LOCAL CLASS FIELD THEORY VIA LUBIN-TATE

**JALE DINLER**

**KOC UNIVERSITY**
**JULY 2013**

# Local Class Field Theory via Lubin-Tate

by

Jale Dinler

A Thesis Submitted to the

Graduate School of Sciences and Engineering

in Partial Fulfillment of the Requirements for

the Degree of

Master of Science

in

Mathematics

Koc University

**June 2013**

Koc University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by

Jale Dinler

and have found that it is complete and satisfactory in all respects,

and that any and all revisions required by the final

examining committee have been made.

Committee Members:

______________________________________________

Asst. Prof. Dr. Kazım Büyükboduk. (Advisor)

______________________________________________

Assoc. Prof. Dr. Emre Alkan

______________________________________________

Prof. Dr. K. İlhan İkeda

Date: ______________________________

**ABSTRACT**

In this thesis, our goal is to show that a local field K does not have a canonical maximal totally ramified abelian extension. However, for a given prime element $\pi$ of K, we are going to show that a maximal totally ramified abelian extension of $K_\pi$ of K can be constructed by using Lubin-Tate formal group laws.

**ÖZET**

Bu tezde, bir lokal K cisminin doğal maksimal dallanmış abelyen genişlemesi olmadığını ancak K'de verilen herhangi bir asal $\pi$ elemanı için Lubin-Tate formal grup teorisi kullanılarak K'nin maksimal dallanmış abelyen genişlemesi $K_{\pi}$'nin inşa edilebileceğini göstereceğiz.

**ACKNOWLEDGEMENTS**

First and foremost, I would like to express my deepest appreciation and sincere gratitude to my advisor to Asst. Prof. Dr. Kazım Büyükboduk for giving me the opportunity to study Number Theory under his supervisiom in Koc University. I believe that I have improved my skills and perspective thank to his suggestions, supports, comments and deepest knowledge during master education, since 2011.

I would like to thank to all of my instructors in Koç University for their inspirational lectures and special attentions during masters.

Last of all to you my precious family, who always support and encourage me to reach the best I can.

## TABLE OF CONTENTS

## Chapter I

## INTRODUCTION

Local class field theory studies the abelian Galois extensions of a local field K. A local field is a field that is complete with respect to a discrete valuation and has a finite residue field. For example $\mathbb{Q}_p$, the completion of $\mathbb{Q}$ with respect to the p-adic metricis a local field. $\forall \alpha \in \mathbb{Q}$, the norm of $\alpha$ is $|\alpha| = p^{-v(\alpha)}$ where $v(\alpha) = c$ such that $\alpha = p^c \mu$ and p does not divide $\mu$.

Local class field theory was born as a branch of class field theory which studies the abelian extensions of global fields however, the works of F.K. Schmidt and Chevalley shows that the results in local class field theory can also be derived independently. Lubin and Tate showed that formal groups over local fields can be used to derive important results in local class field theory such as constructing totally ramified abelian extensions of a local field which are used to prove the Artin Reciprocity Map.

In section 2, we will introduce local fields and prove Hensel's Lemma and the existence of Teichmüller representatives to derive some preliminary results on the extensions of local fields. Section 3 and 4, will give a definition and some general properties of formal groups and Lubin-Tate formal groups, respectively. Finally in section 5, we will construct totally ramified abelian extensions of a local field K and show that there is no canonical maximal totally ramified abelian extension of K.

Section 2 is based on the results of Matsumura [4] and Fesenko-Vostokov [3].

The work on sections 3, 4 and 5 are derived from Milne [2] and Iwasawa [1].

## Chapter II

## PRELIMINARIES

**Discrete Valuation:** Let K be a field. Then $v_K$ on K is called a discrete valuation if

(i) $v_K : K^\times \to \mathbb{Z}$ is a surjective homomorphism: $v_K(xy) = v_K(x)v_K(y)$, $\forall x, y \in K^\times$

(ii)$v_K(x+y) \geq min\{v_K(x), v_K(y)\}$

(iii)$v_K(x) = \infty \Leftrightarrow x = 0$

**Multiplicative Valuation:** $| \, . \, | : K \to \mathbb{R}_{\geq 0}$ is a multiplicative valuation if $\forall x, y \in K$

(i) $|xy| = |x||y|$

(ii) $|x+y| \leq max\{|x|, |y|\}$

(iii) $|x| = 0 \Leftrightarrow x = 0$

The ring of integers (valuation ring) $O_K$ of K, is the set of elements with nonnegative valuation; $O_K = \{x \in K : v_K(x) \geq 0\} = \{x \in K : |x| \leq 1\}$. Observe that $v_K(1) = v_K(1) + v_K(1)$. So, $v_K(1) = 0$. Notice that, $\forall x \in K$, $x \notin O_K \Rightarrow x^{-1} \in O_K$. Because; $x \notin O_K \Rightarrow v_K(x) < 0$.

$0 = v_K(1) = v_K(xx^{-1}) = v_K(x) + v_K(x^{-1}) \Rightarrow v_K(x^{-1}) > 0 \Rightarrow x^{-1} \in O_K$.

$O_K$ is a local ring. It is enough to show that the set of ideals of $O_K$ is totally ordered. Let I, J be any two ideals of $O_K$. If $\exists x \in I$ such that $x \notin J$, then for any nonzero $y \in J$, $xy^{-1} \notin O_K$. (Otherwise, $x = (xy^{-1})y \in J$). Then $x^{-1}y \in O_K$ and $y = x(x^{-1}y) \in I$. Hence $J \subseteq I$. From this follows that the set of ideals of $O_K$ is totally ordered and $O_K$ has unique maximal ideal, denoted by $m_K$.

If $\mu \in O_K$ is a unit in $O_K$, Then, $v_K(\mu) \geq 0$ and $v_K(\mu^{-1}) \geq 0$. As $0 = v_K(1) = v_K(\mu) + v_K(\mu^{-1})$, $v_K(\mu) = 0$. Hence,

$m_K = \{x \in O_K : v_K(x) > 0\} = m_K = \{x \in O_K : |x| \leq 1\}$.

Since $v_K$ is surjective, $\exists \pi_K \in O_K$ such that $v_K(\pi_K) = 1$. $\pi_K$ is called a uniformizer element of $O_K$. Notice that $\pi_K$ is irreducible; if $\pi_K = ab$, for some $a, b \in O_K$, then $1 = v_K(\pi_K) = v_K(a)v_K(b)$. As $v_K(a), v_K(b) \geq 0$, either $v_K(a) = 0$ and a is a unit or $v_K(b) = 0$ and b is a unit.

**Remark:** For any $c \in \mathbb{R}$, $c > 1$, $|x - y| = c^{-v_K(x-y)}$ defines a topology on K and $a + \pi_K^i O_K$ where a is a representative for $O_K/m_K$ in $O_K$ and $i \in \mathbb{Z}$, is a basis of this topology.

$O_K$ is a P.I.D. Let I be an ideal of $O_K$. Then $\{v_K(a) : a \in I\}$ is a set of nonnegative elements and thus, has a minimal element $v_K(x)$ for some $x \in I$. If $v_K(x) = 0$, then x is a unit and $I = O_K$. Otherwise, $v_K(x) = n > 0$ $\Rightarrow v_K(x) = v_K(\pi_K^n) + v_K(\mu)$, where $\mu \in O_K$ is a unit. So, $x = \pi_K^n \mu$. Then $I = xO_K = \pi_K^n O_K = (\pi_K^n)$. In particular, $m_K = (\pi_K)$.

Let S be a set of representatives for $O_K/m_K$ in $O_K$, with $0 \in S$. Every unit $\mu \in O_K$ can be uniquely written as $\mu = \sum_{i \geq 0} s_i \pi_K^i$, where $s_i \in S$. As S is a set of complete representatives, $\exists s_0 \in S$ such that $\mu \equiv s_0 \pmod{m_K}$, i.e. $v_K(\mu - s_0) > 0$. (Notice that $s_0 \notin m_K$ as $\mu$ is a unit) Similarly, $\exists s_1 \in S$ such that $\pi^{-1}(\mu - s_0) \equiv s_1 \pmod{m_K}$, i.e. $v_K(\mu - s_0 - \pi s_1) > 1$. So this technique shows that for each n, $\exists s_n$ such that $v_K(\mu - s_0 - \pi s_1 - ... - \pi^n s_n) > n$. So if

$\sum_{i=0}^{\infty} s_i\pi_K^i$ converges, then it converges to $\mu$. As $v_K(s_m\pi_K^m + ... + s_{n+1}\pi_K^{n+1} \geq n+1$, $(\sum_{i=0}^{n} s_i\pi_K^i)_{n\in\mathbb{N}}$ is Cauchy, hence converges to $\mu$ since K is complete. Assume that $\sum_{i\geq 0} s_i\pi_K^i = \sum_{i\geq 0} t_i\pi_K^i$. Then, $\sum_{i\geq 0}(s_i - t_i)\pi_K^i = 0$. So, $\sum_{i\geq 0}(s_i - t_i)\pi_K^i$ is divisible by all the powers of $\pi_K$. But this is only true when $s_i - t_i \in m_K$. So $s_i = t_i$, as the representative of $m_K$ in $O_k$ was chosen to be 0.

By using this property of units in $O_K$, we are going to show that every $x \in K$, x can be written as $\sum_{i\in\mathbb{Z}} s_i\pi_K^i$ uniquely. Notice that it is enough to show $x = \pi_K^n\mu$, where $n \in \mathbb{Z}$ and $\mu$ is a unit in $O_K$. Assume that $x = \pi_K^n\mu = \pi_K^m\xi$. Then $n = v_K(\pi_K^n\mu) = v_K(\pi_K^m\xi) = m$. So, $m = n \Rightarrow \pi_K^n\mu = \pi_K^n\xi \Rightarrow \mu = \xi$.

### 2.1 Hensel's Lemma and Teichmüller Representatives

**Lemma 2.2** (Hensel's Lemma): Let K be a local field and $O_K$ be its ring of integers. Let $f(X) \in O_K[X]$ and $\alpha_0 \in O_K$. If $f(\alpha_0) \in m_K$ and $f'(\alpha_0) \notin m_K$, then there exists a unique $\alpha \in O_K$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{m_K}$.

*Proof.* The idea behind the proof is defining a Cauchy sequence $a_0, a_1, ...$ and converging to a root $\alpha$ of f with this sequence. Let $a_0 = \alpha_0$. Define $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$. One should be careful about whether $f'(a_n)$ is invertible or not. As $f'(\alpha_0) \notin m_K$, inductively one can show that $f'(a_n) \notin m_K$.

To show that $(a_n)_{n\in(N)}$ is Cauchy, we have to prove inductively:

(i) $|a_n| \leq 1$

(ii) $|f'(a_n)| = |f'(a_0)|$

(iii)$|f(a_n)| \leq |f'(a_0)|^2 t^{2^{n-1}}$ where $t = \frac{|f(\alpha_0)|}{|f'(\alpha_0)|^2} < 1$ since $f(\alpha_0) \in m_K$ implies $|f(\alpha_0)| < 1$ and $f'(\alpha_0) \notin m_K$ implies $|f'(\alpha_0)| = 1$.

