.3):

Theorem 6.4.1. *There exist homeomorphisms*

$$\gamma : \mathcal{U}_k \cong \mathrm{Gal}(L/k_{ur}), \tag{6.104}$$

$$\gamma_\pi : \mathcal{U}_k \cong \mathrm{Gal}(k_\pi^{m,\infty}/k_{ur}^m), \tag{6.105}$$

which also induce the homomorphisms γ^n and γ_π^n in 6.79 and 6.82, respectively.

Now take $m = 1, \pi \in k = k_\pi^1$ and denote $k_\pi^{1,\infty}$ by k_π. Then we have the following:

$$L = k_{ur}k_\pi, \;\; k = k_{ur} \cap k_\pi. \tag{6.106}$$

The extension k_π is a maximal totally ramifed over k in L and

$$\mathrm{Gal}(L/k) = \mathrm{Gal}(L/k_\pi) \times \mathrm{Gal}(L/k_{ur}) \cong \mathrm{Gal}(k_{ur}/k) \times \mathrm{Gal}(k_\pi/k). \tag{6.107}$$

$$\begin{tikzcd}
 & k_{ur}k_\pi = L \arrow[dl, dash] \arrow[dr, dash] & \\
k_{ur} \arrow[dr, dash] & & k_\pi \arrow[dl, dash] \\
 & k_{ur} \cap k_\pi = k &
\end{tikzcd} \tag{6.108}$$

Also we have:

$$\gamma_\pi : \mathcal{U}_k \cong \mathrm{Gal}(k_\pi/k), \tag{6.109}$$

which is a homeomorphism.

Lemma 6.4.2. *Let $g = h \circ [\pi]_f$, where $g, h \in \mathcal{O}_k[[X]]$, $\pi \in k$ and $f \in \mathcal{F}_\pi^1$. Then for $n \geq 0$,*

$$g \equiv 0 \mod \mathfrak{p}_k^n \iff h \equiv 0 \mod \mathfrak{p}_k^n. \tag{6.110}$$

Proof. ($\Leftarrow$) If we assume $h \equiv 0 \mod \mathfrak{p}_k^n$, then the coefficients in the composition $h \circ [\pi]_f$ is equivalent to 0 mod $\mathfrak{p}_k^n$. ($\Rightarrow$) Use induction on n. The proposition is true for $n = 0$, since $h \in \mathcal{O}_k[[X]]$. So assume $g \equiv 0 \mod \mathfrak{p}_k^n$, $n \geq 1$. This implies that $g \equiv 0 \mod \mathfrak{p}_k^{n-1}$ and $g = \pi^{n-1}g_1$, where $g_1 \in \mathcal{O}_k[[X]]$. By the induction assumption, $h \equiv 0 \mod \mathfrak{p}_k^{n-1}$, $h = \pi^{n-1}h_1$, where $h_1 \in \mathcal{O}_k[[X]]$. So $g_1 = h_1 \circ [\pi]_f$. On the other hand, since $g \equiv 0 \mod \mathfrak{p}_k^n$, this implies that $g_1 \equiv 0 \bmod \mathfrak{p}_k$. Observe that $[\pi]_f = f(X) \equiv X^q \bmod \mathfrak{p}_k$. So we have

$$h_1(X^q) = h_1 \circ [\pi]_f = g_1 \equiv 0 \bmod \mathfrak{p}_k. \tag{6.111}$$

This implies that $h_1(X) \equiv 0 \bmod \mathfrak{p}_k$. Finally $h = \pi^{n-1}h_1 \equiv 0 \bmod \mathfrak{p}_k^n$ which completes the proof. □

Remark. Note that the lemma holds for $h, g \in \mathcal{O}_{\hat{K}}[[X]]$, where $K = k_{ur}$. Also observe that $g \equiv 0 \mod \mathfrak{p}_k^n \iff h \equiv 0 \mod \mathfrak{p}_k^n$ implies $g = 0 \iff h = 0$.

Now we fix a prime π in k and $m \geq 1$. Let $k' = k_{ur}^m$ and $\varphi' = \varphi_{k'}$. Recall that $\varphi' = \varphi_k^m$. Let π' be a prime in k'. We know that π is also prime in k', so we have $\pi' = \pi\alpha$, where $\alpha \in \mathcal{U}_{k'}$. Let

$$u = N_{k'/k}(\alpha) \in \mathcal{U}_k. \tag{6.112}$$

Lemma 6.4.3. *Let $f \in \mathcal{F}_\pi^1$, $f' \in \mathcal{F}_{\pi'}^m$ and $\theta(X)$ as in 5.40. Then we have:*

$$\theta^{\varphi'} = \theta \circ [u]_f. \tag{6.113}$$

Proof. Define g_{m-1} and g'_{m-1} for f and f', respectively, as in Lemma 6.1.1. Then the following holds:

$$g'_{m-1} \circ \theta = \theta^{\varphi'} \circ g_{m-1}. \tag{6.114}$$

Put $a = N_{k'/k}(\pi') = \pi^m u$. Then $g'_{m-1} \equiv aX$ mod deg 2. Also, since $f' \in \mathcal{F}_{\pi'}^m$, we have $f'^{\varphi'} = f'$. By the equation 6.15,

$$f' \circ g'_{m-1} = g'^{\varphi}_{m-1} \circ f'. \tag{6.115}$$

In the view of the uniqueness part of the equation 5.29, we conclude that

$$g'_{m-1} = [a]_{f'} = [a]_f^{\theta}. \tag{6.116}$$

This implies

$$g'_{m-1} \circ \theta = \theta \circ [a]_f = \theta \circ [u]_f \circ [\pi^m]_f. \tag{6.117}$$

