國立臺灣大學理學院數學系

硕士論文

Department of Mathematics
College of Science
National Taiwan University

Master Thesis

局部體上形式群之跡映射

Trace Maps for Formal Groups over Local Fields

李彥穎
Yen-Ying Lee

指導教授：陳其誠 博士

Advisor: Ki-Seng Tan, Ph.D.

中華民國 99 年 6 月

June, 2010

誌謝

首先要先感謝我的指導教授陳其誠老師在這兩年來的指導。對於資質駑鈍的我，總是不厭其煩地為我解答學業上的疑問，且在生活上也給予我許多的建議和指導。另外要感謝幫我口試的教授：美麗的陳燕美老師和帥氣的謝銘倫老師。在中央和台大求學的時候，曾經修過兩位老師的課，學習到許多關於數論的知識。

感謝許多系上學長姐以及學弟妹，在這兩年的研究所期間，因為有你們，所以一路上走得順利許多。一同努力的同學們，家豪、佳原、君羊、硯仁、裕元、宇揚，感謝你們這兩年來，無論是在修課、讀書會或是一些飯後閒聊，到後來的論文寫作還有口試準備時的幫忙，都給予我很大的幫助。

最後，我要感謝我的父母，在我大學指考分發選擇校系時，對我選擇就讀數學系的決定給予支持，更一直在背後支撐我念完研究所，真的很感謝你們，我愛你們。

摘要

本篇論文主要是探討局部體上形式群的跡映射的性質，以及它在阿貝爾簇上的應用。

關鍵字：跡映射　形式群　局部體　阿貝爾簇

Abstract

In this paper, we discuss properties of trace maps for formal groups over local field and their application to abelian varieties.

Keywords:trace map, formal group, local field, abelian variety

Contents

Trace Maps for Formal Groups over Local Fields

Yen-Ying Lee

1 Introduction

Consider a complete local field F that is either a finite extension of $\mathbb{Q}_p$ or the field of fraction of the formal power series ring $\mathbb{F}[[t]]$ over a finite field $\mathbb{F}$ of characteristic p. Let A be an abelian variety defined over F and let K/F be a $\mathbb{Z}_p$-extension. A celebrated theorem of Mazur says if A has good ordinary reduction and $char.(F) = 0$, then

$$|\mathrm{H}^1(\mathrm{Gal}(K/F), A(K))| < \infty \tag{1.1}$$

and the bound can be given in terms of the reduction of A ([2], Proposition 4.3.9). The proof is mainly based on analysing the p-divisible group of the associated formal group $\mathscr{F}$ (the kernel of the reduction).

In the process of time, there has been generalizations of the theorem as well as simplifications of the proof. For instance, under the condition that A has good ordinary reduction, Tan [5] shows that the theorem holds for every $\mathbb{Z}_p^d$-extension over every local field, Coates and Greenberg [1] extends the theorem to the case where $char.(F) = 0$ and K/F is a deeply ramified extension. Here we have to remind the reader that every (pro-finite) Galois extension K/F such that the Galois group is a p-adic Lie group is deeply ramified (Theorem 2.13, [1]). There is a common feature in both works. Indeed, to deduce (1.1), they both prove, under their own conditions, the equality

$$\mathrm{H}^1(F, \mathscr{F}) = \mathrm{H}^1(\mathrm{Gal}(K/F), \mathscr{F}(m_K)), \tag{1.2}$$

where m_K denote the maximal ideal of (the ring of integers) of K.

The work of [1] is truly ingenious, as it depends only on well-known ramification theory while its result is much more general than others. It proves that (1.2) holds if $\mathscr{F}$ is any commutative formal group over F and K/F is deeply ramified. The only drawback is it is limited to the condition that F is of characteristic zero. Considering this, one might wonder if it is possible to carry over the theory to the characteristic p case. It turns out that after some modification, the theory of deeply ramification can also be established in characteristic p so that every ramified $\mathbb{Z}_p^d$-extension is deeply ramified and (1.2) holds for every commutative formal group $\mathscr{F}$ and every deeply ramified extension K/F. This is described in [6], in which one can also find the following surprising consequence:

***Theorem* 1.1.** *Let F be a local field of characteristic p and let A/F be an abelian variety having super-singular reduction. If K/F is a ramified $\mathbb{Z}_p$-extension, then*

$$\mathrm{H}^1(\mathrm{Gal}(K/F), A(K)) \simeq \bigoplus_{i=1}^{\infty} \mathbb{Q}_p/\mathbb{Z}_p \times T,$$

where T is a finite group.

The aim of this thesis is two-fold: (1) to check, step by step, all details to make sure the related assertions in [6] hold, and then, (2) to provide a convenient access to the detailed documentation of the theory. The content of the thesis is as follows.

Suppose F'/F is a finite extension. Then certainly $\mathrm{Tr}_{F'/F}(m_{F'}) \subset m_F$ and in a way, the size of $\mathrm{Tr}_{F'/F}^{-1}(m_F)/m_{F'}$ (which is related to the different) measures the depth of ramification of the extension. Roughly speaking, an extension K/F is deeply ramified if the trace map $m_{KF'} \longrightarrow m_K$ is surjective, for every F'. Thus, the ramification of F'/F is kind of "absorbed" in that of K/F. In general, we can write

$$F \subset F_1 \subset F_2 \subset \cdots \subset F_n \subset \cdots \subset F_\infty = K,$$

where each F_n/F is a finite extension. Write $F'_n = F'F_n$. Then $m_K = \bigcup_n m_{F_n}$. Also, an $x \in m_{F_n}$ is contained in $\mathrm{Tr}_{KF'/K}(m_{KF'})$ if and only if $x \in \mathrm{Tr}_{F'_k/F_k}(m_{F'_k})$, for some $k \geq n$. K/F is deeply ramified means not only such k exists for each x, but also a lower bound of k can be given explicitly in terms of n as well as the valuation of x.

An immediate application of the theory is that if K/F is deeply ramified, then for every formal group $\mathscr{F}$ over F and every finite extension K'/K, the trace map

$$\mathscr{N}_{K'/K} : \mathscr{F}(m_{K'}) \longrightarrow \mathscr{F}(m_K)$$

is surjective. In particular, if K'/K is a cyclic extension, then we have

$$\mathrm{H}^2(\mathrm{Gal}(K'/K), \mathscr{F}(m_{K'})) = 0.$$

Then further computation shows

$$\mathrm{H}^1(\mathrm{Gal}(K'/K), \mathscr{F}(m_{K'})) = 0,$$

for cyclic extension. By applying the inflation-restriction exact sequence as well as the fact that $\mathscr{F}(m_{K'})$ is a p-group, we deduce that the above holds for every Galois extension K'/K, and hence (1.2) holds, as $\mathrm{H}^1(K, \mathscr{F}(m_{\bar{K}}))$ is the direct limit of $\mathrm{H}^1(\mathrm{Gal}(K'/K), \mathscr{F}(m_{K'}))$.