These 3 properties can be proven inductively by using the identities:

(a) Let $f(X) = \sum_{i=0}^{n} b_i X^i$. Then $f(X+Y) = b_0 + b_1(X+Y) + ... + b_n(X+Y)^n$. If we rearrange this sum, we get $f(X+Y) = \sum_{i=0}^{n} b_i X^i + (\sum_{i=1}^{n-1} i b_i X^i)Y + g(X,Y)Y^2$ where $g(X,Y) \in O_K[X,Y]$, i.e $f(X+Y) = f(X) + f'(X)Y + g(X,Y)Y^2$.

(b)$f(X) - f(Y) = b_1(X-Y) + b_2(X^2 - Y^2) + ... + b_n(X^n - Y^n)$. So $f(X) - f(Y) = (X-Y)h(X,Y)$ where $h(X,Y) \in O_K[X,Y]$.

The properties (i), (ii) and (iii) will give that $(a_n)_{n\in\mathbb{N}}$ is Cauchy:

$$\begin{aligned}
|a_m - a_n| &= |a_m - a_{m-1} + ... + a_{n+1} - a_n| \\
&\leq max\{|a_m - a_{m-1}|, ..., |a_{n+1} - a_n|\} \\
&= max\{\frac{|f(a_{m-1})|}{|f'(a_{m-1})|}, ..., \frac{|f(a_n)|}{|f'(a_n)}\} \\
&\leq |f'(a_0)|t^{2^{i-1}} \\
&\leq t^{2^{i-1}}
\end{aligned}$$

for some $m-1 \geq i \geq n$. Since $t < 1$, $(a_n)_{n\in\mathbb{N}}$ is Cauchy, because K is complete, it is convergent. Let $\lim_{n\to\infty} a_n = \alpha$. So by (i), $|\alpha| \leq 1$, i.e. $\alpha \in O_K$. Letting $n \to \infty$ in (iii), $|f(\alpha)| \leq |f'(a_0)|^2 t^{2^{n-1}} \Rightarrow |f(\alpha)| = 0$.

Next step is to show $\alpha \equiv \alpha_0 \pmod{m_K}$. We will show $a_n \equiv \alpha_0 \pmod{m_K}$ inductively and then let $n \to \infty$.

For $n = 1$, $a_1 - \alpha_0 = a_1 - a_0 = \frac{-f(a_0)}{f'(a_0)}$. As $f(a_0) \in m_K$ and $f'(a_0) \notin m_K$, $\frac{-f(a_0)}{f'(a_0)} \in m_K$, i.e. $a_1 \equiv \alpha_0 \pmod{m_K}$.

For any $n \geq 1$, we have

$$\begin{aligned} |a_{n+1} - a_n| &= \frac{|f(a_n)|}{|f'(a_n)|} = \frac{|f(a_n)|}{|f'(a_0)|} \; by \; (ii) \\ &\leq |f'(a_0)| t^{2^{n-1}} \leq |f'(a_0)| t = |f'(\alpha_0)| \frac{|f(\alpha_0)|}{|f'(\alpha_0)|^2} \\ &\leq \frac{|f(\alpha_0|}{|f'(\alpha_0)|} \end{aligned}$$

So, $a_{n+1} - a_n \in m_K$, i.e. $|a_{n+1} - a_n| < 1$.

Rewriting $a_{n+1} - \alpha$ as $a_{n+1} - a_n + a_n - \alpha$, we get $|a_{n+1} - \alpha| \leq max\{|a_{n+1} - a_n|, |a_n - \alpha|\}$. By induction hypothesis, $|a_n - \alpha| < 1$. We also showed $|a_{n+1} - a_n| < 1$. Hence, $|a_{n+1} - \alpha| < 1$, i.e. $a_{n+1} - \alpha \in m_K$.

Uniqueness of $\alpha$: Assume that $\exists \beta \in O_K$ such that $f(\beta) = 0$ and $\beta \equiv \alpha_0 \pmod{m_K}$. Let $\beta = \alpha + h$ for some $h \in O_K$. As $\beta - \alpha_0 \in m_K$ and $\alpha - \alpha_0 \in m_K$, $\beta - \alpha \in m_K$. So $|\beta - \alpha| < 1$. Now,

$0 = f(\beta) = f(\alpha + h) = f(\alpha) + f'(\alpha)h + zh^2 = f'(\alpha)h + zh^2$ for some $z \in O_K$ by the identity (a).

If $h \neq 0$, then $f'(\alpha) = -zh$.

$\Rightarrow |f'(\alpha)| = |-zh| \leq |h| = |\beta - \alpha| < 1$. But if we let $n \to \infty$ in (ii), $|f'(\alpha)| = |f'(a_0)| = |f'(\alpha_0)| = 1$. So, we have a contradiction. Thus, $h = 0$ and $\beta = \alpha$. □

**Example:** Let $K = \mathbb{Q}_{11}$ and $f(X) = X^2 - 5$. Then f has a root $\alpha_0 = 4 \in \mathbb{Z}/11\mathbb{Z}$ and $f'(4) = 8 \neq 0 \in \mathbb{Z}/11\mathbb{Z}$. So, by Hensel's lemma, we can lift $\alpha_0 = 4$ to an $\alpha \in \mathbb{Z}_{11}$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{11}$. We know that $\alpha = 4 + a_1 11 + a_2 11^2 + ....$ We want to find $a_1, a_2, ....$ Observe that $f(\alpha) = 0 \Leftrightarrow 11^k \mid f(\alpha), \forall k \in \mathbb{N}$. In order this to be true,

$11^n \mid f(4 + a_1 11 + ... + a_{n-1} 11^{n-1})\ \forall n \in \mathbb{N}$. So, one can find the value of $a_{n-1}$'s by applying this formula for each n.

Hensel's Lemma can be used to prove the existence of Teichmüller representatives.

Let $\alpha \in k^\times$ and $a \in O_K$ such that $\bar{a} = \alpha$. If a satisfies $X^{q-1} - 1$, then a is said to be a Teichmüller representative of $\alpha$.

Teichmüller representatives are in bijection with k. Since $X^{q-1} - 1$ splits into $q - 1$ distinct linear factors in $k^\times$, we can apply Hensel's Lemma. So, for each distinct root $\alpha_0 \in k^\times$, there exists an $\alpha$ of $X^{q-1} - 1$ in $O_K$ such that $\alpha \equiv \alpha_0 \pmod{m_K}$.

Note that the map $\alpha \mapsto \alpha \pmod{m_K}$ gives a multiplicative group homomorphism between the Teichmüller representatives and $k^\times$. So, Teichmüller representatives and $k^\times$ are isomorphic.

**Lemma 2.3:** $O_K^\times \simeq k^\times \bigoplus (1 + m_K)$

*Proof.* Let $\varphi : O_K^\times \twoheadrightarrow k^\times$ map $\alpha$ to $\alpha \pmod{m_K}$. Then $ker\varphi = 1 + m_K$. Consider the exact sequence

$0 \to 1 + m_K \hookrightarrow O_K^\times \twoheadrightarrow k^\times \to 0$. Let $T \subseteq O_K$ be the set of Teichmüller representatives. As $T \simeq k^\times$ with given isomorphism above, $\exists g : k^\times \to T$ such that $\varphi \circ g = id$. Hence, the exact sequence splits and $O_K^\times \simeq k^\times \bigoplus (1 + m_K)$ follows.

□

### 2.2 Extensions of Local Fields

Let L be a finite separable extension of the local field K. Then $v_K$ extends uniquely to L such that $\forall\alpha \in L$, $v_L(\alpha) = \frac{1}{f(L/K,v_L)} v_K(N_{L/K}(\alpha))$ and L is complete with respect to $v_L$, [3, pg 41, 42]. $f := f(L/K, v_L)$ is the inertia degree of L/K and $f = [k_L : k]$ where $k_L$ is the residue field of L. Let $\pi_L$ be a prime element of L. Observe that $v_K(< \pi_K >)$ is a subgroup of $v_L(< \pi_L >)$. $[v_L(< \pi_L >) : v_K(< \pi_K >)] = e(L/K, v_L)$ is called the ramification index of L/K. Let $e := e(L/K, v_L)$. In general $ef \leq [L : K] = n$, however, in our case, when L is complete, $ef = n$, [3, pg. 40].

If E is an infinite extension of K, it may not be local. Since $v_K$ extends uniquely to each finite subextension of E over K, it also extends to E, but it may not be discrete. Yet, a local ring and its maximal ideal can be defined as $O_E = \cup O_L$, $m_E = \cup m_L$ where $K \subseteq L \subseteq E$ and L/K is finite. By checking their valuations, it is easy to see that $\forall\alpha, \beta \in O_E$, $\alpha + \beta$, $\alpha\beta \in O_E$. So $O_E$ is indeed a ring. Let E/K be Galois. Define a topology on Gal(E/K)=G such that for any $\sigma \in G$, $B_L(\sigma) = \{\tau \in G : \tau|_L = \sigma|_L\}$ where $K \subseteq L \subseteq E$ and L/K is finite, are the open balls of this topology. We claim that $\{B_L(\sigma)\}_{\sigma\in G}$ forms a basis for this topology. Let $\sigma \in G$. Then by definition, $\sigma \in B_L(\sigma)$. Let $B_L(\sigma)$, $B_F(\tau) \in \{B_L(\sigma)\}_{\sigma\in G}$ and $\delta \in B_L(\sigma) \cap B_F(\tau)$. Consider $B_{LF}(\delta)$. (Note that $[L : K] \leq \infty$ and $[F : K] \leq \infty$ gives that $[LF : K] \leq \infty$) Let $\lambda \in B_{LF}(\delta)$. Then $\lambda|_{LF} = \delta|_{LF}$ by definition. So, $\lambda|_L = \delta|_L = \sigma|_L$ and $\lambda|_F = \delta|_F = \tau|_F$. Hence $\lambda \in B_L(\sigma) \cap B_F(\tau)$. Therefore, $\{B_L(\sigma)\}_{\sigma\in G}$ forms a basis.

Observe that if $\iota$ is the identity map, then $B_L(\iota) = Gal(E/L)$. Also, if $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$, then $\tau \in B_L(\sigma) \Leftrightarrow \tau(\alpha_i) = \sigma(\alpha_i), 1 \leq i \leq n$.

If E/K is finite, for any $\sigma \in Gal(E/K)$, $B_E(\sigma) = \{\sigma\}$. So, the topology on Gal(E/K) is discrete. However, if E/K is infinite, this is not the case.

**Theorem 2.4:** Gal(E/K) is compact.

*Proof.* Consider the map $\varphi : Gal(E/K) \to \Pi Gal(L/K)$ given by $\sigma \mapsto (\sigma|_L)$ where $E \supseteq L \supseteq K$ and L/K is finite. Since $E = \cup L$, $ker\varphi = \{\iota\}$, i.e. $\varphi$ is injective. Observe that the topology on $\Pi Gal(L/K)$ is the product topology of discrete topologies. Since a discrete topology is compact if and only if it is finite, each Gal(L/K) is compact. By Tychonoff, $\Pi Gal(L/K)$ is compact. As any closed subset of a compact space is compact, if $\varphi(Gal(E/K))$ is closed and $\varphi^{-1}$ is continuous, then Gal(E/K) would be compact.