Since $f \in \mathcal{F}_\pi^1$, we have $f = [\pi]_f$ and $g_{m-1} = [\pi^m]_f$. So,

$$\theta^{\varphi'} \circ [\pi^m]_f = \theta \circ [u]_f \circ [\pi^m]_f. \tag{6.118}$$

Since $\theta^{\varphi'} \circ [\pi^m]_f = \theta \circ [u]_f \circ [\pi^m]_f = (\theta^{\varphi'} - (\theta \circ [u]_f)) \circ [\pi^m]_f$, by Lemma 6.4.2,

$$\theta^{\varphi'} = \theta \circ [u]_f. \tag{6.119}$$

□

Theorem 6.4.4. *Let π and π' be primes in k such that $\pi' = \pi u$, where $u \in \mathcal{U}_{n+1}$. Then $k_\pi^n = k_{\pi'}^n$.*

Proof. Apply Lemma 6.4.3 with $m = 1$, $\varphi = \varphi'$ and $\pi' = u\pi$. Take $\alpha' \in W_{f'}^n$. Then $\alpha' = \theta(\alpha)$, where $\alpha \in W_f^n$. By the preceding lemma,

$$\theta^{\varphi}(\alpha) = \theta([u]_f(\alpha)). \tag{6.120}$$

Since $u \in \mathcal{U}_{n+1}$, $[u]_f$ is the identity automorphism, so $\theta^{\varphi}(\alpha) = \theta(\alpha)$. We know that $k_{ur} \cap k_\pi^n = k$, so we can extend φ to $L^n = k_{ur}k_\pi^n$ over k_π^n. Call that automorphism φ^*. Since $\alpha \in W_f^n \subseteq k_\pi^n$, we see that

$$\theta(\alpha)^{\varphi^*} = \theta^{\varphi^*}(\alpha) = \theta^{\varphi}(\alpha) = \theta(\alpha), \tag{6.121}$$

where $\alpha' = \theta(\alpha) \in L^n = k_{ur}(W_{f'}^n)$. So $\alpha' \in k_\pi^n$. Then we obtain

$$k_{\pi'}^n = k(W_{f'}^n) \subseteq k_\pi^n. \tag{6.122}$$

Since $u^{-1} \in \mathcal{U}_{n+1}$ and $\pi = u^{-1}\pi'$, similarly we obtain $k_\pi^n \subseteq k_{\pi'}^n$. Hence $k_{\pi'}^n = k_\pi^n$. □

For brevity, the following theorem will be provided without proof. Its proof is based on the norm operator of Coleman. Refer to [8] for the complete proof.

Theorem 6.4.5. *Let π be a prime in k. Then*

$$N(k_\pi^n/k) = <\pi> \times \mathcal{U}_{n+1},\ n \geq -1, \tag{6.123}$$

and

$$N(k_\pi/k) = <\pi> . \tag{6.124}$$

If F is totally ramified over k, containing k_π, then

$$N(F/k) = <\pi> . \tag{6.125}$$

6.5. HOMOMORPHISM ρ_k AND PROOF OF $L_k = k^{ab}$

Recall that $L = k_{ur}(W_f)$ and L/k is an Abelian extension. So

$$k \subseteq L \subseteq k^{ab}. \tag{6.126}$$

We denote L by L_k when k is varied. Since we know that $\text{Gal}(L/k_\pi) \cong \text{Gal}(k_{ur}/k)$ for $\pi \in k$, there exists a unique automorphism $\lambda_\pi \in \text{Gal}(L/k)$ such that

$$\lambda_\pi|_{k_{ur}} = \varphi_k \text{ and } \lambda_\pi|_{k_\pi} = 1. \tag{6.127}$$

We showed that $<\varphi_k>$ is dense in $\text{Gal}(k_{ur}/k)$, so $<\lambda_\pi>$ is dense in $\text{Gal}(L/k_\pi)$ which implies the fixed field of λ_π in L is k_π.

Now we fix a prime $\pi_0 \in k$. We know that every $x \in k^\times$ can be uniquely written as $x = \pi_0^m u$, where $m \in \mathbb{Z}$, $u \in \mathcal{U}_k$, and $m = v(x)$. For such an x, we define

$$\rho : k^\times \to \text{Gal}(L/k), \tag{6.128}$$

$$x \mapsto \lambda_{\pi_0}^m \circ \gamma(u^{-1})(x), \tag{6.129}$$

where $\gamma : \mathcal{U}_k \cong \text{Gal}(L/k_{ur})$ is the isomorphism in 6.104 ($\text{Gal}(L/k) = \text{Gal}(L/k_\pi) \times \text{Gal}(L/k_{ur})$). It is clear that this is a homomorphism between the Abelian groups $k^\times$ and $\text{Gal}(L/k)$ and by the definitons of the maps, it satisfies the following conditions:

$$\rho(x)|_{k_{ur}} = \lambda_{\pi_0}^m|_{k_{ur}} = \varphi_k^m. \tag{6.130}$$

Lemma 6.5.1. *Let $\pi' \in k'$, where $k' = k_{ur}^m$ for $m \geq 1$. Put $x = N_{k'/k}(\pi')$. Then $\rho(x)$ is the* *unique element* $\xi \in \mathrm{Gal}(L/k)$ *such that*

$$\xi|_{k_{ur}} = \varphi_k^m, \;\; \xi|_{k_{\pi'}^{m,\infty}} = 1. \tag{6.131}$$