We organize this thesis in the following way. The theory of deeply ramification in characteristic p is established in Chapter 1. In chapter 2, the trace map of a formal group is studied and (1.2) is proved . Then the result is applied in Chapter 3 to prove Theorem 1.1.

2 Deeply Ramified Extension

Most material of this section are from [1] and [3], except some modification that are mostly from [6]. From now on, we assume $char.(F) = p$. In this section, every field extension F is assume to a separable algebraic extension. In particular, if L is a field extension F, then it is the union of its finite intermediate extensions, and hence the valuation ord_F on F can be uniquely extended to L. Also, if L/F is finite, then it had its own valuation ord_L that has value 1 at every prime element. We have

$$\mathrm{ord}_L = e(L/F)\,\mathrm{ord}_F,$$

where $e(L/F)$ denotes the ramification index. Let $\mathcal{O}_L$, m_L and l denote the ring of integers of L, the maximal ideal and the residue field.

2.1 Ramification groups

Let L/F be a finite Galois extension with $\mathrm{Gal}(L/F) = G$. We may write $\mathcal{O}_L = \mathcal{O}_F[x]$, $x \in L$, as a $\mathcal{O}_F$-algebra ([3], III.6, Proposition 12).

Lemma 2.1. *Let $i \in \mathbb{Z}$, $i \geq -1$ and $g \in G$. The following are equivalent:*

(a) *g operates trivially on $\mathcal{O}_L/m_L^{i+1}$.*

(b) $\mathrm{ord}_L(gv - v) \geq i + 1$, *for all $v \in \mathcal{O}_L$.*

(c) $\mathrm{ord}_L(gx - x) \geq i + 1$.

Proof. For (a)$\Longleftrightarrow$(b): Take $v \in \mathcal{O}_L$. Then

$$\begin{aligned} g\bar{v} = \bar{v} \quad &\Longleftrightarrow \quad gv - v \in m_L^{i+1} \\ &\Longleftrightarrow \quad \mathrm{ord}_L(gv - v) \geq i + 1 \end{aligned}$$

For (a)$\Longleftrightarrow$(c): Let x_i be the image of x in $\mathcal{O}_L/m_L^{i+1}$. Then $gx_i = x_i$ if and only if $\mathrm{ord}_L(gx - x) \geq i + 1$. □

Proposition 2.2. *For each $i \geq -1$, let $G_{(i)}$ be the set of g satisfied the conditions in* Lemma 2.1. *Then the $G_{(i)}$ form a decreasing sequence of normal subgroups of G. In particularly, $G_{(-1)} = G$, $G_{(0)}$ is the inertia subgroup of G and $G_{(i)} = \{1\}$ for $i \gg 1$.*

Proof. That $G_{(i)}$ a normal subgroup is from the conditional (a) in Lemma 2.1. Others are just from the definition. □

Definition. The *i-th lower-numbering ramification group of* $G = \mathrm{Gal}(L/F)$ is the set of g satisfying the conditions in Lemma 2.1.

Remark. Suppose $H \subset G$ and $F' = L^H$. Then

$$H_{(i)} = G_{(i)} \cap H.$$

The lower-numbering is compatible with taking sub-group.

Definition. The *Herbrand function* $\phi_{L/F} : [-1, \infty) \longrightarrow [-1, \infty)$ is defined as

$$\phi_{L/F}(u) = \begin{cases} \displaystyle\int_0^u \frac{1}{[G_{(0)} : G_{(t)}]}\, dt, & 0 \leq u; \\ u, & -1 \leq u \leq 0. \end{cases}$$

Also, let $\psi_{L/F}$ denote the inverse function of $\phi_{L/F}$.

***Lemma* 2.3.** *Denote* $i_G(s) = \mathrm{ord}_L(sx - x)$. *Then*

$$\phi_{L/K}(u) = -1 + \frac{1}{e(L/F)} \sum_{s \in G} \inf(i_G(s), u+1).$$

Proof. If $u = 1$, then both sides equal -1. Suppose $u > -1$. Let $n \geq 0$ denote the integer such that $n - 1 < u \leq n$ and write $g_m = |G_m|$. Then

$$\begin{aligned} R.H.S &= -1 + \frac{1}{g_0} \sum_{m=1}^{n-1} (g_m - g_{m+1})(m+1) + \frac{g_n}{g_0}(u+1) \\ &= \sum_{m=1}^{n-1} \frac{g_m}{g_0} + \frac{g_n}{g_0}(u + 1 - n) \\ &= \phi_{L/K}(u) \end{aligned}$$

□

***Definition*.** Define the *upper-numbering ramification group* as

$$G^{(v)} := G_{(u)},$$

with $v = \phi_{L/F}(u)$.

Remark. Let M/F be a Galois intermediate extension of L/F and let $H = \mathrm{Gal}(L/M)$. Then we have $\phi_{M/F} \circ \phi_{L/M} = \phi_{L/F}$ and $\psi_{L/M} \circ \psi_{M/F} = \psi_{L/F}$. Consequently, the upper-numbering is compatible with Galois quotient in the sense that

$$G^{(v)}H/H = (G/H)^{(v)}.$$

Let G_F denote the Galois group $\mathrm{Gal}(\bar{F}/F)$ where $\bar{F}$ is a fixed separable closure of F. By the above compatible property, we can define the upper-numbering ramification groups $G_F^{(v)} \subset G_F$ as the projective limit of $\mathrm{Gal}(L/F)^{(v)}$ for L running over all finite Galois extension of F. Then we denote $F^{(v)} = \bar{F}^{G_F^{(v)}}$.

2.2 The different and the conductor

Let L/F be a finite extension and let $\delta_{L/F}$ the different of L/F. Also, let $\mathcal{O}_L = \mathcal{O}_F[x]$ and let $f(X)$ be the minimal polynomial of x over F.

***Lemma* 2.4.** *Suppose* L/F *is an Galois extension with* $G = \mathrm{Gal}(L/F)$. *Then*

$$\mathrm{ord}_L(\delta_{L/F}) = \int_{-1}^{\infty} (g_{(u)} - 1)\, du.$$

Proof. It is from the following:

$$\begin{aligned}
\mathrm{ord}_L(f'(x)) &= \sum_{s\in G, s\neq \mathrm{id}} \mathrm{ord}_L(sx-x) \\
&= \sum_{m=-1}^{N} (g_{(m)} - g_{(m+1)})(m+1), \text{ for } N \gg 0 \\
&= \sum_{m=-1}^{\infty} (g_{(m)} - 1) \\
&= \int_{-1}^{\infty} (g_{(u)} - 1)\, du.
\end{aligned}$$

□

The following relates the different to the upper-numbering ramification.