$\underline{\varphi(Gal(E/K)) \text{ is closed}}$: If $(\sigma|_L)$ is not in the image of Gal(E/K), then $\exists \sigma|_{L'}$ and $\sigma|_{L''}$ such that $L' \subseteq L''$ and $(\sigma|_{L''})|_{L'} \neq \sigma|_{L'}$.
Let $U = \Pi_{L \neq L', L''} Gal(L/K) \bigoplus \{\sigma|_{L'}\} \bigoplus \{\sigma|_{L''}\}$. U is open in $\Pi Gal(L/K)$ and $U \cap \varphi(Gal(E/K)) = \emptyset$. Hence $\varphi(Gal(E/K))$ is closed.

$\underline{\varphi^{-1} \text{ is continuous}}$: Let $B_L(\sigma)$ be an open subset of Gal(E/K). Then $\tau \in B_L(\sigma)$ if and only if $\tau(\alpha_i) = \sigma(\alpha_i), 1 \leq i \leq n$ where $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$. So $\varphi$ maps $B_L(\sigma)$ to $\Pi S_\sigma$ such that $S_\sigma = B_F(\sigma)$ where $F = K(\alpha_{i_1}, ..., \alpha_{i_k})$, $\{\alpha_{i_1}, ..., \alpha_{i_k}\} \subseteq \{\alpha_1, ..., \alpha_n\}$, on finitely many terms and $S_\sigma = Gal(L/K)$ on infinitely many terms. Thus, $\varphi$ is an open mapping and $\varphi^{-1}$ is continuous. From this follows, Gal(E/K) is compact.

□

### 2.2.1 Unramified Extensions

Let L/K be a finite extension of degree n. If $[k_L : k] = n$, then L/K is unramified. As $[k_L : k] = n$, $e(L/K, v_L) = 1$. So, $v_L(\pi_K) = v_L(\pi_L)$. Hence, one can say that L/K is unramified if and only if a prime element of K remains prime in L.

Unramified extensions can be characterized through the following lemma:

**Lemma 2.5:** Let L/K be a finite, Galois extension. L/K is unramified $\Leftrightarrow Gal(L/K) \simeq Gal(k_L/k)$.

*Proof.* Since k is a finite field , it is perfect. i.e. $k_L$ is separable. Also, $k_L/k$ is a finite field extension, say of degree n. Then, $k_L$ is the splitting field of the polynomial $X^{q^n} - X$. Hence, $k_L/k$ is Galois.

If $Gal(L/K) \simeq Gal(k_L/k)$, then $|Gal(L/K)| = |Gal(k_L/k)|$. Hence $[L : K] = [k_L : k]$, i.e. L/K is unramified.

If L/K is unramified, then consider the map $\phi : Gal(L/K) \rightarrow Gal(k_L/k)$ given by $\sigma \rightarrow \bar{\sigma}$ where $\overline{\sigma}(\overline{x}) = \overline{\sigma(x)}$. It is easy to see that $\phi$ is well- defined and a homomorphism. $\phi$ is surjective, since each $\overline{\sigma}$ maps $\alpha$ to a distinct conjugate of $\alpha$ and these distinct conjugates lift to a distinct $\beta \in L$ by Hensel's Lemma. In other words, for each $\overline{\sigma} \in Gal(k_L/k)$, $\exists \sigma \in Gal(L/K)$ such that $\sigma$ maps $\beta$ to its distinct conjugates.

As $|Gal(L/K)| = |Gal(k_L/k)|$, surjectivity implies injectivity. Hence, $Gal(L/K) \simeq Gal(k_L/k)$. □

**Remark:** Composite of two finite unramified extensions is unramified. Let L/K, $L'$/K be finite and unramified. Let $k_{L'} = k(\overline{\alpha})$ for some $\overline{\alpha} \in k_{L'}$.

By lemma 2.4, $\overline{\alpha}$ can be lift to some $\alpha \in L'$ and $L' = K(\alpha)$, $LL' = L(\alpha)$ follows. Observe that $\alpha \in O_{L'} \subseteq O_{LL'}$ since $\overline{\alpha} \neq 0$. So $v_{LL'}(\alpha) \geq 0$. Let $g(X) = Irr(\alpha, L)$ and $g(X) = a_n X^n + ... + a_0$. Then $v_{LL'}(\alpha) = \frac{1}{f(LL'/L, v_{LL'})} v_L((-1)^n a_0) \geq 0$, thus $v_L(a_0) \geq 0$. Hence $g(X) \in O_L[X]$ [3, pg 37]. So it makes sense to talk about $\overline{g}(X) \in k_L[X]$. $\overline{g}$ is irreducible in $k_L$ since g is irreducible in $O_L$. So $deg(\overline{g}) = deg(g)$, i.e. $LL'/L$ is unramified. As both $LL'/L$, L/K is unramified, $LL'/K$ is unramified.
Therefore, one can define a maximal unramified extension $K^{ur}$ of K as the union of unramified extensions of finite degree. The lemma below will show that $K^{ur} \subseteq K^{ab}$.

**Lemma 2.6:** For any local field K and positive integer n, there exists a unique unramified extension L of degree n over K, which is Galois with cyclic Galois group.

*Proof.* We know that the elements of k are the roots of $X^q - X$. Since k is a finite field, it has a unique extension $\mathbb{F}_{q^n}$ of degree n which is the splitting field of $X^{q^n} - X$. Let $\bar{g}(X)$ be the minimal polynomial of a primitive $(q^n - 1)$st of unity over k. As $\bar{g}$ is separable, we can lift $\bar{g}(X)$ to a $g(X) \in K[X]$. Note that g is irreducible and separable since $\bar{g}$ is. Let L be the splitting field of g(X) over K. Then L/K is Galois and $[L : K] = deg(g) = deg(\bar{g}) = n$. So $[k_L : k] \leq n$. However, by construction $\mathbb{F}_{q^n} \subseteq k_L$, i.e. $[k_L : k] \geq n$. Therefore, $[k_L : k] = n$ and L/K is unramified of degree n. By lemma 2.4, $Gal(L/K) \simeq Gal(k_L/k)$. Since, $Gal(k_L/k)$ is cyclic, generated by the Frobenius map $\varphi(x) = x^q$, Gal(L/K) is cyclic and the automorphism $\sigma \in Gal(L/K)$ such that $\sigma(x) \equiv x^q \pmod{m_L}$ for all $x \in L$, generates the

Gal(L/K) and is denoted by $Frob_{L/K}$.

Now let L/K and $L'$/K be two distinct unramified extensions of degree n. Then $LL'$/K is unramified and so, $Gal(LL'/K)$ is expected to be cyclic as proven above. However, $LL'$/K is unramified implies that $LL'/(L \cap L')$ is unramified. Let $[L : L \cap L'] = m$. Then $[L' : L \cap L'] = m$ and $Gal(L/(L \cap L')) \simeq \mathbb{Z}/m\mathbb{Z} \simeq Gal(L/(L \cap L'))$. Therefore, $Gal(LL'/(L \cap L')) \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$, which is not cyclic. Hence there is a unique unramified extension L/K of degree n. □

Let $K_n/K$ be the unique unramified extension of degree n. Then $K^{ur} = \cup K_n$. Frobenius automorphism extends to $K^{ur}$ and can be identified as the image of generators of $Gal(K_n/K) = \mathbb{Z}/n\mathbb{Z}$. Hence $Gal(K^{ur}/K)$ is the profinite completion of $\mathbb{Z}$:

$$Gal(K^{ur}/K) = \varprojlim Gal(K_n/K).$$

**2.2.2 Ramified Extensions**

If $[k_L : k] = 1$, then L/K is totally ramifed. Let L/K be Galois and $I_n = \{\sigma \in Gal(L/K) : v_L(x - \sigma x) \geq n + 1, \forall x \in L\}$. Our claim is that $I_n$ is a subgroup of Gal(L/K). As $v_L(x - x) = \infty$, identity map is in $I_n$. Let $\sigma \in I_n$. Then $v_L(x - \sigma x) \geq n + 1$. i.e. $x - \sigma x \in m_L^{n+1}$. As $\sigma \in Gal(L/K)$, $\sigma^{-1}x - x \in \sigma^{-1}m_L^{n+1} = m_L^{n+1}$. Therefore $\sigma^{-1} \in I_n$. Let $\sigma, \tau \in I_n$. Then $\sigma\tau x - x = \sigma(\tau x - x) + \sigma x - x \in m_L^{n+1}$. So $I_n$ is indeed a subgroup of Gal(L/K). These subgroups are called higher ramification groups. Observe that $Gal(L/K) \supseteq I_0 \supseteq I_1 \supseteq ...$

Let $\phi : Gal(L/K) \twoheadrightarrow Gal(k_L/k)$ such that $\phi(\sigma) \mapsto \overline{\sigma}$ where $\overline{\sigma}(\overline{x}) = \overline{\sigma(x)}$. Consider the exact sequence

$$0 \to I_0 \to Gal(L/K) \to Gal(k_L/k) \to 0.$$

Notice that $\sigma \in ker\phi \Leftrightarrow \sigma x \equiv x \pmod{m_L} \Leftrightarrow v_L(x - \sigma x) \geq 1 \Leftrightarrow \sigma \in I_0$. So, $Gal(L/K)/I_0 \simeq Gal(k_L/k)$. Notice that, L/K is unramified if and only if $I_0 = \{1\}$ and L/K is totally ramified if and only if $I_0 = Gal(L/K)$. In general, if $L_0$ is the largest unramified subextension of L/K, then $Gal(L/L_0) \simeq I_0$.

**Lemma 2.7:** Let L/K be totally ramified and let $\pi_L \in L$ be a prime element. Then the group $I_n = \{\sigma \in Gal(L/K) : v_L(\sigma\pi_L - \pi_L) \geq n + 1\}$

*Proof.* Observe that if $\sigma \in I_n$, then $v_L(\sigma x - x) \geq n+1$, $\forall x \in L$, in particular for $x = \pi_L$. So, $I_n \subseteq \{\sigma \in Gal(L/K) : v_L(\sigma\pi_L - \pi_L) \geq n + 1\}$.
We know that $x \in L$ can be written uniquely as $x = \sum_{i\in\mathbb{Z}} a_i\pi_L^i$ where $a_i$'s are chosen from a set of representatives of $k_L$ in $O_L$. So, these representatives can be chosen as Teichmüller representatives, $a_1, ..., a_q$. As L/K is totally ramified, $k_L$ and k are the same field. Therefore, these $a_i$'s are actually in $O_K$ and are fixed by any $\sigma \in Gal(L/K)$.
Now let $\tau \in \{\sigma \in Gal(L/K) : v_L(\sigma\pi_L - \pi_L) \geq n + 1\}$. If $\forall x \in L$, $v_L(\tau x - x) \geq v_L(\tau\pi_L - \pi_L)$, then $I_n \supseteq \{\sigma \in Gal(L/K) : v_L(\sigma\pi_L - \pi_L) \geq n+1\}$. Observe that, $\tau x - x \in m_L$ since L/K is totaly ramified, i.e $Gal(L/K) = I_0$ and $\tau \in I_0$. So $v_L(\tau x - x) = v_L(\tau(\sum_{i\in\mathbb{Z}} a_i\pi_L^i) - \sum_{i\in\mathbb{Z}} a_i\pi_L^i)) = v_L(\sum_{i\in F} a_i(\tau^i\pi_L - \pi_L^i)) \geq 1$. Therefore, for $i \leq 0$, $a_i = 0$ and $v_L(\tau x - x) = v_L(\tau\pi_L - \pi_L) + v_L(a_1 + a_2(\tau\pi_L - \pi_L) + ...)$. Since $a_1 + a_2(\tau\pi_L - \pi_L) + ... \in O_L$,

$v_L(\tau x - x) \geq v_L(\tau\pi_L - \pi_L)$.