Proof. The existence and uniqueness of such an element is guaranteed by the isomorphism given in 6.103. We know that $\rho(x)$ satisfies 6.130, so we only need to prove the following:

$$\rho(x)|_{k_{\pi'}^{m,n}} = 1, \;\; n \geq 1. \tag{6.132}$$

Since k'/k is an unramified extension, $\pi_0 \in k'$. Hence $\pi = \pi_o\varepsilon$, where $\varepsilon \in \mathcal{U}_{k'}$. This implies that

$$x = N_{k'/k}(\pi') = \pi_0^m u, \; u = N_{k'/k}(\varepsilon) \in \mathcal{U}_k. \tag{6.133}$$

Take $f \in \mathcal{F}_{\pi_0}^1$, $f' \in \mathcal{F}_{\pi'}^m$ and let $\theta(X)$ be as in 5.40. By Lemma 6.4.3,

$$\theta^{\varphi'} = \theta \circ [u]_f, \tag{6.134}$$

where φ' is the extension of $\varphi_{k'}$ to $\widehat{K} = \widehat{k_{ur}}$. Let $\alpha' \in W_{f'}^n = \theta(W_f^n)$ and $\alpha' = \theta(\alpha)$, where $\alpha \in W_f^n$. Then by the definition of ρ,

$$\rho(x)(\alpha) = \gamma(u^{-1})(\alpha) = [u^{-1}]_f(\alpha). \tag{6.135}$$

Since $\theta(X) \in \mathcal{O}_{\widehat{K}}[[X]]$ and $\rho(x)$ can be extended to φ' (which means that it acts on $\widehat{K}$ as φ'),

$$\rho(x)(\alpha') = \rho(x)(\theta(\alpha)) = \theta^{\varphi'}(\rho(x)(\alpha)) = \theta \circ [u]_f \circ [u^{-1}]_f(\alpha) = \theta(\alpha) = \alpha'. \tag{6.136}$$

So $\rho(x)|_{k_{\pi'}^{m,n}} = 1$ (Recall $k_{\pi'}^{m,n} = k'(W_{f'}^n)$). □

Theorem 6.5.2. *There exists a unique homomorphism*

$$\rho_k : k^\times \to \mathrm{Gal}(L/k) \tag{6.137}$$

such that $\rho_k(\pi) = \lambda_\pi$ *for every prime* $\pi \in k^\times$.

Proof. Apply Lemma 6.5.1 with $m = 1$ and $\pi = \pi'$. Then $\rho(\pi)$ is the unique element in

$\mathrm{Gal}(L/k)$ satisfying the following conditions:

$$\rho(\pi)|_{k_{ur}} = \varphi_k, \;\; \rho(\pi)|_{k_\pi} = 1. \tag{6.138}$$

So by the equations in 6.127, $\rho(\pi) = \lambda_\pi$. This implies that ρ defined above satisfies the condition mentioned in the theorem. Since the multiplicative group $k^\times$ of k is generated by the primes in k (recall that $\pi = \pi' u$ implies $u = \pi/\pi'$), $\rho = \rho_k$. □

The definition of map ρ_k is actually independent of π_0. To see this, take a prime π in k and let

$$x = \pi^m u, \;\; m = v(x), \;\; u \in \mathcal{U}_k, \;\; x \in k^\times. \tag{6.139}$$

Then we have

$$\rho_k(x) = \rho_k(\pi)^m \circ \rho_k(u) = \lambda_\pi^m \circ \gamma(u^{-1}), \tag{6.140}$$

$$\rho(x)|_{k_{ur}} = \lambda_\pi^m|_{k_{ur}} = \varphi_k^m, \tag{6.141}$$

where $m = v(x)$.

Theorem 6.5.3. *The map ρ_k has the following properties:*

(i) It is injective and continuous in Krull topology of $\mathrm{Gal}(L/k)$ *and v-topology of $k^\times$.*

(ii) The image of ρ_k is dense in $\mathrm{Gal}(L/k)$ *and consists of all elements ξ in* $\mathrm{Gal}(L/k)$ *such that $\xi|_{k_{ur}} = \varphi_k^m$, $m \in \mathbb{Z}$. Also, if $\xi|_{k_{ur}} = \varphi_k$, then there is a unique prime $\pi \in k$ such that $\xi = \rho_k(\pi)$.*

Proof. (i) Assume that $\rho_k(x) = 1$, where $x = \pi_k^m u$. Then $\rho_k(x)|_{k_{ur}} = \varphi_k^m = 1$. Since the order of φ_k is infinite, $m = 0$ and $x = u$. This implies that $\gamma(u^{-1}) = 1$. Since γ is an isomorphism, $u = 1$, which means that $x = 1$. So ρ_k is injective. To prove the continuity of ρ_k, consider a member of the basis of neighborhoods for $\mathrm{Gal}(L/k) : W \times V$, where W and V are open in $\mathrm{Gal}(L/k_\pi)$ and $\mathrm{Gal}(L/k_{ur})$, respectively. Since $pr_2 \circ \rho_k(\mathcal{U}_k)$ is surjective (here pr_2 is the projection map from $\mathrm{Gal}(L/k_\pi) \times \mathrm{Gal}(L/k_{ur})$ to $\mathrm{Gal}(L/k_{ur})$) and $\mathcal{U}_k$ is homeomorphic to $\mathrm{Gal}(L/k_{ur})$, the inverse image of $(\{1\} \times V) \cap (\{1\} \times \mathrm{Gal}(L/k_{ur}))$ under ρ_k is $\mathcal{U}_n^{-1}$ for some $n \geq 0$. On the other hand, the $pr_1 \circ \rho_k(k^\times)$ is $< \lambda_\pi >$. So, the inverse image of $(W \times \{1\}) \cap (\mathrm{Gal}(L/k_\pi) \times \{1\})$ is equal to $\{\pi_k^i | i \in I \subseteq \mathbb{Z}\}$. Hence

$\rho_k^{-1}((W \times V) \cap \rho_k(k^\times))$ is the following open set:

$$\bigcup_{i \in I} \pi_k^i \mathcal{U}_n^{-1}. \tag{6.142}$$

This proves that ρ_k is continuous.