***Proposition* 2.5.** *Suppose L/F is a finite extension. Then*

$$\mathrm{ord}_L(\delta_{L/F}) = e(L/F) \int_{-1}^{\infty} 1 - \frac{1}{[L : L \cap F^{(v)}]}\, dv.$$

Proof. First, assume that L/F is a Galois extension and $G = \mathrm{Gal}(L/F)$. Then $L \cap F^{(v)} = L^{G^{(v)}}$ and $[L : L \cap F^{(v)}] = |G^{(v)}|$. Since $v = \phi_{L/F}(u)$, $dv = \frac{1}{[G_{(0)} : G_{(u)}]} du$, the change of variable together with Lemma 2.4 imply

$$\begin{aligned}
\mathrm{ord}_L(\delta_{L/F}) &= \int_{-1}^{\infty} (g_{(u)} - 1)\, du \\
&= \int_{-1}^{\infty} (|G^{(v)}| - 1)[G^{(0)} : G^{(v)}]\, dv \\
&= e(L/F) \int_{-1}^{\infty} 1 - \frac{1}{|G^{(v)}|}\, dv \\
&= e(L/F) \int_{-1}^{\infty} 1 - \frac{1}{[L : L \cap F^{(v)}]}\, dv
\end{aligned}$$

In general, let M/F be a Galois extension containing L and let $G = \mathrm{Gal}(M/F)$, $H = \mathrm{Gal}(M/L)$ and $h_{(u)} = |H_{(u)}|$. From the multiplicative property of different, we have $\delta_{M/F} = \delta_{M/L} \cdot \delta_{L/F}$. Then

$$\begin{aligned}
\mathrm{ord}_M(\delta_{L/M}) &= \mathrm{ord}_M(\delta_{M/F})) - \mathrm{ord}_M(\delta_{M/L}) \\
&= \int_{-1}^{\infty} g_{(u)} - h_{(u)}\, du \\
&= \int_{-1}^{\infty} g_{(u)} - |H \cap G_{(u)}|\, du \\
&= \int_{-1}^{\infty} ([M : M \cap F^{(v)}] - [M : (M \cap F^{(v)})L])[G^{(0)} : G^{(v)}]\, dv \\
&= e(M/F) \int_{-1}^{\infty} 1 - \frac{1}{[(M \cap F^{(v)})L : M \cap F^{(v)}]}\, dv.
\end{aligned}$$

Then the proposition is proved, since $[(M \cap F^{(v)})L : M \cap F^{(v)}] = [L : L \cap F^{(v)}]$, $\mathrm{ord}_M(\delta_{L/F}) = \mathrm{ord}_L(\delta_{L/F}) \cdot e(M/L)$ and $e(M/F) = e(M/L) \cdot e(L/F)$. □

Definition. For any finite extension L over F, the *conductor* $f(L/F)$ is defined to be the infimum of all $w \in [-1, \infty)$ such that $L \subset F^{(w-1)}$.

By Hasse-Arf Theorem ([3], IV.4), if L/F is a finite abelian extension, if v is a jump in the filtration $G^{(v)}$, then v must be an integer. In this case, the conductor $f(L/F)$ is an integer. Furthermore, if

$$U_F^{(i)} = \begin{cases} \mathcal{O}_F^*, \text{ if } i = 0 \\ 1 + \pi^i \mathcal{O}_F, \text{ if } i > 0. \end{cases}$$

where π is a uniformizer of F, then the reciprocity map

$$F^* \longrightarrow G = \mathrm{Gal}(L/F)$$

sends $U_F^{(w)}$ onto $G^{(w)}$ (XV.2, [3]). Therefore, the conductor $f(L/F)$ is indeed the smallest *integer* w enjoying the property $U_F^{(w)} \subset \mathrm{N}_{L/F}(L^*)$ (see XV.2, [3]).

***Corollary* 2.6.** *Let L be a finite extension of F. Then*

$$\frac{e(L/F)f(L/F)}{2} \leq \mathrm{ord}_L(\delta_{L/F}) \leq e(L/F)f(L/F).$$

Proof. If $w > f(L/F) - 1$, then $F^{(w)} \cap L = L$. Therefore, Proposition 2.5 implies

$$\begin{aligned}
\mathrm{ord}_L(\delta_{L/F}) &= e(L/F) \int_{-1}^{f(L/F)-1} (1 - \frac{1}{[L : L \cap F^{(w)}]})\, dw \\
&\leq e(L/F)(f(L/F) - 1 - (-1)) \cdot 1 \\
&= e(L/F)f(L/F).
\end{aligned}$$

On the other hand, if $w < f(L/F) - 1$, then $[L : L \cap F^{(w)}] \geq 2$, and hence

$$\begin{aligned} \mathrm{ord}_L(\delta_{L/F}) &\geq e(L/F) \int_{-1}^{f(L/F)-1} \frac{1}{2}\, dw \\ &= e(L/F) \frac{f(L/F)}{2}. \end{aligned}$$

□

The following classical lemma will be frequently used.

***Lemma* 2.7.** *Suppose L/F is a finite extension and let $b(L/F)$ denote the integral part of* $\mathrm{ord}_L(\delta_{L/F})/e(L/F)$. *Then*

$$\mathrm{Tr}_{L/F}(\mathcal{O}_L) = m_F^{b(L/F)}.$$

Proof. For simplicity, write $t = b(L/F)$. Let ϖ_F denote a uniformizer of F. Since $t \cdot e(L/F) \leq \mathrm{ord}_L(\delta_{L/F})$, we have

$$\varpi_F^t \mathcal{O}_L \supset \delta_{L/F},$$

which tells us that

$$\mathrm{Tr}_{L/F}(\mathcal{O}_L) \subset \varpi_F^t \mathcal{O}_F.$$

On the other hand, we have

$$(t+1) \cdot e(L/F) > \mathrm{ord}_L(\delta_{L/F})$$

that implies

$$\mathrm{Tr}_{L/F}(\mathcal{O}_L) \not\subseteq \varpi_F^{t+1} \mathcal{O}_F.$$

□

2.3 Deeply ramified extensions and trace maps

Let K be a (possibly infinite) extension of F. We say that K has *finite conductor* over F if $K \subset F^{(w)}$ for some fixed $w \in [-1, \infty)$.

***Proposition* 2.8.** *The following assertions are equivalent:*

(a) *K has finite conductor over F*

(b) *As F' runs over all finite intermediate extension of K/F,* $\mathrm{ord}_F(\delta_{F'/F})$ *is bounded*

.

Remark. From the multiplicative of the different, we can see from (b) that the proposition implies that K has finite conductor over F if and only if K has finite conductor over some finite intermediate extension F'.