Hence, $\tau \in I_n$. □

**Lemma 2.8:** Let L be a finite Galois extension of K. If the residue field of L has order $q'$, then $[I_0 : I_1] \mid (q'-1)$ and $[I_n : I_{n+1}] \mid q'$ for $n \geq 1$. Furthermore, for large enough m, $I_n = 1$ for all $n > m$ and $I_1$ has p-power order.

*Proof.* Let $\pi_L$ be a prime element of L. We claim that there is a homomorphism $\varphi : I_0 \to O_L^\times/(1+m_L) \simeq k^\times$ given by $\sigma \to \frac{\sigma\pi_L}{\pi_L}$ and $ker\varphi$ contains $I_1$. Observe that $\sigma\pi_L$ and $\pi_L$ has the same valuation as $\sigma \in Gal(L/K)$. Thus, $\frac{\sigma\pi_L}{\pi_L}$ is a unit.

Let $\sigma,\ \tau \in I_0$. Then

$$\begin{aligned}
\tau(\frac{\sigma\pi_L}{\pi_L}) &\equiv \frac{\sigma\pi_L}{\pi_L} \pmod{m_L} \\
\frac{\tau(\sigma\pi_L)}{\tau\pi_L} &\equiv \frac{\sigma\pi_L}{\pi_L} \pmod{m_L} \\
\frac{\tau\sigma\pi_L}{\pi_L} &\equiv \frac{\tau\pi_L}{\pi_L}.\frac{\sigma\pi_L}{\pi_L} \pmod{m_L}
\end{aligned}$$

So, $\varphi(\tau\sigma) = \varphi(\tau)\varphi(\sigma)$, i.e. $\varphi$ is a homomorphism.

Now, we want to show that $ker\varphi \supseteq I_1$. If $\sigma \in I_1$, then $\sigma\pi_L \equiv \pi_L \pmod{m_L^2}$. This gives that $\frac{\sigma\pi_L}{\pi_L} \equiv 1 \pmod{m_L}$. Hence $\sigma \in ker\varphi$. From this follows, $I_0/I_1 \hookrightarrow O_L^\times/(1+m_L) \simeq k^\times$. Hence $[I_0 : I_1] \mid (q'-1)$.

Now consider the map $\lambda : 1 + m_L^n \twoheadrightarrow k_L (= O_L/m_L)$ given by $1 + \pi^n\mu \mapsto \mu$. $\lambda$

is a homomorphism since,

$$
\begin{aligned}
\lambda((1+\pi_L^n\mu)(1+\pi_L^n\nu)) &= \lambda(1+\pi_L^n(\mu+\nu+\pi_L^n\mu\nu)) \\
&= \mu+\nu+\pi_L^n\mu\nu \equiv \mu+\nu \pmod{m_L},\ i.e \\
\lambda((1+\pi_L^n\mu)(1+\pi_L^n\nu)) &= \mu+\nu \\
&= \lambda(1+\pi_L^n\mu)+\lambda(1+\pi_L^n\nu).
\end{aligned}
$$

Observe that $1+\pi_L^n\mu \in ker\lambda \Leftrightarrow \mu \in m_L \Leftrightarrow 1+\pi_L^n\mu \in 1+m_L^{n+1}$. So, $ker\lambda = 1+m_L^{n+1}$ and $(1+m_L^n)/(1+m_L^{n+1}) \simeq k_L$ follows.

Consider the map $\phi : I_n \to (1+m_L^n)/(1+m_L^{n+1})$ given by $\sigma \mapsto \frac{\sigma\pi_L}{\pi_L}$. $\phi$ is a homomorphism and $ker\phi \supseteq I_{n+1}$ (the proof is same as n=0 case). Therefore, $I_n/I_{n+1} \hookrightarrow (1+m_L^n)/(1+m_L^{n+1}) \simeq k_L$ and $[I_n : I_{n+1}] \mid q'$ follows. As every element of $k_L$ has p-power order, so do the elements of $I_n/I_{n+1}$. In particular, as $[I_2 : I_1] \mid |I_1|$, $p \mid |I_1|$. By Cauchy's theorem, $I_1$ has an element of order p.
Let $L_0$ be the maximal unramified subextension of L/K. Then L/$L_0$ is totally ramified. By Lemma 2.7, the $n^{th}$ ramification group of $Gal(L/L_0) = G$ coincides with the set $\{\sigma \in G : \sigma\pi_L - \pi_L \geq n+1\}$. Let $n > max\{\sigma \in G : v_L(\sigma\pi_L - \pi_L)\}$. Then $I_n = \{1\}$. □

# Chapter III

## FORMAL GROUP LAWS

Let A be a commutative ring with unity. A formal power series with coefficients in A is an infinite sequence

$$f = (a_0, a_1, ...), \qquad a_i \in A, \quad i \in \mathbb{N}$$

Formal power series with coefficients in A forms a commutative ring and is denoted by A[[X]]. Addition and multiplication are defined in the usual way:

$$\begin{aligned}(a_0, a_1, ...) + (b_0, b_1, ...) &= (a_0 + b_0, a_1 + b_1, ...)\\ (a_0, a_1, ...)(b_0, b_1, ...) &= (c_0, c_1, ...)\\ where\ c_n &= \sum_{i=0}^{n} a_i b_{n-i}\end{aligned}$$

One may think of formal power series without the notion of convergence. So, in contrast to power series, we are not allowed to substitute a value $\alpha \in A$ into $f(X) \in A[[X]]$ because $f(\alpha)$ is an infinite sum which has a definite value when it is convergent. As an immediate result of this is that the composition f(g(X)) only makes sense when $g(X) \in A[[X]]$.

**Definition:** A commutative formal group law is a power series $F \in A[[X,Y]]$ such that

$$\begin{aligned} (i) \quad & F(X,Y) = F(Y,X) \\ (ii) \quad & F(X,0) = X \; and \; F(0,Y) = Y \\ (iii) \quad & F(F(X,Y),Z) = F(X,F(Y,Z)) \end{aligned}$$

Notice that (ii) implies that F has no constant term, so (iii) makes sense. Property (ii) can also be interpreted as $F(X,Y) \equiv X + Y \pmod{deg.2}$ [2, pg 16-17]

Now, our goal is to show that XA[[X]] is a commutative group with the operation $F(X,Y) := X +_F Y$. Observe that (i) gives commutativity, (ii) identity and (iii) associativity. So if $f[X] \in XA[[X]]$ has an inverse in XA[[X]], we're done. To show that inverses exist, it is enough to prove that X is invertible in XA[[X]]. Because if $i_F(X) \in XA[[X]]$ is the inverse of X, then $i_F(f(X))$is the inverse of $f(X) \in XA[[X]]$

**Lemma 3.1:** There is a unique $i_F(X) \in XA[[X]]$ such that $F(X, i_F(X)) = 0$.

*Proof.* As $F(X,Y) = X + Y + \sum_{i,j\geq 1} a_{ij} X^i Y^j$, F contains no higher order terms in only one variable. So one can construct $i_F(X)$ inductively such that $F(X, h_n(X)) \equiv 0 \pmod{deg.\ n+1}$ where $i_F(X) \equiv h_n(X) \pmod{deg.\ n+1}$. If $F(X, h_n(X)) \equiv 0 \pmod{deg.\ n+1}$, since $h_n$ is unique, one can uniquely define $h_{n+1}(X) = h_n(X) + b_{n+1}X^{n+1}$ and $F(X, h_{n+1}) \equiv 0 \pmod{deg.\ n+1}$. Clearly, $h_2(X) = -X + a_{11}X^2$ (since $F(X, h_2) \equiv X + (-X + a_{11}X^2) + a_{11}X(-X + a_{11}X^2) \equiv 0 \pmod{deg.\ 3}$) and the rest follows.

$\square$

So, $(XA[[X]], +_F)$ is an abelian group.

Let F(X, Y) and G(X, Y) be two commutative formal group laws over A. Then $f(X) \in XA[[X]]$ is a group homomorphism if $f(X +_F Y) = f(X) +_G f(Y)$, written as $f : F \to G$. In other words, $f : F \to G$ is a homomorphism if and only if $f \circ F = G \circ f$.
If there exist a $g(X) \in XA[[X]]$ such that $g : G \to F$ and $f \circ g = g \circ f = X$, then f is an isomorphism. A homomorphism $f : F \to F$ is called an endomorphism.

**Example:** Let $F(X, Y) = X + Y + XY$ and $f(X) = (1 + X)^p - 1$. It is easy to see that $f(X +_F Y) = f(X) +_F f(Y)$. So, f is an endomorphism.

**Lemma 3.2:**
(i) $(Hom(F, G), +_G)$ is a subgroup of XA[[X]].
(ii) $(End(F), +_F, \circ)$ is a ring.

*Proof.* (i) As $Hom(F, G)$ is a subset of XA[[X]], it is already commutative and associative. So it is enough to prove that $Hom(F, G)$ is closed and $\forall f \in Hom(F, G)$, $i_G \circ f \in Hom(F, G)$.
Let $f,\ g \in Hom(F, G)$ and $h = f +_G g$. Then $h(X +_F Y) = f(X +_F Y) +_G g(X +_F Y)$. As $f, g \in Hom(F, G)$ and Hom(F,G) is commutative and associative, $h(X +_F Y) = (f(X) +_G g(X)) +_G (f(Y) +_G g(Y)) = h(X) +_G h(Y)$.

Therefore, $h \in Hom(F,G)$.

Let $f \in Hom(F,G)$. We want to show that $(i_G \circ f) \circ F = G \circ (i_G \circ f)$. But first, we need to show $i_G \circ G = G \circ i_G$ and $\forall f,g,h \in XA[[X]], f \circ (g \circ h) = (f \circ g) \circ h$. $G(G, G \circ i_G) = G(X,Y) +_G (i_G(X) +_G i_G(Y)) = (X +_G Y) +_G (i_G(X) +_G i_G(Y)) = (X +_G i_G(X)) +_G (Y +_G i_G(Y)) = 0 +_G 0 = 0$. As $G(G, i_G \circ G)$ is also 0 and the inverse is unique, $i_G \circ G = G \circ i_G$.