(ii) Since the image of ρ_k is equal to $< \lambda_\pi > \times \operatorname{Gal}(L/k_{ur})$ and $< \lambda_\pi >$ is dense in $\operatorname{Gal}(L/k_\pi)$, the first part is obvious (recall that the closure of a product is the product of the closures). The second part of (ii) is the consequence of the fact that any automorphism $\xi \in \operatorname{Gal}(L/k)$ is completely determined by the automorphisms $\xi|_{k_{ur}}$ and $\xi|_{k_\pi}$. □

Let k'/k be a finite extension of local fields. Now we prove a lemma about the following maps:

$$\rho_k : k^\times \to \operatorname{Gal}(L_k/k), \tag{6.143}$$

$$\rho_{k'} : k'^\times \to \operatorname{Gal}(L_{k'}/k'). \tag{6.144}$$

Let $M = L_k \cap L_{k'}$. The extension L_k/k is Abelian, so this means that $\rho_k(x)$ induces an automorphism of M over k for $x \in k^\times$. If we take $x' \in k'^\times$, then $\rho_{k'}(x')$ also induces an automorphism of M over k (as $k \subseteq k'$).

Lemma 6.5.4. *Suppose k'/k is a totally ramified finite extension of local fields. Then the following equality holds:*

$$\rho_{k'}(x')|_M = \rho_k(N_{k'/k}(x'))|_M, \; \textit{for all } x' \in k'^\times. \tag{6.145}$$

Proof. We know that $k'^\times$ is generated by the primes in k', so if we prove the equality 6.145 for a prime $\pi' \in k'$, we prove the lemma. Extend $\rho_{k'}(\pi')$ to an automorphism ξ of k^{alg} and let F denote the fixed field of ξ in k^{alg}. Recall that the fixed field of $\lambda_{\pi'}(= \rho_{k'}(\pi'))$ in $L_{k'}$ is $k'_{\pi'}$. Hence,

$$F \cap L_{k'} = k'_{\pi'}, \; F \cap k'_{ur} = k'. \tag{6.146}$$

This implies F/k' is totally ramified and also $k' \subseteq k'_{\pi'} \subseteq F$. By Theorem 6.4.5, $N(F/k') = < \pi' >$. Observe that $\xi|_{k'_{ur}} = \rho_{k'}(\pi')|_{k'_{ur}} = \varphi_{k'}$ by the equation 6.141. Also, since k'/k is totally ramified, $\varphi_{k'}|_{k_{ur}} = \varphi_k$. So we have the following:

$$\xi|_{k_{ur}} = (\xi|_{k'_{ur}})|_{k_{ur}} = \varphi_{k'}|_{k_{ur}} = \varphi_k. \tag{6.147}$$

Put $\psi = \xi|_{L_k}$. Then clearly $\psi|_{k_{ur}} = \varphi_k$. By Theorem 6.5.3, $\psi = \rho_k(\pi)$ for some $\pi \in k$. Recall that k_π is the fixed field of $\rho_k(\pi)$ in L_k, so $k \subseteq k_\pi \subseteq F$. Considering the fact that F/k' and k'/k are totally ramified, we conclude that F/k is also totally ramified. Then again by Theorem 6.4.5, $N(F/k) = < \pi >$. Since $N(F/k') = < \pi' >$, it is easy to see that $N_{k'/k}(\pi') \in N(F/k)$ (recall that $k \subseteq k' \subseteq k''$ implies $N(k''/k) \subseteq N(k'/k)$). But k'/k is a totally ramified extension, so $N_{k'/k}(\pi')$ is a prime in k. That is,

$$N_{k'/k}(\pi') = \pi. \tag{6.148}$$

Finally,

$$\rho_{k'}(\pi')|_M = \xi|_M = \psi|_M = \rho_k(\pi)|_M = \rho_k(N_{k'/k}(\pi'))|_M. \tag{6.149}$$

□

As a direct consequence, consider the case $k \subseteq k' \subseteq L_k$. Then clearly $k \subseteq k' \subseteq M$. Hence

$$\rho_k(N_{k'/k}(k'^{\times}))|_{k'} = \rho_{k'}(k'^{\times})|_{k'} = 1. \tag{6.150}$$

Now we prove that $L = k^{ab}$. To prove this, the following lemmata will be established first.

Lemma 6.5.5. *Let k be a p-field and k'/k a cyclic extension of degree p over k. Then*

$$N_{k'/k}(k'^{\times}) \neq k^{\times}. \tag{6.151}$$

Proof. Denote the Galois group of k'/k by G and let G_n be the ramification groups of the extension k'/k for $n \geq 0$. By assumption, G is a cyclic group and also of order p, so every G_n is either G or $\{1\}$.