Proof. First, we assume that K has finite conductor over F, that is $K \subset F^{(u)}$ for some $u \in [-1, \infty)$, or equivalently $f(F'/F) \leq u+1$ (that is equivalent to $F' \subset F^{(u)}$), for all finite intermediate extensions F' of K/F. From Corollary 2.6, we have

$$\begin{aligned} \mathrm{ord}_F(\delta_{F'/F}) &= \frac{\mathrm{ord}_{F'}(\delta_{F'/F})}{e(F'/F)} \\ &\leq \frac{e(F'/F)f(F'/F)}{e(F'/F)} \\ &= f(F'/F) \\ &\leq u+1. \end{aligned}$$

On the other hand, if $\mathrm{ord}_F(\delta_{F'/F})$ is bounded by C, then Corollary 2.6 also implies

$$\begin{aligned} f(F'/F) &\leq \frac{2\,\mathrm{ord}_{F'}(\delta_{F'/F})}{e(F'/F)} \\ &= 2\,\mathrm{ord}_F(\delta_{F'/F}) \\ &\leq 2C. \end{aligned}$$

Therefore, every F' is contained in $F^{(w)}$ for $w > 2Ce(F)$, and hence K is contained in $F^{(w)}$, too. □

We are mostly interested in the case where K does not have finite conductor. Such K must be an infinite extension of F. Since K/F is algebraic (hence pro-finite), we can write

$$K = \bigcup_{n=0}^{\infty} F_n, \quad F_n \subseteq F_{n+1}, \text{ for all } n \geq 0,\ [F_n : F] < \infty \tag{2.1}$$

From now on, we will choose and fix such F_n, $n = 0, 1, ...$ for a given K/F. In particular, if L/F is a $\mathbb{Z}_p$-extension and L_n denotes its nth layer, then we choose $F_n = L_n$, $n = 0, 1, ...$ for L.

Lemma 2.9. *Suppose L/F is a ramified $\mathbb{Z}_p$-extension. Then*

$$\mathrm{ord}_F(\delta_{L_n/F}) = \mathrm{ord}_{L_n}(\delta_{L_n/F})/e(L_n/F) \to \infty \text{ as } n \to \infty.$$

Proof. Write $G = \mathrm{Gal}(L/F)$ and $G_n = \mathrm{Gal}(L_n/F)$. Let $\{U^{(w)}\}$ be the filtration of $\mathcal{O}_F^*$ described in Section 2.2.

For a continuous character $\chi : G \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$ (where $\mathbb{Q}_p/\mathbb{Z}_p$ is endowed with the discrete topology), let $f(\chi)$ denote its conductor, that is the smallest integer w enjoying the property $U^{(w)} \subset \ker(\chi)$. In view of the equalities $(1+x)^p = 1+x^p$ and $\chi^p(g) = \chi(g^p)$, we see that

$$pf(\chi^p) \leq f(\chi).$$

Let π be a uniformizer of F and let $\pi^{\Delta_n}\mathcal{O}_F$ denote the discriminant of L_n/F. Also, let $\chi_1 : G_n \longrightarrow \mathbb{C}^*$ be a primitive character in the sense that every character of G_n is some of its powers. From the conductor-discriminant formula, we see that as $n \to \infty$,

$$\begin{aligned}
\Delta_n &= (p^n - p^{n-1})f(\chi_1) + (p^{n-1} - p^{n-2})f(\chi_1^p) + \cdots + f(\chi_1^{p^n}) \\
&\geq (p^n - p^{n-1})pf(\chi_1^p) + (p^{n-1} - p^{n-2})f(\chi_1^p) + \cdots + f(\chi_1^{p^n}) \\
&\geq (p^n - p^{n-1})p^n f(\chi_1^{p^n}) + (p^{n-1} - p^{n-2})f(\chi_1^p) + \cdots + f(\chi_1^{p^n}) \\
&= C_1 p^{2n} + O(p^{2n-1}), \text{ for some positive constant } C_1.
\end{aligned}$$

Consequently,

$$\mathrm{ord}_F(\delta_{L_n/F}) \geq C_2 p^n + O(p^{n-1}), \text{ for some positive constant } C_2.$$

□

Proposition 2.10. *Assume that K has finite conductor. Then there exist finite cyclic extension K' of K such that $\mathrm{Tr}_{K'/K}(m_{K'}) \neq m_K$.*

Proof. Claim 1: There exist an integer $b \geq 0$, such that for n sufficiently large,

$$\mathrm{Tr}_{F_n/F}(\mathcal{O}_{F_n}) = m_F^b. \tag{2.2}$$

Let

$$r_n = \mathrm{ord}_F(\delta_{F_n/F}) = \frac{\mathrm{ord}_{F_n}(\delta_{F_n/F})}{e(F_n/F)}.$$

Proposition 2.8 says that r_n is bounded. Also, let b_n be the integral part of r_n. Then from Lemma 2.7, we see that

$$\mathrm{Tr}_{F_n/F}(\mathcal{O}_{F_n}) = m_F^{b_n},$$

and hence b_n increases with n. Since it is bounded, the claim is proved.

Choose a ramified $\mathbb{Z}_p$-extension Φ/F and let Φ_t denote its t-th layer.

Claim 2: There exist some positive integers t and n_0 so that if $F'_n = F_n\Phi_t$, then

$$\mathrm{Tr}_{F'_n/F_n}(m_{F'_n}) \subset m_F m_{F_n}, \text{ for all } n \geq n_0.$$

Take $K' = K\Phi_t$. Then $m_{K'} = \cup m_{F'_n}$, and hence Claim 2 implies

$$\mathrm{Tr}_{K'/K}(m_{K'}) \subset m_F m_K.$$

This proves the proposition.

To prove the claim, we choose n_0 so that (2.2) hold for $n \geq n_0$ and we choose t so that $\mathrm{ord}_F(\delta_{\Phi_t/F}) \geq b+3$. The existence of such t is due to Lemma 2.9. Lemma 2.7 says that $\mathrm{Tr}_{\Phi_t/F}(m_{\Phi_t}) \subset m_F^{b+3}$, and hence

$$\mathrm{Tr}_{F'_n/F}(m_{F'_n}) \subset \mathrm{Tr}_{\Phi_t/F}(m_{\Phi_t}) \subset m_F^{b+3}.$$

Suppose Claim 2 were false for some $n \geq n_0$. As $\mathrm{Tr}_{F'_n/F_n}(m_{F'_n})$ is an ideal of $\mathcal{O}_{F_n}$, we have

$$\mathrm{Tr}_{F'_n/F_n}(m_{F'_n}) \supseteq m_F m_{F_n}.$$

Taking trace at both side to F and applying (2.2), we have

$$\mathrm{Tr}_{F'_n/F}(m_{F'_n}) \supseteq m_F \,\mathrm{Tr}_{F_n/F}(m_{F_n}) \supseteq m_F^{b+2}.$$

That's a contradiction. □

Now let K' be any finite extension of K. It's well known (see [3] X.4, Lemma 6) that there exist an integer $n_0 \geq 0$ together with a finite extension F'_{n_0} over F_{n_0} satisfying:

$$F'_{n_0}K = K',\ F'_{n_0} \cap K = F_{n_0},\ [K' : K] = [F'_{n_0} : F_{n_0}]$$

Moreover, if K' is a Galois extension over K, then we also can choose F'_{n_0} to be a Galois extension of F_{n_0}. Once we have F_{n_0}, then we define $F'_n = F'_{n_0}F_n$ for all $n \geq n_0$.