If $f, g$ *and* $h \in XA[[X]]$, then $(fg) \circ h = (f \circ h)(g \circ h)$. Then for any $n \in \mathbb{N}$, $f^n \circ g = (f \circ g)^n$. For $f(X) = X^n$, $(f \circ g) \circ h = (g \circ h)^n = f \circ (g \circ h)$. So, if $f(X) = \sum_{n \geq 1} a_n X^n$, then both are equal to $\sum_{n \geq 1} a_n (g \circ h)^n$.

Thus, $G \circ (i_G \circ f) = (G \circ i_G) \circ f = (i_G \circ G) \circ f = i_G \circ (G \circ f) = i_G \circ (f \circ F) = (i_G \circ f) \circ F$.

Hence, $(Hom(F,G), +_G)$ is a subgroup of XA[[X]].

(ii) In (i), we showed that $(End(F), +_F))$ is an abelian group and $\circ$ is associative. So, we only need to prove that $\circ$ is distributive.

Let $f,\ g$ *and* $h \in End(F)$. $f \circ (g +_F h) = f \circ (F(g(X), h(Y)) = F(g(X), h(Y)) \circ f = F(f \circ g(X), f \circ h(Y)) = (f \circ g)(X) +_F (f \circ h)(Y)$. Thus $\circ$ is distributive over $+_F$.

Hence $(End(F), +_F, \circ)$ is a ring.

□

Now, let $A = O_K$ and $F \in A[[X,Y]]$ be a commutative formal group law. Let $F(X,Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j$. Observe that for any, $x,\ y \in m_L$, as $i,\ j \to \infty$, F(x,y) converges to an element $x +_F y \in m_L$. Therefore, $(m_L, +_F)$ is a commutative group.

**Example:** Let $F(X,Y) = X + Y + XY$ and $f(X) = (1+X)^p - 1$. It is easy to see that the map $a \mapsto a+1$, from $(m_L, +_F)$ to $(1+m_L, .)$ is an isomorphism and the below diagram commutes:

$$\begin{array}{ccc} m_L & \xrightarrow{\quad f \quad} & m_L \\ \Big\downarrow {\scriptstyle a \to a+1} & & \Big\downarrow {\scriptstyle a \to a+1} \\ 1+m_L & \xrightarrow{a \to a^p} & 1+m_L \end{array}$$

## Chapter IV

## LUBIN TATE FORMAL GROUPS

For a given prime elemenet $\pi \in K$, let $F_\pi$ denote the set of power series $f(X) \in O_K[[X]]$ such that:
(i) $f(X) \equiv \pi X \pmod{deg.2}$
(ii) $f(X) \equiv\ X^q \pmod{\pi}$
where q is the number of elements in the residue field k of K.

**Example:** $f(X) = \pi X + X^q$ is in $F_\pi$.

**Lemma 4.1:** Let $f, g \in F_\pi$ and let $\phi_1(X_1, X_2, ..., X_n) \in O_K[[X_1, X_2, ..., X_n]]$ be a linear form. Then there is a unique $\phi \in O_K[[X_1, X_2, ..., X_n]]$ such that:
(i) $\phi \equiv \phi_1 \pmod{deg.\ 2}$
(ii) $f(\phi(X_1, ..., X_n)) = \phi(g(X_1), ..., g(X_n))$.

*Proof.* We are going to construct $\phi$ inductively such that $\forall n \in \mathbb{N}$, $\phi \equiv \phi_n \pmod{deg.\ n+1}$ where each $\phi_n$ is unique and satisfies (i) and (ii) $\pmod{deg.\ n+1}$.
For $n = 1$, our candidate is $\phi_1$ because of the uniqueness.
Let $\phi_1(X_1, ..., X_n) = a_1X_1 + ... + a_nX_n$ for $a_1, ..., a_n \in O_K$. (i) $\phi_1 \equiv \phi_1 \pmod{deg.\ 2}$
(ii)$f(\phi_1(X_1, ..., X_n)) \equiv \pi\phi_1(X_1, ..., X_n) \equiv \pi(a_1X_1 + ... + a_nX_n) \pmod{deg.\ 2}$
$\phi_1(g((X_1), ..., g(X_n)) \equiv \pi\phi_1(\pi X_1, ..., \pi X_n) \equiv \pi(a_1X_1 + ... + a_nX^n) \pmod{deg.\ 2}$

So $f \circ \phi_1 \equiv \phi_1 \circ g \pmod{deg. 2}$.
Let $\phi_n$ be unique and satisfies (i) and (ii) $\pmod{deg. n+1}$. Define $\phi_{n+1} = \phi_n + h$ where $h \in O_K[[X_1, ..., X_n]]$ is homogeneous of degree $n+1$. (Notice that since $\phi_n$ is unique there is no other candidate for $\phi_{n+1}$) Then
$f \circ \phi_{n+1} \equiv f \circ (\phi_n + h) \equiv \pi\phi_n + \pi h \equiv f \circ \phi_n + \pi h \pmod{deg. n+2}$ and $\phi_{n+1} \circ g \equiv (\phi_n + h) \circ g \equiv \phi_n \circ g + h \circ g \equiv \phi_n \circ g + h(g(X_1), ..., g(X_n)) \equiv \phi_n \circ g + h(\pi X_1, ..., \pi X_n) \equiv \phi_n \circ g + \pi^{n+1} h \pmod{deg. n+2}$
We want to check that if such h exists, i.e we want that $h \in O_K[[X_1, ..., X_n]]$. Observe that (ii) is satisfied if $f \circ \phi_n - \phi_n \circ g \equiv (\pi^{n+1} - \pi)h \pmod{deg. n+2}$. Since $f(X) \equiv g(X) \equiv X^q \pmod{\pi}$ and charK=p ($q = p^r$), $f \circ \phi_n - \phi_n \circ g \equiv (\phi_n(X_1, ..., X_n)^q - \phi_n(X_1^q, ..., X_n^q) \equiv 0 \pmod{\pi}$, i.e. $\pi$ divides $f \circ \phi_n - \phi_n \circ g$. Also, $\pi^n - 1$ is a unit in $O_K$. Therefore such h exists over $O_K$ and our construction of $\phi_{n+1}$ is valid. Hence, there is a unique $\phi \in O_K[[X_1, ..., X_n]]$ which satisfies (i) and (ii). □

**Theorem 4.2:** For each $f \in F_\pi$ there exists a unique commutative formal group law $F_f$ with coefficients in $O_K$ such that $f \in End(F_f)$.

*Proof.* By lemma 4.1, $\forall f \in F_\pi$, $\exists F_f \in O_K[[X, Y]]$ such that $F_f(X, Y) \equiv X + Y \pmod{deg. 2}$ and $f \circ F_f = F_f \circ f$. So it is enough to show $F_f$ is a commutative formal group law.
(i)<u>$F_f(X, Y) = F_f(Y, X)$</u>: Let $G(X, Y) = F_f(Y, X)$. Then $G(X, Y) \equiv X + Y \equiv F_f(Y, X) \pmod{deg. 2}$.
Also, $f \circ G(X, Y) = f \circ F_f(Y, X) = F_f(Y, X) \circ f = F_f(f(Y), f(X)) = G(f(X), f(Y)) = G(X, Y) \circ f$ So both $G(X, Y) = F_f(Y, X)$ and $F_f(X, Y)$ satisfies the two conditions. By uniqueness, $F_f(X, Y) = F_f(Y, X)$

(ii)$\underline{F_f(X,0) = X \text{ and } F_f(0,Y) = Y}$: As $F_f(X,Y) \equiv X + Y \pmod{deg.\ 2}$ and $f \circ F_f = F_f \circ f$, $F_f(X,0) = X$ and $F_f(0,Y) = Y$. (It is mentioned in chapter 3 that these two conditions are same).

(iii)$\underline{F_f(F_f(X,Y),Z) = F_f(X,F_f(Y,Z))}$:
$F_f(F_f(X,Y),Z) \equiv X + Y + Z \equiv F_f(X,F_f(Y,Z) \pmod{deg.\ 2}$.
$f \circ F_f(X,F_f(Y,Z)) = F_f(f(X), f \circ F_f(Y,Z)) = F_f(f(X), F_f(Y,Z) \circ f) = F_f(X,F_f(Y,Z)) \circ f$. and
$f \circ F_f(X,F_f(Y,Z)) = F_f(f(X), f \circ F_f(Y,Z)) = F_f(f(X), F_f(Y,Z) \circ f) = F_f(X,F_f(Y,Z)) \circ f$. So, again by uniqueness, $F_f(F_f(X,Y),Z) = F_f(X,F_f(Y,Z))$.

□

Let $f \in F_\pi$ and $F_f$ be the Lubin-Tate formal group law given by theorem 4.2. Let $a \in O_K$. Then, there exists a unique $[a]_f \in O_K[[X]]$ such that
(i) $[a]_f \equiv aX \pmod{deg.\ 2}$
(ii)$f \circ [a]_f = [a]_f \circ f$
Notice that $[\pi]_f = f$.

**Theorem 4.3:** For each $a \in O_K$, $[a]_f \in End(F_f)$. Furthermore, $O_K$ can be embedded into $End(F_f)$ with the map $a \mapsto [a]_f$.

*Proof.* Let $a \in O_K$. We want to show that $[a]_f \circ F_f = F_f \circ [a]_f$.
(i) $[a]_f \circ F_f \equiv aX + aY \pmod{deg.\ 2}$ and $F_f \circ [a]_f \equiv aX + aY \pmod{deg.\ 2}$.
(ii) $f \circ ([a]_f \circ F_f) = (f \circ [a]_f) \circ F_f = [a]_f \circ (f \circ F_f) = ([a]_f \circ F_f) \circ f$
$f \circ (F_f \circ [a]_f) = (f \circ F_f) \circ [a]_f = F_f \circ (f \circ [a]_f) = F_f \circ ([a]_f \circ f) = (F_f \circ [a]_f) \circ f$.
Since both $[a]_f \circ F_f$ and $F_f \circ [a]_f$ satisfies the conditions (i) and (ii), by uniqueness, $[a]_f \circ F_f = F_f \circ [a]_f$.

Let $\varphi : O_K \to End(F_f)$ given by the map $a \mapsto [a]_f$.

$\varphi$ is a ring homomorphism, i.e. $[a]_f \circ [b]_f = \varphi(a)\varphi(b) = \varphi(ab) = [ab]_f$ and $[a]_f + [b]f = \varphi(a)\varphi(b) = \varphi(a+b) = [a+b]_f$

(i) $[a]_f \circ [b]_f \equiv abX \equiv [ab]_f \pmod{deg.\ 2}$

(ii) $([a]_f \circ [b]_f) \circ f = [a]_f \circ ([b]_f \circ f) = [a]_f(\circ f \circ [b]_f) = ([a]_f \circ f) \circ [b]_f = f \circ ([a]_f \circ [b]_f)$ and $[ab]_f \circ f = f \circ [ab]_f$. By uniqueness, $\varphi(a)\varphi(b) = \varphi(ab)$.