Case 1: Suppose $G_0 = \{1\}$. Then by Theorem 3.10.1, $e_{k'/k} = 1$ and $f_{k'/k} = p$ which implies that k'/k is unramified. In the view of the equation 3.55, $p|v(N_{k'/k}(x'))$ for $x' \in k'^{\times}$. Since the valuations of prime elements are equal to 1 in k, $N_{k'/k}(k'^{\times}) \neq k^{\times}$.

Case 2: Now assume $G_0 = G$. In this case k'/k is totally ramified. Also, $[G_0 : G_1]$ is coprime to p. So there is an integer $s \geq 1$ such that

$$G_0 = G_1 = \dots = G_s, \;\; G_{s+1} = G_{s+1} = \dots = 1. \tag{6.152}$$

Fix a prime $\pi_{k'}$ and take the minimal polynomial $f(X)$ of $\pi_{k'}$ (over k). By Theorem 3.9.3, we know that $\mathcal{D}_{k'/k} = f'(\pi_{k'})\mathcal{O}_{k'}$. Since

$$f'(\pi_{k'}) = \prod_{\xi \in G,\ \xi \neq 1} (\pi_{k'} - \xi(\pi_{k'})) \tag{6.153}$$

and $G_{s+1} = 1$, $v'(\pi_{k'} - \xi(\pi_{k'})) = s + 1$ for all $\xi \neq 1$. This implies that

$$v'(f'(\pi_{k'})) = (p-1)(s+1), \;\; \mathcal{D}_{k'/k} = \mathfrak{p}_{k'}^{(p-1)(s+1)}. \tag{6.154}$$

Let $x' \in \mathcal{U}'_{s+1} = 1 + \mathfrak{p}_{k'}$. Put $x' = 1 + y'$, where $y' \in \mathfrak{p}_{k'}^{s+1}$. We see that

$$N_{k'/k}(x') = \prod_{\xi \in G}(1 + \xi(y')) = 1 + \sum_{\omega} y'^{\omega} + N_{k'/k}(y'), \tag{6.155}$$

where ω runs through all the elements $\xi_1 + \cdots + \xi_m$, $1 \leq m \leq p-1$. Since $|G|$ is prime, the left multiplication by $\rho(\neq 1)$ does not stabilize any element, so $\omega, \rho\omega, \dots, \rho^{p-1}\omega$ are distinct elements. Then we can decompose $\sum_{\omega} y'^{\omega}$ into sums of the following form:

$$\sum_{\xi \in G} y^{\xi\omega} = T_{k'/k}(y^{\omega}). \tag{6.156}$$

Since k'/k is totally ramified and $y' \in \mathfrak{p}_{k'}^{s+1}$,

$$\mathcal{D}_{k'/k} y'^{\omega} \subseteq \mathfrak{p}_{k'}^{(p-1)(s+1)+(s+1)} = \mathfrak{p}_{k'}^{p(s+1)} = \mathfrak{p}_{k}^{s+1}. \tag{6.157}$$

So we have

$$T_{k'/k}(y'^{\omega}) \in T_{k'/k}(\mathfrak{p}_{k'}^{s+1}\mathcal{D}_{k'/k}^{-1}) = \mathfrak{p}_{k'}^{s+1} T_{k'/k}(\mathcal{D}_{k'/k}^{-1}) \subseteq \mathfrak{p}_{k}^{s+1}. \tag{6.158}$$

Observe that $y' \in \mathfrak{p}_{k'}^{s+1}$ implies $N_{k'/k}(y') \in \mathfrak{p}_{k}^{s+1}$ by the equation 3.55. Hence by 6.155,

$$N_{k'/k}(x') \equiv 1 \mathfrak{p}_{k}^{s+1}, \;\; x' \in \mathcal{U}'_{s+1}, \tag{6.159}$$

which implies $N_{k'/k}(\mathcal{U}'_{s+1}) \subseteq \mathcal{U}_{s+1}$. So we can define the following homomorphism using the norm map $N_{k'/k}$:

$$\alpha : \mathcal{U}'/\mathcal{U}'_{s+1} \to \mathcal{U}/\mathcal{U}_{s+1}. \tag{6.160}$$

Since k'/k is totally ramified, $\mathcal{O}_{k'}/\mathfrak{p}_{k'} \cong \mathcal{O}_k/\mathfrak{p}_k = \mathbb{F}_q$. So by 3.46,

$$[\mathcal{U}' : \mathcal{U}'_{s+1}] = [\mathcal{U} : \mathcal{U}_{s+1}] = (q-1)q^s. \tag{6.161}$$

If we take $\varepsilon = \xi(\pi')/\pi'$, where $\pi' \in k'$ and $\xi(\neq 1) \in G$, $v'(\xi(\pi') - \pi') = s+1$ implies that $\varepsilon \in \mathcal{U}'_s \setminus \mathcal{U}'_{s+1}$. But valuations are invariant under automorphisms, so $N_{k'/k}(\varepsilon) = 1$. This means that α is not injective, and as a result of the fact that $[\mathcal{U}' : \mathcal{U}'_{s+1}]$ is finite, it is not surjective. Then $N_{k'/k}(\mathcal{U}') \neq \mathcal{U}$ and consequently $N_{k'/k}(k'^{\times}) \neq k^{\times}$. □

Lemma 6.5.6. *Let k be a p-field and k'/k a cyclic extension of degree p, then $k' \subseteq L$.*

Proof. Assume $k' \nsubseteq L$. So $k' \cap L \neq k'$. Since $[k' : k] = p$, $[k' \cap L : k] \neq p$, and $[k' \cap L : k] \mid p$, so we have the following:

$$k' \cap L = k, \;\; \mathrm{Gal}(k'L/k) \cong \mathrm{Gal}(k'/k) \times \mathrm{Gal}(L/k). \tag{6.162}$$