***Lemma* 2.11.** *Suppose K'/K is a finite extension and F'_n is defined as above for $n \geq n_0$. Then there exist $\eta = \eta(K'/K) \geq 0$ such that*

$$\lim_{n\to\infty} \operatorname{ord}_F(\delta_{F'_n/F_n}) = \eta.$$

Proof. We will prove the lemma by showing that $\operatorname{ord}(\delta_{F'_n/F_n})$ is a decreasing sequence for all $n \geq n_0$, as $\operatorname{ord}(\delta_{F'_n/F_n}) \geq 0$. Denote $d = [K' : K]$. Then $[F'_n : F_n] = [F'_m : F_m] = d$, and hence every basis of F'_n over F_n is also a basis of F'_m over F_m for all $m \geq n$. In particular, if $m \geq n$ and $\omega_1(n), \cdots, \omega_d(n)$ is a basis of $\mathcal{O}_{F'_n}$ over O_{F_n}, then they generate a submodule of finite index in $\mathcal{O}_{F'_m}$ over $\mathcal{O}_{F_m}$. This implies that the discriminant, $\Delta(F'_n/F_n)$, of F'_n over F_n is a multiple of the discriminant $\Delta(F'_m/F_m)$. On the other hand, we have

$$\operatorname{ord}_F(\delta_{F'_n/F_n}) = \frac{1}{d}\operatorname{ord}_F(\Delta(F'_n/F_n)),$$

for every n. Therefore, the lemma is proved. □

***Lemma* 2.12.** *Suppose K' is a finite extension over K. If*

$$\lim_{n\to\infty} \operatorname{ord}_F(\delta_{F'_n/F_n}) = 0,$$

then $\operatorname{Tr}_{K'/K}(m_{K'}) = m_K$.

Proof. The lemma is proved in two exclusive cases:

Case 1: $e(F_n/F)$ is bounded, as $n \to \infty$.

In this case, there exist an integer n_1 such that K/F_{n_1} is unramified. From the multiplicative property of different, we have $\delta_{F'_{n+1}/F_{n+1}} = \delta_{F'_n/F_n}$ for all $n \geq n_1$. Since the given limit is 0, we must have $\delta_{F'_n/F_n} = \mathcal{O}_{F'_n}$ for $n \geq n_1$. Then it follows from Lemma 2.7 that $\operatorname{Tr}_{K'/K}(m_{K'}) = m_K$.

Case 2: $e(F_n/F) \to \infty$, as $n \to \infty$

In this case, if ϖ_n is the uniformizer of F_n, then $\operatorname{ord}_F(\varpi_n) \to 0$, as $n \to \infty$. For each $n \geq n_0$, let a_n denote the integer so that

$$\operatorname{Tr}_{F_n'/F_n}(\mathcal{O}_{F_n'}) = \varpi_n^{a_n} \mathcal{O}_{F_n}. \tag{2.3}$$

By Lemma 2.7, we have

$$\operatorname{ord}_F(\varpi_n^{a_n}) \leq \operatorname{ord}_F(\delta_{F_n'/F_n}). \tag{2.4}$$

Therefore, $\lim\limits_{n\to\infty} \operatorname{ord}_F(\varpi_n^{a_n}) = 0$, and hence $\lim\limits_{n\to\infty} \operatorname{ord}_F(\varpi_n^{a_n+1}) = 0$. For each given $x \in m_K$, then we can find n sufficiently large such that $x \in \mathcal{O}_{F_n}$ and $\operatorname{ord}_F(\varpi_n^{a_n+1}) < \operatorname{ord}_F(x)$. Then from (2.3), $x \in \operatorname{Tr}_{F_n'/F_n}(\varpi_n \mathcal{O}_{F_n'})$. This means $x \in \operatorname{Tr}_{K'/K}(m_{K'})$, and the proof is completed. $\square$

***Lemma* 2.13.** *Assume K does not have finite conductor. Then for each $w \in [-1, \infty)$, we have $[F_n : F_n \cap F^{(w)}] \to \infty$, as $n \to \infty$. In particular, $e(F_n/F) \to \infty$, as $n \to \infty$.*

Proof. First, we observe that if K is a finite extension of $K \cap F^{(w)}$, then it can be expressed a composition of $K \cap F^{(w)}$ and for some finite extension of F, and hence K must have finite conductor, as the conductor of $K \cap F^{(w)}$ is bounded by w. Thus, we can choose a sequence $\{\beta_1, \beta_2, \ldots\} \subset K$ such that $d_i = \deg_{K\cap F^{(w)}}(\beta_i)$ is a strictly increasing sequence. Since $\beta_i \in F_{n_i}$ for some n_i, if $n \geq n_i$, then $\beta_i \in F_n$, and consequently, $[F_n : F_n \cap F^{(w)}] \geq d_i$. This implies $[F_n : F_n \cap F^{(w)}] \to \infty$, as $n \to \infty$. Also, since $F^{(0)}$ is the maximal unramified extension of F, $e(F_n) = [F_n : F_n \cap F^{(0)}$. Therefore, the second statement is from the special case where $w = 0$. $\square$

Let $\mathcal{O}^0_{F_n'}$ denote the kernel of the trace map $\mathcal{O}_{F_n'} \longrightarrow \mathcal{O}_{F_n}$ and let a_n be the integer defined by (2.3). Also, let ϖ_n be a local uniformizer of F_n.

***Lemma* 2.14.** *Assume K' is a cyclic extension over K and τ is a generator of* $\operatorname{Gal}(K'/K)$*. Then for all $n \geq n_0$, we have*

$$\varpi_n^{a_n} \mathcal{O}^0_{F_n'} \subset (\tau - 1)\mathcal{O}_{F_n} \tag{2.5}$$

Proof. Write $G = \mathrm{Gal}(F_n'/F_n) = \mathrm{Gal}(K'/K)$. By Artin's normal basis theorem, there exists $e \in F_n'$ so that

$$\{{}^\sigma e \mid \sigma \in G\}$$

form a basis of F_n' over F_n. By multiplying e by a suitable power of ϖ if necessary, we can assume that $e \in \mathcal{O}_{F_n'}$. Then

$$E := \sum_\sigma \mathcal{O}_{F_n} \cdot {}^\sigma e \simeq \mathcal{O}_{F_n}[G]$$

and is an sub $\mathcal{O}_{F_n}$-module of $\mathcal{O}_{F_n'}$ of finite index. This implies that the Herbrad quotient of E is trivial and so is that of $\mathcal{O}_{F_n'}$. Therefore, we have

$$|\mathcal{O}_{F_n}/\varpi^{a_n}\mathcal{O}_{F_n}| = |\,\mathrm{H}^2(G, \mathcal{O}_{F_{n'}})| = |\,\mathrm{H}^1(G, \mathcal{O}_{F_{n'}})| = |\mathcal{O}^0_{F_n'}/(\tau-1)\mathcal{O}_{F_n'}|.$$

This means if

$$\mathcal{O}^0_{F_n'}/(\tau-1)\mathcal{O}_{F_n'} \simeq \bigoplus_{i=1}^m \mathcal{O}_F/\varpi^{\alpha_i}\mathcal{O}_F,$$

then $\alpha_1 + \cdots + \alpha_m = a_n$. Consequently, ϖ^{a_n} annihilates $\mathcal{O}^0_{F_n'}/(\tau-1)\mathcal{O}_{F_n'}$, and the lemma is proved. □

***Proposition* 2.15.** *The following assertions are equivalent for K:*

(a) *K/F does not have finite conductor;*

(b) *For every finite extension K' over K, we have* $\lim_{n\to\infty} \mathrm{ord}_F(\delta_{F_n'/F_n}) = 0$

(c) *For every finite extension K' over K, we have* $\mathrm{Tr}_{K'/K}(m_{K'}) = m_K$.