(i) $[a]_f + [b]_f \equiv aX + bX \equiv (a+b)X \equiv [a+b]_f \pmod{deg.\ 2}$

(ii) $([a]_f + [b]_f) \circ f = [a]_f \circ f + [b]_f \circ f$ (since $f, [a]_f, [b]_f \in End(F_f)$ and $(End(F_f), +_F, \circ)$ is a ring) $= f \circ [a]_f + f \circ [b]_f = f \circ ([a]_f + [b]_f)$. Also, $[a+b]_f \circ f = f \circ [a+b]_f$.

So, $\varphi(a+b) = \varphi(a) + \varphi(b)$. Hence $\varphi$ is a ring homomorphism.

$\varphi$ is injective: if $a \neq b$, then by condition 1, $[a]_f \neq [b]_f$.

Therefore, $a \mapsto [a]_f$ gives an injective ring homomorphism from $O_K$ to $End(F_f)$. □

More generally, if $f, g \in F_\pi$ and $a \in O_K$, then there exists a unique $[a]_{g,f} \in O_K[[X]]$ such that

(i) $[a]_{g,f} \equiv aX \pmod{deg.\ 2}$

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

Observe that $[a]_{g,f} \circ F_f \equiv aX + aY \equiv F_g \circ [a]_{f,g} \pmod{deg.\ 2}$. Also $g \circ ([a]_{g,f} \circ F_f) = (g \circ [a]_{g,f}) \circ F_f = ([a]_{g,f} \circ f) \circ F_f = [a]_{g,f} \circ (f \circ F_f) = [a]_{g,f} \circ (F_f \circ f) = (a_{g,f} \circ F_f) \circ f$ and

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

Hence by uniqueness, $[a]_{g,f} \circ F_f = F_g \circ [a]_{g,f}$, i.e. $[a]_{g,f} \in Hom(F_f, F_g)$.

Similarly, one can show that $[ab]_{h,f} = [a]_{h,g} \circ [b]_{g,f}$.

**Theorem 4.4:** For any $f, g \in F_\pi$, $F_f \simeq F_g$ as formal $O_K$-modules.

*Proof.* Let $\mu$ be a unit in $O_K$. Then $X = [1]_{f,f} = [\mu]_{f,g} \circ [\mu^{-1}]_{g,f}$. So, $[\mu]_{f,g} : F_f \to F_g$ is an isomorphism. □

This isomorphism implies that the choice of $f \in F_\pi$ is not important.

**Definition:** A formal $O_K$-module A is a commutative formal group law $F_f$ and an injective ring homomorphism $O_K \hookrightarrow End(F_f)$, $a \mapsto [a]_f$.

Note that $(m_L, +_f)$ is an abelian group for a finite extension L/K.

By the uniqueness idea in lemma 4.1, it can be shown that $(m_L, +_f)$ has a $O_K$-module structure with scalar multiplication $a.x = [a]_f(x)$, $\forall a \in O_K$ and $\forall x \in m_L$.

# Chapter V

## CONSTRUCTING ABELIAN EXTENSIONS

As we introduce Lubin-Tate formal groups, we are ready to give a construction of totally ramified abelian extensions of a local field K.

Let $\pi \in K$ be a prime element and $f \in F_\pi$. We know that the choice of f is not important. Let $\Lambda_f = m_K^s = \{\alpha \in K^s\} \mid |\alpha| < 1\}$. Note that $\forall \alpha, \beta \in \Lambda_f$, $F_f(\alpha, \beta) = \alpha +_F \beta$ converges to an element in $\Lambda_f$ and $\Lambda_f$ has an $O_K$-module structure with scalar multiplication $a.x = [a]_f(x)$.

Let $\Lambda_{f,n}$ be the subset of $\Lambda_f$ such that $\forall \alpha \in \Lambda_f$, $\alpha \in \Lambda_{f,n}$ if and only if $[\pi^n]_f(\alpha) = 0$.

$\Lambda_{f,n}$ is a submodule of $\Lambda_f$.

Let $\alpha,\ \beta \in \Lambda_{f,n}$. Then $[\pi^n]_f(\alpha +_f\ i_{F_f}(\beta)) = [\pi^n]_f(F_f(\alpha,\ i_{F_f}(\beta))$. As $[\pi^n]_f \in End(F_f)$, $[\pi^n]_f(F_f(\alpha,\ i_{F_f}(\beta)) = F_f([\pi^n]_f(\alpha),\ [\pi^n]_f(i_{F_f}(\beta))) = F_f(0,\ [\pi^n]_f(i_{F_f}(\beta))) = [\pi^n]_f(i_{F_f}(\beta)) = i_{F_f}([\pi^n]_f(\beta)) = 0$ (since $i_{F_f}$ also in $End(F_f)$, which is proven in lemma 3.2)

So $\Lambda_{f,n}$ is a subgroup, hence a submodule of $\Lambda_f$.

**Proposition 5.1:** The $O_K$-module $\Lambda_{f,n}$ is isomorphic to $O_K/(\pi^n)$. Hence, $End(\Lambda_{f,n}) \simeq O_K/(\pi^n)$ and $Aut(\Lambda_{f,n}) \simeq (O_K/(\pi^n))^x$.

*Proof.* Let $h : F_f \to F_g$ be an isomorphism. Then the diagram below commutes and h induces an isomorphism of $O_K$ modules $\Lambda_f \to \Lambda_g$.

$$\begin{array}{ccc} \Lambda_f & \xrightarrow{a \hookrightarrow F_f(a,0)} & F_f \\ \Big\downarrow {\scriptstyle a \to h(a)} & & \Big\downarrow {\scriptstyle h} \\ \Lambda_g & \xrightarrow{a \hookrightarrow F_g(a,0)} & F_g \end{array}$$

So the choice of f is not important. Let $f(X) = \pi X + X^q$. Observe that $f^{(n)}$ has finitely many roots. So, $\Lambda_{f,n}$ is finitely generated. Also, $\forall \alpha \in \Lambda_{f,n}$, $\pi^n.\alpha = 0$. Thus, $\Lambda_{f,n}$ is a torsion-module. Since $O_K$ is a PID, we can apply the structure theorem of finitely generated torsion-modules over a PID to $\Lambda_{f,n}$:
$\Lambda_{f,n} \simeq O_K/(\pi^{d_1}) \bigoplus O_K/(\pi^{d_2}) \bigoplus ... \bigoplus O_K/(\pi^{d_n})$, $d_1 \leq ... \leq d_n$

Observe that $f(X) = X(\pi + X^{q-1})$ and $g(X) = \pi + X^{q-1}$ is an Eisenstein polynomial. Let L be the splitting field of f. If $\alpha$ is a nonzero root of f, then $g(X) = Irr(\alpha, K)$, thus $v_L(\alpha) = \frac{1}{f(L/K,v_L)} v_K(N_{L/K}(\alpha)) = \frac{1}{f(L/K,v_L)} v_K(N_{L/K}(\pi)) > 0$. So all the roots of f lie in $\Lambda_f$. Hence, for $n = 1$, $\Lambda_{f,n}$ has q elements and by the structure theorem $\Lambda_{f,1} \simeq O_K/(\pi)$.
Assume that proposition 5.1 is true for n. Let $\varphi : \Lambda_{f,n+1} \to \Lambda_{f,n}$ given by $\alpha \mapsto \pi.\alpha$. We want to show that $\varphi$ is surjective.
Let $\beta \in \Lambda_{f,n}$. Consider the polynomial $f(X) - \beta = \pi X - X^q - \beta$. Then any root $\xi$ of this polynomial has a positive valuation. So, all roots of $f(X) - \beta$ is in $\Lambda_f$.

Observe that if $f(\xi) - \beta = 0$, then $f(\xi) \in \Lambda_{f,n}$, i.e. $\pi^n.f(\xi) = 0$, thus $f^{n+1}(\xi) = 0$. So, $\xi \in \Lambda_{f,n+1}$, i.e $\forall \beta \in \Lambda_{f,n}$, $\exists \xi \in \Lambda_{f,n+1}$ such that $\varphi(\xi) = \beta$. Therefore, $\varphi : \Lambda_{f,n+1} \to \Lambda_{f,n}$ is surjective and $ker\varphi = \{\alpha \in \Lambda_{f,n+1} \mid \pi.\alpha = 0\} = \Lambda_{f,1}$. Consider the exact sequence:

$$0 \to \Lambda_{f,1} \to \Lambda_{f,n+1} \to \Lambda_{f,n} \to 0$$

By induction hypothesis, $\Lambda_{f,n} \simeq O_K/(\pi^n)$. So, $|\Lambda_{f,n}| = q^n$. Since, $\Lambda_{f,n} \simeq \Lambda_{f,n+1}/\Lambda_{f,1}$, $|\Lambda_{f,n+1}| = q^{n+1}$. Then $\Lambda_{f,n+1} \simeq O_K/(\pi^n) \bigoplus O_K/(\pi)$ or $\Lambda_{f,n+1} \simeq O_K/(\pi^{n+1})$. The only way $\pi$ maps $\Lambda_{f,n+1}$ to $O_K/(\pi^n)$ is if $\Lambda_{f,n+1}$ contains $O_K/(\pi^{n+1})$ as its subgroup. Hence, $\Lambda_{f,n+1}$ is isomorphic to $O_K/(\pi^{n+1})$. $End(\Lambda_{f,n}) \simeq O_K/(\pi^{n+1})$ and $Aut(\Lambda_{f,n}) \simeq (O_K/(\pi^{n+1}))^x$ follows.

□

**Lemma 5.2:** Let $F \in O_K[[X_1, ..., X_n]]$ and L/K be finite, Galois with $Gal(L/K) = G$. Then, $\forall \alpha_1, ..., \alpha_n \in m_L$ and $\forall \sigma \in G$:
$\sigma F(\alpha_1, ..., \alpha_n) = F(\sigma\alpha_1, ..., \sigma\alpha_n)$.

*Proof.* If F is a polynomial, since $\sigma$ fixes K, the equality holds. Otherwise, let $F \equiv F_k \pmod{deg.\ k+1}$. As $|\sigma\alpha| = |\alpha|$, $\forall \sigma \in G$, $\sigma$ is continuous, so it preserves limits, i.e. if $\lim_{k\to\infty} \alpha_k = \alpha$, then $\lim_{k\to\infty} \sigma\alpha_k = \sigma(\lim_{k\to\infty} \alpha_k) = \sigma\alpha$. So, $\sigma F(\alpha_1, ..., \alpha_n) = \sigma \lim_{k\to\infty} F_k(\alpha_1, ..., \alpha_n) = \lim_{k\to\infty} \sigma F_k(\alpha_1, ..., \alpha_n) = \lim_{k\to\infty} F_k(\sigma\alpha_1, ..., \sigma\alpha_n) = F(\sigma\alpha_1, ..., \sigma\alpha_n)$. □

In particular Gal(L/K) act as an $O_K$-module isomorphism on $\Lambda_{f,n}$. Let $K_{\pi,n} = K[\Lambda_{f,n}]$ be the subfield of $K^s$ generated by $\Lambda_{f,n}$ over K. Note that for a given prime element $\pi \in K$, $\Lambda_f \simeq \Lambda_g$ as $O_K$-modules, $\forall f, g \in F_\pi$. Hence

$K_{\pi,n}$ is independent of the choice of f. Observe that $K_{\pi,n}$ is the splitting field of $f^n$, thus $K_{\pi,n}/K$ is Galois.