Let π be a prime in k. Then we know that $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(k_{ur}/k) \times \mathrm{Gal}(k_\pi/k)$. By 6.162,

$$\mathrm{Gal}(k'L/k) \cong \mathrm{Gal}(k'/k){\times}\mathrm{Gal}(k_{ur}/k){\times}\mathrm{Gal}(k_\pi/k) \cong \mathrm{Gal}(k'k_\pi/k){\times}\mathrm{Gal}(k_{ur}/k). \tag{6.163}$$

This implies that $k'k_\pi \cap k_{ur} = k$ which means that $k'k_\pi$ is a totally ramified extension over k, containing k_π. Then by Theorem 6.4.5, $N(k'k_\pi/k) =< \pi >$ and so $\pi \in N(k'/k)$. The the prime elements of k generate field $k^{\times}$. Hence $N(k'/k) = k^{\times}$, which contradicts Lemma 6.5.5. We conclude that $k' \subseteq L$. □

Lemma 6.5.7. *Let p be a prime in $\mathbb{Z}$, k be a field and $\zeta_p \subseteq k$, where ζ_p is a primitive p-th root of unity. Let s be an integer, $s \geq 0$ and there exists a cyclic extension k', which is of degree p^s over k. Also, suppose that $k' \subseteq k''$, where k'' is a cyclic extension of degree p^{s+1} over k. Then ζ_p is the norm of an element of k'.*

Proof. Take a generator σ of $\mathrm{Gal}(k''/k)$. Let $\tau = \sigma^{p^s}$. Then τ is a generator of $\mathrm{Gal}(k''/k')$.

Since $\zeta_p \in k' \subseteq k''$, by Kummer theory ([18], Chapter 14.7), there exists $\alpha \in k''$ such that

$$k'' = k'(\alpha), \;\; \alpha^{\tau-1} = \zeta_p, \tag{6.164}$$

where $\alpha^{\tau-1} = \tau(\alpha)\alpha^{-1}$. Let $\beta = \alpha^{\sigma-1}$. Then we see that

$$\beta^{\tau-1} = (\alpha^{\sigma-1})^{\tau-1} = (\alpha^{\tau-1})^{\sigma-1} = \zeta_p^{\sigma-1} = 1. \tag{6.165}$$

This implies that $\tau(\beta) = \beta$, so $\beta \in k'$. Note that

$$\tau - 1 = \sigma^{p^s} - 1 = (\sigma - 1)\sum_i \sigma^i, \;\; 0 \leq i \leq p^s. \tag{6.166}$$

So, β satisfies the following:

$$N_{k'/k}(\beta) = \beta^{\sum_i \sigma^i} = \alpha^{(\sigma-1)\sum_i \sigma^i} = \alpha^{\tau-1} = \zeta_p, \tag{6.167}$$

where $0 \leq i \leq p^s$. □

Now, after establishing the preceding lemmata, we are ready to prove that $L = k^{ab}$.

(Step 1) We know that $k \subseteq k_{ur} \subseteq k^{ab}$. So we can extend Frobenius automorphism φ_k of k to an automorphism ψ of k^{ab}. Denote the fixed field of ψ in k^{ab} by F_ψ. Then by Lemma 3.7.3 we have the following:

$$F_\psi k_{ur} = k^{ab}, \;\; F_\psi \cap k_{ur} = k, \;\; \mathrm{Gal}(k^{ab}/F_\psi) \cong \mathrm{Gal}(k_{ur}/k). \tag{6.168}$$

Put $\sigma = \psi|_L$. Then we see that $\sigma|_{k_{ur}} = \psi|_{k_{ur}} = \varphi_k$. By Theorem 6.5.3, $\sigma = \rho_k(\pi)$ for some prime $\pi \in k$. The fixed field of σ in L is $L \cap F_\psi$. Also we know that $\sigma = \rho_k(\pi) = \lambda_\pi$, so we have the following:

$$k \subseteq k_\pi = L \cap F_\psi \subseteq F_\psi. \tag{6.169}$$

To prove that $L = k^{ab}(= k_\pi k_{ur})$, we need to show that $F_\psi = k_\pi$. We have the following diagram:

$$\begin{tikzcd}
 & k^{ab} = F_\psi k_{ur} \arrow[dl, dash] \arrow[dr, dash, "?"] & \\
F_\psi \arrow[d, dash, "?"] & & L = k_\pi k_{ur} \arrow[dll, dash] \arrow[d, dash] \\
k_\pi \arrow[dr, dash] & & k_{ur} \arrow[dl, dash] \\
 & k &
\end{tikzcd} \tag{6.170}$$

(Step 2) Now consider a finite extension k' of k such that

$$k \subseteq k_\pi^0 \subseteq k' \subseteq F_\psi, \tag{6.171}$$

where $k_\pi^0 = k_\pi^{1,0}$. By Lemma 3.7.3, $F_\psi \cap k_{ur} = k$, so k'/k is a totally ramified Abelian extension. Hence, by Theorem 3.10.1, $[k' : k]$ is the product of a factor of $q-1$ and a power of p, where q is the order of the residue fields of k', k. Recall that $[k_\pi^0 : k] = q-1$, so $[k' : k_\pi^0]$ is a power of p for any k'.