Proof. We have (b) implies (c) from Lemma 2.12, and that (c) implies (a) by Proposition 2.10.

Next, we prove (a) implies (b). We can assume that K' is a Galois extension of K (otherwise, we can replace K' by it's Galois closure over K, and use the multiplicative property of the different). Then can take F_n' to be Galois over F_n, for all $n \geq n_0$. Suppose K does not have finite conductor. Again, from the multiplicative property of the different, we have

$$\delta_{F_n'/F_n} = \delta_{F_n'/F_{n_0}} \cdot \delta^{-1}_{F_n/F_{n_0}}.$$

Applying Proposition 2.5 to both F'_n/F_n and F_n/F_{n_0}, we get

$$\mathrm{ord}_F(\delta_{F'_n/F_n}) = e(F_{n_0}/F)^{-1}\int_{-1}^{\infty} \frac{1}{[F_n : F_n \cap F_{n_0}^{(w)}]} - \frac{1}{[F'_n : F'_n \cap F_{n_0}^{(w)}]}\, dw.$$

As $F_{n_0}^{(w)}$ is Galois over F_{n_0}, it and F_n are linearly disjoint over $F_n \cap F_{n_0}^{(w)}$. Thus, if $R'_n(w)$ denote $F'_n \cap F_{n_0}^{(w)}$, then we have

$$[F_n : F_n \cap F_{n_0}^{(w)}] = [F_n R'_n(w) : R'_n(w)].$$

Certainly, $F_n R'_n(w) \subset F'_n$. On the other hand, if $F'_{n_0} \subset F_{n_0}^{(w_0)}$, for some w_0 and $w \geq w_0$, then $F'_n \subset F_n R'_n(w)$. Therefore,

$$\begin{aligned}\mathrm{ord}_F(\delta_{F'_n/F_n}) = &\ e(F_{n_0}/F)^{-1}\int_{-1}^{w_0} \frac{1}{[F_n : F_n \cap F_{n_0}^{(w)}]} - \frac{1}{[F'_n : F'_n \cap F_{n_0}^{(w)}]} \\ \leq &\ e(F_{n_0}/F)^{-1}\int_{-1}^{w_0} \frac{1}{[F_n : F_n \cap F_{n_0}^{(w)}]} \\ \leq &\ \frac{w_0+1}{e(F_{n_0}/F)[F_n : F_n \cap F_{n_0}^{(w_0)}]}\end{aligned}$$

that tends to 0, as $n \to \infty$ (Lemma 2.13). □

Definition. The extension K/F is *deeply ramified*, if the equivalent conditions in Proposition 2.15 are satisfied.

Suppose K'/K is a field extension. If K/F does not have finite conductor, then neither does K'/F. Thus, a field extension of a deeply ramified extension is also deeply ramified.

***Proposition* 2.16.** *Every ramified $\mathbb{Z}_p^d$-extension over F is deeply ramified.*

Proof. By Proposition 2.8 and Lemma 2.9, every ramified $\mathbb{Z}_p$-extension of F does not have finite conductor. Since every ramified $\mathbb{Z}_p^d$-extension contains a ramified intermediate $\mathbb{Z}_p$-extension, it is also deeply ramified. □

***Proposition* 2.17.** *If K/F is deeply ramified, then*

$$H^1(K, m_{\bar{F}}) = 0.$$

Proof. We need to prove $\mathrm{H}^1(\mathrm{Gal}(K'/K), m_{K'}) = 0$ for all finite Galois extensions K'/K, as $\mathrm{H}^1(K, m_{\bar{F}})$ is the direct limit (union) of them. Recall that every extension of K is also deeply ramified over F. In particular, if K'' is the fixed field of a Sylow p-subgroup of $\mathrm{Gal}(K'/K)$, then K''/F is also deeply ramified. As $m_{K'}$ is a $\mathbb{Z}_p$-module, the restriction-corestriction formula tells that the restriction map induces an injection

$$\mathrm{H}^1(\mathrm{Gal}(K'/K), m_{K'}) \longrightarrow \mathrm{H}^1(\mathrm{Gal}(K'/K''), m_{K'}).$$

Thus, by replacing K with K'', we can assume that $\mathrm{Gal}(K'/K)$ is a p-group, and hence is solvable. The we prove by the induction on the order $|\mathrm{Gal}(K'/K)|$. By taking a non-trivial cyclic subgroup H in the center of $\mathrm{Gal}(K'/K)$ (and denote $K'' = (K')^H$) and applying the inflation-restriction exact sequence:

$$0 \longrightarrow \mathrm{H}^1(\mathrm{Gal}(K'/K)/H, m_{K''}) \longrightarrow \mathrm{H}^1(\mathrm{Gal}(K'/K), m_{K'}) \longrightarrow \mathrm{H}^1(H, m_{K'}),$$

we can reduce the proof to showing $\mathrm{H}^1(H, m_{K'}) = 0$. Hence, in the following, we can assume that K'/K is a cyclic extension. Let τ be a generator of $\mathrm{Gal}(K'/K)$. We need to show that the kernel $m^0_{K'}$ of the trace map $m_{K'} \to m)K$ equals $(\tau - 1)m_{K'}$.

Suppose $x \in m^0_{K'}$ is obtained from $m^0_{F'_{n_1}}$, for some n_1. Since $\mathrm{ord}_F(\delta_{F'_n/F_n})$ tends to 0 (see Proposition 2.15(b)), as n goes to ∞, and hence so does $\mathrm{ord}_F(m_{F_n} \cdot \delta_{F'_n/F_n})$ (Lemma 2.13), we can choose n so that $\mathrm{ord}_F(x)$ is greater than $\mathrm{ord}_F(m_{F_n} \cdot \delta_{F'_n/F_n})$. Then by (2.3), (2.4) and Lemma 2.14, we see that $x \in (\tau - 1)m_{F'_n} \subset (\tau - 1)m_{K'}$. □

It can be shown (as in [1]) that $\mathrm{H}^1(K, m_{\bar{F}}) = 0$ also implies K/F is deeply ramified, although we do not need this.