**Theorem 5.3:**

- $(i)$ *For each n,* $K_{\pi,n}$ *is totally ramified of degree* $(q-1)q^{n-1}$.
- $(ii)$ *The action of* $O_K$ *on* $\Lambda_{f,n}$ *defines an isomorphism* $(O_K/(\pi^n))^x \to Gal(K_{\pi,n}/K)$.
- $(iii)$ *For each n,* $\pi$ *is a norm from* $K_{\pi,n}$ *to* $K$.

*Proof.* As the choice of f is not important, let $f(X) = \pi X + X^q$ and $\alpha_1$ be a nonzero root of f. Construct a sequence of roots $\alpha_2, ..., \alpha_n$ such that $\alpha_i$ is a root of $f(X) - \alpha_{i-1}$. Since $f(\alpha_2) - \alpha_1 = 0$, $f^{(2)}(\alpha_2) = f(\alpha_1) = 0$. So $\alpha_2$ is a root of $f^{(2)}$ and $f(\alpha_2) \neq 0$ since $\alpha_1$ is nonzero. Inductively, it can be shown that each $\alpha_i$ is a root of $f^{(i)}$ and is not a root of $f^{(i-1)}$. Consider the sequence of fields:

$$K \subseteq K[\alpha_1] \subseteq ... \subseteq K[\alpha_n] \subseteq K[\Lambda_{f,n}]$$

(i)

The idea is to show $K[\alpha_1]/K$ and for each i, $K[\alpha_i]/K[\alpha_{i-1}]$ are totally ramified. Observe that $\alpha_1$ is the root of the Eisentein polynomial $g(X) = \pi + X^{q-1}$. So, $[K[\alpha_1] : K] = q - 1$. Since the norm of $\alpha_1$ over K is $\pi$, $v_{K[\alpha_1]}(\alpha_1) > 0$. Hence, $\alpha_1 \in m_{K[\alpha_1]}$. We claim that $(\alpha_1) = m_{K[\alpha_1]}$. Observe that $\pi = -\alpha_1^{q-1}$. So, $v_{K[\alpha_1]}(\pi) = (q-1)v_{K[\alpha_1]}(\alpha_1)$. If $\exists \alpha \in m_{K[\alpha_1]}$ such that $m_{K[\alpha_1]} = (\alpha)$, then $v_{K[\alpha_1]}(\alpha) \leq v_{K[\alpha_1]}(\alpha_1)$ (*) and $v_{K[\alpha_1]}(\pi) = n v_{K[\alpha_1]}(\alpha)$ where $q - 1 \leq n$ by (*). But, $n = e(K[\alpha_1]/K, v_{K[\alpha_1]}) \leq q-1$. So, $q-1 = n$ and $v_{K[\alpha_1]}(\alpha_1) = v_{K[\alpha_1]}(\alpha)$.

Therefore, $m_{K[\alpha_1]} = (\alpha_1)$.

As $v_{K[\alpha_1]}(\pi) = (q-1)v_{K[\alpha_1]}(\alpha_1)$ and $m_{K[\alpha_1]} = (\alpha_1)$, $e(K[\alpha_1]/K, v_{K[\alpha_1]}) = q-1 = [K[\alpha_1] : K]$, thus $K[\alpha_1]/K$ is totally ramified.

We want to show that $f(X) - \alpha_{i-1}$ is the irreducible polynomial of $\alpha_i$ over $K[\alpha_{i-1}]$. Just like in the case $i = 1$,by comparing valuations, one can prove inductively that $m_{K[\alpha_i]} = (\alpha_i)$ and $[K[\alpha_i] : K[\alpha_{i-1}]] = q = e(K[\alpha_i]/K[\alpha_{i-1}], v_{K[\alpha_i]})$. Hence, $f(X) - \alpha_{i-1}$ is Eisenstein over $K[\alpha_{i-1}])$ and $K[\alpha_i]/K[\alpha_{i-1}]$ is totally ramified. From this follows, $K[\alpha_i]/K$ is totally ramified and $[K[\Lambda_{f,n}] : K] \geq (q-1)q^{n-1}$ (1).
By definition, $K[\Lambda_{f,n}]$ is the splitting field of $f^{(n)}$. As $\Lambda_{f,n} = \{\alpha \in \Lambda_f \mid f_{(n)}(\alpha)\} = 0$, $Gal(K[\Lambda_{f,n}]/K)$ maps $\Lambda_{f,n}$ to itself. Therefore, $|Gal(K[\Lambda_{f,n}]/K)| \leq |Aut(\Lambda_{f,n})|$ $=|(O_K/(\pi^n))| = q^n - q^{n-1} = (q-1)q^{n-1}$, thus $[K[\Lambda_{f,n}] : K] \leq (q-1)q^{n-1}$ (2). By (1) and (2), $[K[\Lambda_{f,n}] : K] = (q-1)q^{n-1}$. So, $K[\Lambda_{f,n}] = K[\alpha_n]$, hence $K[\Lambda_{f,n}]/K$ is totally ramified of degree $(q-1)q^{n-1}$.

(ii)
By proposition 5.1, $Aut(\Lambda_{f,n}) \simeq (O_K/(\pi^n))^x$, thus $Gal(K[\Lambda_{f,n}]/K) \simeq (O_K/(\pi^n))^x$.

(iii)
Observe that $\alpha_n$ is a root of $(\frac{f(X)}{X}) \circ f^{(n-1)} = \pi + ... + X^{(q-1)q^{n-1}} \in O_K[X]$. Since, $[K[\alpha_n] : K] = (q-1)q^{n-1}$, $f(X) = Irr(\alpha_n, K)$. Hence $N_{K[\alpha_n]/K}(\alpha_n) = (-1)^{(q-1)q^{n-1}}\pi = \pi$.

□

Let $K_\pi = \cup K_{\pi,n}$. Then $Gal(K_\pi/K) = \varprojlim Gal(K_{\pi,n}/K) = \varprojlim((O_K/(\pi^n))^\times) = O_K^\times$. Recall that if $f \in F_\pi$ and $f' \in F_{\pi'}$ are isomorphic then they induce an $O_K$-module isomorphism between $\Lambda_{f,n}$ and $\Lambda_{f',n}$. Thus, $K_{\pi,n} \simeq K_{\pi',n}$ and $K_\pi \simeq K_{\pi'}$. However, in general this is not the case. If $\pi$ *and* $\pi'$ are distinct prime elements of K, then $K_{\pi,n} = K_{\pi',n}$ if and only if $\pi \equiv \pi' \pmod{m^n}$.

**Lemma 5.4:** Let $\pi, \pi'$ be prime elements of $\widehat{K^{ur}}$ and let $f \in F_\pi$ and $f' \in F_{\pi'}$ be power series in $\widehat{O_K^{ur}}$. Let $\phi \in \widehat{O_K^{ur}}[[X_1, ..., X_n]]$ be a linear form such that $\pi'\phi(X_1, ..., X_n) = \pi\phi^\varphi(X_1, ..., X_n)$. Then there exists a unique power series $\rho(X_1, ..., X_n) \in \widehat{O_K^{ur}}[[X_1, ..., X_n]]$ such that $\rho \equiv \phi \pmod{deg.\ 2}$ and $f' \circ \rho = \rho^\varphi \circ f$.

This lemma is proven in [1, pg. 47-49]. Observe that if we replace $\widehat{K^{ur}}$ with an unramified extension $K_n/K$ of degree n, then lemma 5.4 will still hold since completeness is the only thing we need in the proof, [1, pg. 49].

**Lemma 5.5:** For each $\mu \in 1 + m_K^n$, there exists a $\eta \in O_K^s$ such that $\eta\mu = \varphi(\eta)$.

*Proof.* The idea is to recursively construct an $\eta \in O_K^s$ satisfying $\eta\mu = \varphi(\eta)$. Let $\mu = 1 + \pi^n\zeta$ and $\eta = 1 + \pi\xi$ such that
$\frac{\varphi(\eta)}{\eta} = \frac{1+\varphi(\pi^n\xi)}{1+\pi^n\xi} \equiv 1 + \varphi(\pi\xi) - \pi\xi \pmod{\pi^{n+1}}$. Hence, we wish to solve the equation $\varphi(\pi^n\xi) - \pi^n\xi \equiv \pi^n\zeta \pmod{\pi^{n+1}}$. Let $\varphi(\pi^n) = \pi^n\theta$. Then, the above equation becomes $\pi^n\theta\varphi(\xi) - \pi^n\xi - \pi^n\zeta \equiv 0 \pmod{\pi^{n+1}}$. After reducing $\pi^n$, we get $\theta\varphi(\xi) - \xi - \zeta \equiv \theta\xi^q - \xi - \zeta \equiv 0 \pmod{\pi}$. As $\zeta \in O_K$,

$v_k(\zeta) \geq 0$. Since a root of the polynomial $\theta X^q - X - \zeta$ exists in $O_K^s$, $\exists \eta \in O_K^s$ such that $\eta\mu \equiv \varphi(\eta) \pmod{\pi^{n+1}}$. $\square$

**Proposition 5.6:** Let $\pi \equiv \pi' \pmod{m^n}$. Then, $K_{\pi,n} = K_{\pi',n}$.

*Proof.* Let $f' \in F_{\pi'}$, $f \in F_\pi$ and $\alpha' \in \Lambda_{f',n}$. Let $\eta$ be as in lemma 5.5. Then by lemma 5.4, $\exists \rho(X) \in O_K[[X]]$ such that $\rho(X) \equiv \eta X \pmod{deg.\ 2}$ and $f' \circ \rho = \rho^\varphi \circ f$. Observe that $\rho \circ F_f \equiv F_{f'} \circ \rho \equiv \eta(X+Y) \pmod{deg.\ 2}$. Also, as $F_{f'} \in O_K[[X]]$, $\varphi$ fixes the coefficients of $F_{f'}$, thus $f' \circ (F_{f'} \circ \rho) = F_{f'} \circ (f' \circ \rho) = F_{f'}^\varphi \circ (\rho^\varphi \circ f) = (F_{f'} \circ \rho)^\varphi \circ f$. Similarly, $f' \circ (\rho \circ F_f) = (\rho^\varphi \circ f) \circ F_f = (\rho^\varphi \circ F_f) \circ f = (\rho^\varphi \circ F_f^\varphi) \circ f = (\rho \circ F_f)^\varphi \circ f$. By uniqueness condition in lemma 5.4, $\rho \circ F_f = F_{f'} \circ \rho$, i.e. $\rho \in Hom(F_f, F_{f'})$.
Observe that $f'^{(n)} \circ \rho = \rho^{\varphi^n} \circ f^{(n)}$. Thus, $f'^{(n)}(\rho(\alpha)) = 0$ if and only if $f^{(n)}(\alpha) = 0$. Hence, $\Lambda_{f',n} = \rho(\Lambda_{f,n})$. So, $\exists \alpha \in \Lambda_{f,n}$ such that $\rho(\alpha) = \alpha'$.
Note that $f'(X) \equiv \pi' X \pmod{deg.\ 2}$ and $f'^\varphi = f'$, since $f'(X) \in O_K[[X]]$. Our claim is that $\rho$ maps $[\pi']_f$ to $f'$. In other words, we want to show $\rho \circ [\pi']_f = f' \circ \rho$, thus we are going to use the uniqueness of $\rho$.