(Step 3) Now assume $k_\pi \neq F_\psi$. Then there is a cyclic finite extenson E/k, which satisfies the following conditions [6]:

$$k \subseteq E \subseteq F_\psi, \;\; E \nsubseteq k_\pi. \tag{6.172}$$

By (ii), $[E : E \cap k_\pi^0] = [Ek_\pi^0 : k_\pi^0]$ is a power of p (Ek_π^0 is totally ramified), but $[E \cap k_\pi^0 : k]$ is coprime to p since $(E \cap k_\pi^0)/k$ is a subextension of k_π^0/k. Then we see that there exists an extension E' of k, which is cyclic and its degree is a p-power,

$$E' \cap (E \cap k_\pi^0) = k \text{ and } E'(E \cap k_\pi^0) = E. \tag{6.173}$$

Consider:

$$\begin{tikzcd}
 & Ek_\pi^0 \arrow[dl, dash] \arrow[dr, dash, "p^d"] & \\
E \arrow[d, dash] \arrow[dr, dash, "p^d"] & & k_\pi^0 \arrow[dl, dash] \arrow[ddl, dash, "\text{q-1}"] \\
E' \arrow[dr, dash, "p^d"'] & E \cap k_\pi^0 \arrow[d, dash] & \\
 & k &
\end{tikzcd} \tag{6.174}$$

Since $E \cap k_\pi^0 \subseteq k_\pi$ and $E \nsubseteq k_\pi$, we have $E' \nsubseteq k_\pi$. As E'/k is a finite cyclic p-extension of k, replacing E' with a subfield if necessary, a finite cyclic p-extension E' over k can be found, satisfying $k \subseteq E' \subseteq F_\psi$ and $[E' : E' \cap k_\pi] = p$. This can be summarized as follows:

$$\begin{tikzcd}
 & F_\psi \arrow[dl, dash] \arrow[dr, dash, "?"] & \\
E' \arrow[dr, dash, "p"] \arrow[ddr, dash, "p^{s+1}"'] & & k_\pi \arrow[dl, dash] \\
 & E' \cap k_\pi \arrow[d, dash, "p^s"] & \\
 & k &
\end{tikzcd} \tag{6.175}$$

where $s \geq 0$.

Let $l = E' \cap k_\pi$. We know that $\mathcal{U}_k \cong \mathrm{Gal}(k_\pi/k)$ by the isomorphism in 6.109. Denote the subgroup isomorphic to $\mathrm{Gal}(k_\pi/l)$ under this map by $\mathcal{U}'$. Since $\mathcal{U}_k/\mathcal{U}' \cong \mathrm{Gal}(l/k)$, we see that $\mathcal{U}_k/\mathcal{U}'$ is cyclic group of order p^s. Hence there is a character χ of $\mathcal{U}_k/\mathcal{U}'$ with order p^s. We can view it as a continuous character of the compact group $\mathcal{U}_k$ with kernel $\mathcal{U}'$. It will be shown that there exists a continuous character λ with order p^{s+1} such that $\chi = \lambda^p$. We refer the reader to [8] and [19] for the facts below about the structure of $\mathcal{U}_1$ and the character group of $\mathbb{Z}_p$.

Firstly recall that $\mathcal{U}_k = \kappa_k^\times \times \mathcal{U}_1$ by Theorem 3.4.5.

Case 1: Assume that k contains no primitive pth root of unity. Then $\mathcal{U}_1$ is isomorphic to the direct product of finitely or infinitely many copies of $\mathbb{Z}_p$. The set $\chi(\kappa_k^\times)$ must be equal to 1, because the order of $\kappa_k^\times$ is coprime to p. Also, since $\mathcal{U}_1$ is compact, it is enough to study the character group of $\mathbb{Z}_p$. It is known that the character group of the p-adic integers, i.e. $\mathbb{Z}_p$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$, which is a divisible group. So the existence of λ is obvious.

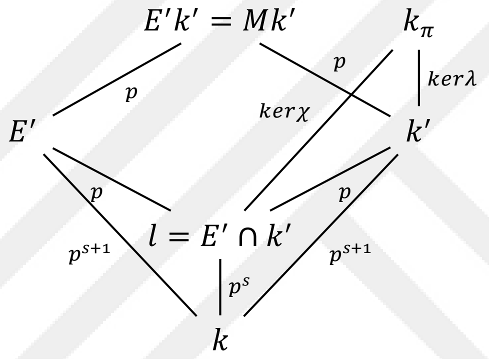
Case 2: Now suppose that k contains a primitive p-th root μ_p of unity. Then k has characteristic 0. This implies that $\mathcal{U}_1 \cong \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d$, where $a \geq 0, d \geq 1$. Since $l \subseteq E'$, where E' is a cyclic extension of degree p^{s+1}, by Lemma 6.5.7, $\mu_p \in N(l/k)$. Hence, it follows from the equation 6.150 that $\rho_k(\mu_p)|_l = 1$, that is, $\mu_p \in \mathcal{U}'$ and $\chi(\mu_p) = 1$. Since $\chi(\mu_p) = 1$, we see that we can find a suitable character on $\mathbb{Z}/p^a\mathbb{Z}$. We can find a character λ on $\mathbb{Z}_p^d$ such that

$\chi = \lambda^p$ as above.