3 Formal Groups and Trace Maps

Fortunately many of the arguments in Section 2 about the formal additive group can be generalized almost immediately to arbitrary commutative formal groups defined over the ring of integer of F. In this section we will carry out this generalization, which is crucial for the application to abelian varieties discussed in Section 4. The material in this section are from [1].

3.1 Formal groups

Let r be a integer ≥ 1, and let $\mathscr{F}$ be a commutative formal group law in r variables, defined over the ring $\mathcal{O}_F$.

Definition. A (commutative) *formal group law* f over $\mathcal{O}_F$ is a family $f(X,Y) = (f_i(X,Y))$ of r formal power series in $2r$ variables X_i, Y_j with coefficients in $\mathcal{O}_F$, which satisfy the axioms

(a) $X = f(X,O) = f(O,X)$,

(b) $f(X, f(Y,Z)) = f(f(X,Y),Z)$,

(c) $f(X,Y) = f(Y,X)$.

It follows immediately from the axiom that

$$f(X,Y) = X + Y + \text{terms of higher degree} \tag{3.1}$$

As usually, for any field extension K/F be any field with $F \subset K$. we define $\mathscr{F}(m_K)$ to be the set m_K^r, endowed with abelian group law:

$$x \oplus y = f(x,y),$$

even through K is not in general complete, as $m_K = \bigcup_n m_{F_n}$ and each m_{F_n} is complete, and hence the power series on the right plainly converge to an element of $m_{F_n}^r$, if $x, y \in m_{F_n}^r$.

3.2 Trace maps

We are going to show the following main theorem for formal groups:

***Theorem* 3.1.** *Let K be any extension of F which is deeply ramified. Then for all finite Galois extensions K' over K, we have*

$$H^i(K'/K, \mathscr{F}(m_{K'})) = 0, \ i = 1, 2. \tag{3.2}$$

Obviously, the theorem is equivalent to

$$H^i(K, \mathscr{F}(m_{\bar{K}})) = 0,\ i = 1, 2, \tag{3.3}$$

if K/F is deeply ramified. By the inflation-restriction exact sequence, we have the following:

***Corollary* 3.2.** *If K is deeply ramified extension of F, then*

$$H^1(F, \mathscr{F}(m_{\bar{F}})) = \mathrm{H}^1(\mathrm{Gal}(K/F), \mathscr{F}(m_K)). \tag{3.4}$$

By applying the argument in the proof of Proposition 2.17 (and, for $i = 2$, we apply the Hoschild-Serre spectral sequence, which generalizes the inflation-restriction exact sequence), we can reduce the proof of Theorem 3.1 to the case where K'/K is cyclic. In that case, the theorem will be proved by applying the trace map on the formal group $\mathscr{F}$.

Now if K be any extension of F, and K' be a finite extension over K, then we recall the trace map

$$\mathscr{N}_{K'/K} : \mathscr{F}(m_{K'}) \to \mathscr{F}(m_K)$$

is defined by $\mathscr{N}_{K'/K}(x) = (\sigma_1 x) \oplus \cdots \oplus (\sigma_d x)$, where $\sigma_1, \cdots, \sigma_d$ denote the distinct embeddings of K' into $\bar{F}$ which fixed K.

We will use the notation introduced in Sec. 2.3, and let ϖ_n denote a uniformizer for the field F_n

***Proposition* 3.3.** *Assume K is an extension of F which is deeply ramified, then for all finite extension K' of K, we have*

$$\mathscr{N}_{K'/K}(\mathscr{F}(m_{K'})) = \mathscr{F}(m_K).$$

***Lemma* 3.4.** *Assume s is an integer ≥ 1, and let $z \in (\varpi_n^s \mathcal{O}_{F'_n})^r$. Then for all $n \geq n_0$, we have*

$$\mathscr{N}_{F'_n/F_n}(z) \equiv \mathrm{Tr}_{F'_n/F_n}(z)\ mod\ \varpi_n^{2s}$$

Proof. From the definition of the formal group, it's easy to see that

$$\mathscr{N}_{F'_n/F_n}(z) = \mathrm{Tr}(z) + H_n(z) \tag{3.5}$$

where $H_n(z)$ is a vector all of whose components are formal power series in the components of $\sigma_1(z), \cdots, \sigma_d(z)$ with coefficients in $\mathcal{O}_F$, which contains only monomials of degree ≥ 2, hence $H_n(z) \equiv 0 \mod \varpi_n^{2s}$. □

Recall that the integers a_n defined in (2.3). From the above lemma, we deduce the following:

***Lemma* 3.5.** *Assume that $n \geq n_0$ and that $s \geq a_n + 1$. For any $y \in \mathscr{F}(\varpi_n^{s+a_n}\mathcal{O}_{F_n})$, there exists $w \in \mathscr{F}(\varpi_n^s\mathcal{O}_{F_n})$ such that*

$$y \ominus \mathscr{N}_{F'_n/F_n}(w) \in \mathscr{F}(\varpi_n^{s+a_n+1}\mathcal{O}_{F_n})$$

***Lemma* 3.6.** *For all $n \geq n_0$, we have*

$$\mathscr{N}_{F'_n/F_n}(\mathscr{F}(m_{F'_n})) \supset \mathscr{F}(\varpi_n^{2a_n+1}\mathcal{O}_{F_n})$$

Proof. For a given z in $\mathscr{F}(\varpi_n^{2a_n+1}\mathcal{O}_{F_n})$, we shall recursively construct a sequence of elements

$$w_\lambda \in \mathscr{F}(\varpi_n^{a_n+\lambda}\mathcal{O}_{F'_n}), \text{ for } \lambda = 1, 2, \ldots$$

such that

$$z \ominus \mathscr{N}_{F'_n/F_n}(w_1 \oplus \cdots \oplus w_\lambda) \in \mathscr{F}(\varpi_n^{2a_n+\lambda+1}\mathcal{O}_{F'_n}), \text{ for } \lambda \geq 1$$

For $\lambda = 1$, applying above lemma with $s = a_n + 1$ and $y = z$. Now assume holds for λ, then applying above lemma again with $s = a_n + \lambda + 1$ and $y = z \ominus \mathscr{N}_{F'_n/F_n}(w_1 \oplus \cdots \oplus w_\lambda)$. We deduce the existence of a $w_{\lambda+1}$ with all require properties. Let $\lambda \to \infty$, the limit $w =_1 \oplus \cdots \oplus w_\lambda \cdots$ exists in $\mathscr{F}(m_{F'_n})$. Then $\mathscr{N}_{F'_n/F_n}(w) = z$ and the proof is completed. □

Proof. (of Proposition 3.3) Take $x \in \mathscr{F}(m_K)$. Since K is deeply ramified, we have $\lim_{n\to\infty} \mathrm{ord}(\varpi_n^{2a_n+1}) = 0$. Hence we can choose n sufficiently large such that $x \in F_n$ and $\mathrm{ord}(\varpi_n^{2an+1}) < \mathrm{ord}(x)$. Thus $x \in \mathscr{F}(\varpi_n^{2a_n+1}\mathcal{O}_{F_n})$, and above lemma shows that x is a norm from $\mathscr{F}(m_{F'_n})$. □