(i) $\rho \circ [\pi']_f \equiv \eta\pi' X \equiv f' \circ \rho \pmod{deg.\ 2}$.
(ii) $f' \circ (\rho \circ [\pi']_f) = (\rho^\varphi \circ f) \circ [\pi']_f = (\rho^\varphi \circ [\pi']_f) \circ f = (\rho \circ [\pi']_f)^\varphi \circ f$, as $[\pi']_f \in O_K[[X]]$. Similarly, $f' \circ (f' \circ \rho) = f'^\varphi \circ (\rho^\varphi \circ f) = (f' \circ \rho)^\varphi \circ f$.

Hence, $\rho \circ [\pi']_f = f' \circ \rho$. Recall that $\pi' = \mu\pi$, thus $[\pi']_f = [\mu]_f \circ [\pi]_f$. So, $\rho \circ [\mu]_f \circ [\pi]_f = \rho \circ [\pi']_f = f' \circ \rho = \rho^\varphi \circ f = \rho^\varphi \circ [\pi]_f$. Therefore, $\rho \circ [\mu]_f = \rho^\varphi$.
Consider the map $\lambda : (O_K)^\times \twoheadrightarrow (O_K/(\pi^n))^\times$ given by $\alpha \mapsto \alpha \pmod{\pi^n}$. So, $ker\lambda = 1 + m_K^n$ and $(O_K)^\times/1 + m_K^n \simeq (O_K/(\pi^n))^\times \simeq Aut(\Lambda_{f,n})$. So, since

$\mu \in 1 + m_K^n$, $[\mu]_f$ acts trivially on $\Lambda_{f,n}$ and thus, $\rho(\alpha)^\varphi = \rho(\alpha)$, $\forall \alpha \in \Lambda_{f,n}$. As $K^{ur} \cap K_{\pi,n} = K$, $Frob_{K^{ur}/K}$ can be extended to an automorphism $\varphi$ of $K^{ur}.K_{\pi,n} = L_n$ such that $L^\varphi = K_{\pi,n}$. Since $\forall \alpha \in K_{\pi,n}$, $\rho^\varphi(\alpha) = \rho(\alpha)$, $\varphi$ fixes $\rho(\alpha) = \alpha'$. Therefore, $K_{\pi',n} \subseteq K_{\pi,n}$. For, $\mu^{-1}$, one can show that $K_{\pi',n} \supseteq K_{\pi,n}$. Hence, $K_{\pi',n} = K_{\pi,n}$. □

This proposition also gives that, $K_\pi/K$ and $K_{\pi'}/K$ are not isomorphic if $\pi \not\equiv \pi' \pmod{m_K^n}$ for some $n \in \mathbb{N}$. However, we are going to show that the choice of $\pi$ is unimportant for $L_\pi = K^{ur}.K_\pi$ over $K^{ur}$. In other words, K does not have a canonical maximal totally ramified abelian extension but $K^{ur}$ does.

Since $K^{ur} \cap K_\pi = K$, $Gal(L_\pi) = Gal(K^{ur}/K) \times Gal(K_\pi/K)$. Now consider the homomorphism

$$\phi_\pi : K^x \to Gal(L_\pi/K) \simeq Gal(K^{ur}/K) \times Gal(K_\pi/K)$$

$$\mu\pi^n \mapsto (Frob^n, [\mu^{-1}]_f)$$

Our goal is to show that the extensions $K^{ur}.K_{\pi,n}$ are independent of the choice of $\pi$. To prove this, we need to show that $F_f$ and $F_{f'}$ are isomorphic over $O_K^{ur}$, and thus, $\Lambda_{f,n}$ are isomorphic $\Lambda_{f',n}$ as $O_K^{ur}$-modules. Note that $K^{ur}$ is not complete in general, so power series evaluated at $m^{ur}$ may not converge. Therefore, we are going to work over $\widehat{K^{ur}}$ instead. Since any $\sigma \in Gal(K^{ur}/K)$ preserves the valuation, $\sigma$ is an isometry, i.e. it is continuous. So it can be extended to $\widehat{K^{ur}}$.

**Lemma 5.7:** $\exists \rho \in \widehat{O_K^{ur}}[[X]]$ such that

(i) $\rho(X) \equiv \eta X \pmod{deg.\ 2}$ for some unit $\eta$

(ii) $\rho^{\varphi} = \rho \circ [\mu]_f$ *where* $\varphi(\eta) = \mu\eta$

(iii) $\rho \circ F_f = F_{f'} \circ \rho$

(iv) $\rho \circ [a]_f = [a]_{f'} \circ \rho$ for all $a \in O_K$, which is an immediate result of (iii) and proposition 4.3.

Since $\eta$ is a unit, by (i) and (iii), $F_f \simeq F_{f'}$ over $\widehat{K^{ur}}$. So, $\widehat{K^{ur}}.K_{\pi,n} \simeq \widehat{K^{ur}}.K_{\pi',n}$ and thus, the choice of $\pi$ is unimportant for $L_\pi = \widehat{K^{ur}}.K_\pi$ and $\widehat{K^{ur}.K_\pi} = \widehat{K^{ur}.K_{\pi'}}$ follows.

**Lemma 5.8:** Let E be an algebraic extension of K in $K^s$ and $\hat{E}$ be its completion. Then $K^s \cap \hat{E} = E$.

*Proof.* Let $\sigma \in Gal(K^s/E)$. Then $\sigma$ fixes E. But we know that $\sigma$ is continuous since it preserves valuations. So by continuity, $\sigma$ also fixes $K^s \cap \hat{E}$. Then $K^s \cap \hat{E} \subseteq E$. But $K^s \cap \hat{E} \supseteq E$, thus, $K^s \cap \hat{E} = E$. □

**Theorem 5.9:** $L_\pi$ and $\phi_\pi$ is independent of the choice of $\pi$.

*Proof.* Recall that $\rho(\Lambda_{f,n}) = \Lambda_{f',n}$. So,

$$\widehat{K^{ur}}[\Lambda_{f',n}] = \widehat{K^{ur}}[\rho(\Lambda_{f,n})] \subseteq \widehat{K^{ur}}[\Lambda_{f,n}] = \widehat{K^{ur}}[\rho^{-1}(\Lambda_{f',n})] \subseteq \widehat{K^{ur}}[\Lambda_{f,n}]$$

Hence, $\widehat{K^{ur}}[\Lambda_{f',n}] = \widehat{K^{ur}}[\Lambda_{f,n}]$. If we apply lemma 5.7 to $K^{ur}[\Lambda_{f',n}]$ and

$K^{ur}[\Lambda_{f,n}]$,

$$\widehat{K^{ur}}[\Lambda_{f',n}] \cap K^s = K^{ur}[\Lambda_{f',n}],\ \widehat{K^{ur}}[\Lambda_{f,n}] \cap K^s = K^{ur}[\Lambda_{f,n}]$$

Therefore, $L_{\pi'} = K^{ur}[\Lambda_{f',n}] = K^{ur}[\Lambda_{f,n}] = L_{\pi}$.

To show that $\phi_\pi$ is independent of the choice of $\pi$, we are going to show that $\phi_\pi(\pi') = \phi_{\pi'}(\pi')$. So, for any uniformizers $\pi, \pi', \varpi \in K$, $\phi_\pi(\pi') = \phi_{\pi'}(\pi') = \phi_\varpi(\pi')$ and $\phi_\pi = \phi_\varpi$ follows since $K^\times$ is generated by the set of uniformizers.

Recall that $\phi_\pi : K^\times \to Gal(K^{ur}/K) \times Gal(K_\pi/K)$ given by the map $\pi^n\mu \mapsto (\varphi^n, [\mu^{-1}]_f)$. So, both $\phi_\pi(\pi')$ and $\phi_{\pi'}(\pi')$ induce $\varphi$ on $K^{ur}$, thus we only need to check the automorphism they give on $K_{\pi'}$. Note that $\phi_{\pi'}(\pi') = [1^{-1}]_{f'}$ is the identity on $K_{\pi'}$. So we want to show that $\phi_\pi(\pi')$ is the identity on $K_{\pi'}$. Let $f \in F_\pi$ and $f' \in F_{\pi'}$. Recall that $\exists \rho(X) \in \widehat{O_K^{ur}[[X]]}$ such that $\rho : F_f \to F_{f'}$ is an isomorphism over $\widehat{K^{ur}}$ and $\rho(\Lambda_{f,n}) = \Lambda_{f',n}$. So, to show that $\phi_\pi(\pi')$ is the identity on $K_{\pi'}$, we need to prove that $\phi_\pi(\rho(\alpha)) = \rho(\alpha)$, for all $\alpha \in \Lambda_{f,n}$ for all n. We know that $\phi_\pi(\pi) = (\varphi, [1^{-1}]_f)$ and $\phi_\pi(\mu) = (id, [\mu^{-1}]_f)$ on $Gal(K^{ur}/K) \times Gal(K_\pi/K)$. Since both $\phi_\pi(\pi)$ and $\phi_\pi(\mu)$ preserves the valuation on $K^{ur}$, they are continuous and can be extended to $\widehat{K^{ur}}$. Since, $\pi' = \mu\pi$, $\phi_\pi(\pi') = \phi_\pi(\mu)\phi_\pi(\pi)$ and $\rho(X) \in \widehat{O_K^{ur}}$, by lemma 5.5,

$$\begin{aligned}\phi_\pi(\pi')(\rho(\alpha)) &= \phi_\pi(\mu)\phi_\pi(\pi)(\rho(\alpha)) = (\phi_\pi(\pi)(\rho))(\phi_\pi(\mu)(\alpha)) \\ &= \rho^\varphi([\mu^{-1}]_f(\alpha)) = \rho(\alpha)\end{aligned}$$

Hence, $\phi_\pi(\pi') = \phi_{\pi'}(\pi')$ and $\phi_\pi$ is independent of the choice of $\pi$.

□

## BIBLIOGRAPHY

[1] K. Iwasawa, Local Class Field Theory, Oxford University Press, New York, 1986.

[2] J. Milne, Class Field Theory, http://www.jmilne.org/math, 1997.

[3] I.B. Vesenko, S.V. Vostokov, Local Fields and Their Extensions $http://sci-lib.org/books\_1/F/fesenko.pdf$, 2001.

[4] H. Matsumura, Commutative Ring Theory, http://www.math.unam.mx/javier/Matsumura.pdf.

[5] J.P. Serre, Local Fields, Springer-Verlag, New York, 1979.

## VITA

Jale Dinler was born in Adana on *9th* of September, 1986. She received a B.Sc. degree in 2009 in Computer Engineering from Boğaziçi University, İstanbul, Turkey. Then, she started M.Sc. program in Mathematics at Koç University, İstanbul. She has studied Number Theory under supervision of Asst. Prof. Dr. Kazım Büyükboduk since 2011.