(Step 4) Now let χ and λ be as above, $\mathcal{U}'' = \ker(\lambda)$ and k' the subfield of k_π, corresponding to $\mathcal{U}''$. So,

$$\mathcal{U}'' \cong \mathrm{Gal}(k_\pi/k'),\ \ \mathcal{U}_k/\mathcal{U}'' \cong \mathrm{Gal}(k'/k). \tag{6.176}$$

Since $l = E' \cap k_\pi$ and $l \subseteq k' \subseteq k_\pi$, $l = E' \cap k'$. Also, according to the diagram, E'/k is a cyclic extension of degree p^{s+1}. Since λ is a character of order p^{s+1}, k'/k is also of degree p^{s+1}. It follows that there exists a cyclic extension M/k of degree p such that $E'k' = Mk'$. Consider the following diagram:



(6.177)

But, by Theorem 6.5.6, M is a subset of $k_\pi = L \cap F$. This implies that $E \subseteq Mk' \subseteq k_\pi$ and this contradicts $E' \nsubseteq k_\pi$. So we have proved that:

$$F = k_\pi,\ k^{ab} = k_{ur}F = k_{ur}k_\pi = L. \tag{6.178}$$

It can be stated as a theorem:

Theorem 6.5.8. *Let k be a local field. Then*

$$k^{ab} = k_{ur}k_\pi. \tag{6.179}$$

for any prime element π of k.

Example 16. Let k be the field of p-adic numbers $\mathbb{Q}_p$. By Example 15, we have

$$k_p^n = \mathbb{Q}_p(W_f^n),\ \ n \geq 1, \tag{6.180}$$

where W_f^n is (the group of) all p^{n+1}-th roots of unity in k^{alg}. So,

$$k_p = \bigcup_n k_p^n = \mathbb{Q}_p(W_f), \tag{6.181}$$

where, W_f is (the group of) all p-power roots of unity in k^{alg}. Also we know that,

$$k_{ur} = \mathbb{Q}_p(V_\infty), \tag{6.182}$$

where V_∞ is (the group of) all roots of unity in k^{alg} with order coprime to p. Therefore $\mathbb{Q}_p^{ab}$ is generated by all roots of unity over $\mathbb{Q}_p$ in k^{alg}.

Finally, we prove that ρ_k is the local Artin map. Recall that Art_k satisfies the following:

(i) For a prime $\pi \in k$, $Art_k(\pi)|_{k_{ur}} = \varphi_k$, where φ_k is the Frobenius automorphism of k_{ur}.

(ii) For each finite Abelian extension k' over k, Ker $Art_k = N(k'/k)$.

Theorem 6.5.9. *The map ρ_k is the local Artin map.*

Proof. Let π be any prime in k. By Theorem 6.3.3, $\pi \in N(k_\pi^n/k)$ for $n \geq 0$, so it follows from (ii) that $Art_k(\pi)|_{k_\pi^n} = 1$. This implies that $Art_k(\pi)|_{k_\pi} = 1$. As $Art_k(\pi)|_{k_{ur}} = \varphi_k$ by (i), we see that $Art_k(\pi) = \lambda_\pi = \rho_k(\pi)$. Since $k^\times$ is generated by prime elements of k, $Art_k = \rho_k$. □

REFERENCES

1. Conrad K. History of Class Field Theory [cited 2019 14 April]. Avaliable from: https://kconrad.math.uconn.edu/ blurbs/gradnumthy/cfthistory.pdf.
2. İkeda I, Serbest E. Fesenko reciprocity map. *St. Petersburg Math. Journal*. 2009;20(3):407-445.
3. Lubin J, Tate J. Formal complex multiplication in local fields. *Annals of Mathematics*. 1965;81(2):380-387.
4. Ribes L, Zalesskii P. *Profinite groups*. Berlin: Springer; 2000.
5. Karpilovsky G. *Topics in field theory*. Amsterdam: North-Holland Mathematical Studies; 1989
6. Smit H. Global Field Isomorphisms: A Class Field Theoretical Approach [cited 2019 14 April]. Avaliable from: https://dspace.library.uu.nl/bitstream/handle/1874/337051/.
7. Liu H. Infinite Galois Theory [cited 2019 14 April]. Avaliable from: http://web.math.rochester.edu/people/faculty/ iosevich/liuhonorsthesis16.pdf.
8. Iwasawa K. *Local class field theory*. New York: Oxford University Press; 1986.
9. Riehl E. Lubin-Tate formal groups and local class field theory [cited 2019 14 April]. Avaliable from: http://www.math.jhu.edu/ eriehl/seniorthesis.pdf.
10. Neukirch J. *Algebraic number theory*. Berlin: Springer; 1999.
11. Engler AJ, Prestel A. *Valued fields*, Berlin: Springer; 2005.
12. Shell N. *Topological fields and near valuations*. New York: CRC Press; 1990.
13. Crivelli F. Absolute Values, Valuations and Completion [cited 2019 14 April]. Avaliable from: http://www2.math.ethz.ch/education/bachelor/seminars/fs2008/algebra/Crivelli.pdf.
14. Iturbe KB. Topological Groups [cited 2019 14 April]. Avaliable from: https://addi.ehu.es/bitstream/handle/ 10810/18039/Topological20Groups.pdf.

15. Milne JS. Class Field Theory [cited 2019 14 April]. Available from: https://www.jmilne.org/math/ CourseNotes/cft.html.

16. Thomas SB. Algebraic Properties of Formal Power Series Composition [cited 2019 14 April]. Avaliable from: https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1021.

17. Godsil CD. *Algebraic combinatorics*. New York: CRC Press; 1993.

18. Dummit D, Foote RM. *Abstract algebra*. Hoboken: John Wiley and Sons, Inc.; 2004.

19. Dikranjan D. Introductin to Topological Groups [cited 2019 14 April]. Avaliable from: https://users.dimi.uniud.it/ dikran.dikranjan/ITG.pdf.