Until further notice in this section, we shall assume that K' is now a finite cyclic extension over K. Under this assumption, Proposition 3.3 can be interpreted as

$$H^2(K'/K, \mathscr{F}(m_{K'})) = 0, \tag{3.6}$$

when K is deeply ramified. We now proceed to show that

$$H^1(K'/K, \mathscr{F}(m_{K'})) = 0 \tag{3.7}$$

when K is deeply ramified. Let $\mathscr{F}(m_{K'})^0$ denote kernel of $\mathscr{N}_{K'/K}$. Then (3.7) is equivalent to

$$\mathscr{F}(m_{K'})^0 = (\tau - 1)\mathscr{F}(m_{K'}) \tag{3.8}$$

where τ is the generator of $\mathrm{Gal}(K'/K)$. We are going to prove the last statement. We can choose n_0 so that for each $n \geq n_0$, F'_n/F_n is a cyclic extension with (the restriction to F'_n of) τ as a generator of $\mathrm{Gal}(F'_n/F_n)$.

***Lemma* 3.7.** *Assume that $n \geq n_0$ and that $s \geq a_n + 1$. If $y \in \mathscr{F}(\varpi_n^{s+a_n}\mathcal{O}_{F'_n})$ satisfies $\mathscr{N}_{F'_n/F_n}(y) = 0$, then there exist $w \in \mathscr{F}(\varpi_n^s\mathcal{O}_{F'_n})$ such that*

$$y \ominus (\tau(w) \ominus w) \in \mathscr{F}(\varpi_n^{s+a_n+1}\mathcal{O}_{F'_n}). \tag{3.9}$$

Remark. We will use the similarly method as above, that is to apply this lemma recursively, and it is important to note that $y \ominus (\tau(w) \ominus w)$ will again be in the kernel of $\mathscr{N}_{F'_n/F_n}$.

Proof. Since $\mathscr{N}_{F'_n/F_n}(y) = 0$, we have

$$\mathrm{Tr}_{F'_n/F_n}(y) \equiv 0 \bmod \varpi_n^{2(s+a_n)}.$$

From the definition of a_n, there exist $u \in (\varpi_n^{2s+a_n}\mathcal{O}_{F'_n})^r$ such that $\mathrm{Tr}_{F'_n/F_n}(y-u) = 0$. From Lemma 2.14, we have

$$\varpi_n^{s+a_n}\mathcal{O}^0_{F'_n} \subset (\tau - 1)\varpi_n^s\mathcal{O}_{F'_n}.$$

Hence, we conclude that there exist $w \in (\varpi_n^s\mathcal{O}_{F'_n})^r$ such that $(\tau - 1)w = y - u$. Moreover, we have

$$\tau(w) \ominus w \equiv (\tau - 1)w \bmod \varpi_n^{2s}.$$

Also, $u = y - (\tau - 1)w \in (\varpi_n^{2s}\mathcal{O}_{F_n'})^r$, by the construction. Then we conclude that

$$y \ominus (\tau(w) \ominus w) \equiv y - (\tau(w) \ominus w) \equiv y - (\tau(w) - w) \equiv 0 \bmod \varpi_n^{2s}.$$

Since $s \geq a_n + 1$, the lemma is proved. □

***Lemma* 3.8.** *For all $n \geq n_0$, we have*

$$\mathscr{F}(\varpi_n^{2a_n+1}\mathcal{O}_{F_n'})^0 \subset (\tau - 1)\mathscr{F}(m_{F_n'}),$$

where $\mathscr{F}(\varpi_n^{2a_n+1}\mathcal{O}_{F_n'})^0$ denote the kernel of $\mathscr{N}_{F_n'/F_n}$ on $\mathscr{F}(\varpi_n^{2a_n+1}\mathcal{O}_{F_n'})$.

Proof. For $z \in \mathscr{F}(\varpi_n^{2a_n+1}\mathcal{O}_{F_n'})^0$, we recursively apply Lemma 3.7 to construct a sequence of elements

$$w_\lambda \in \mathscr{F}(\varpi_n^{a_n+\lambda}\mathcal{O}_{F_n'}), \text{ for } \lambda = 1, 2, \ldots$$

such that

$$z \ominus (\tau(w_1 \oplus \cdots \oplus w_\lambda) \ominus (w_1 \oplus \cdots \oplus w_\lambda)) \in \mathscr{F}(\varpi_n^{2a_n+\lambda+1}\mathcal{O}_{F_n'}). \tag{3.10}$$

Then $w = w_1 \oplus \cdots \oplus w_\lambda \oplus \cdots$ exists in $\mathscr{F}(m_{F_n'})$ and from construction we have $z = \tau(w) \ominus w$. □

Proof. (of (3.7)) Take $x \in \mathscr{F}(m_{K'})^0$. Since K is deeply ramified, we have $\lim_{n\to\infty} \mathrm{ord}(\varpi_n^{2a_n+1}) = 0$. Hence we can choose an integer $n \geq n_0$ such that $x \in F_n'$ and $\mathrm{ord}(x) > \mathrm{ord}(\varpi_n^{2a_n+1})$. Now, $x \in \mathscr{F}(\varpi_n^{2a_n+1})^0$, and from above lemma, we have $x = \tau(y) \ominus y$ for some $y \in \mathscr{F}(m_{F_n'})$. □

Proof. (of Theorem 3.1) As explained right following Corollary 3.2, this is just from (3.6) and (3.7).

□

4 An Application to Abelian Varieties

The material here are from [5]. Suppose A/F is an abelian variety. Let $\mathscr{F}$ be the associated formal group along the zero section of the Néron model. We assume that A has good reduction so that its reduction $\bar{A}$ is an abelian variety over $\mathbb{F}$, the residue field of F. Then we have the exact sequence (from the reduction):

$$0 \longrightarrow \mathscr{F}(m_{\bar{F}}) \longrightarrow A(\bar{F}) \longrightarrow \bar{A}(\bar{\mathbb{F}}) \longrightarrow 0. \tag{4.1}$$

Since the reduction $A(F) \to \bar{A}(\mathbb{F})$ is surjective, the above induces the exact sequence

$$0 \longrightarrow \mathrm{H}^1(F, \mathscr{F}(m_{\bar{F}})) \longrightarrow \mathrm{H}^1(F, A) \longrightarrow \mathrm{H}^1(F, \bar{A}(\bar{\mathbb{F}})). \tag{4.2}$$

Since $\mathscr{F}(m_{\bar{F}})$ is a $\mathbb{Z}_p$-module, every element in $\mathrm{H}^1(F, \mathscr{F}(m_{\bar{F}}))$ is torsion of order equal some power of p. Let $\mathrm{H}^1(F, A)_p$ denote the p-primary part of $\mathrm{H}^1(F, A)$, then the above induces an injective homomorphism

$$\mathrm{H}^1(F, \mathscr{F}(m_{\bar{F}})) \longrightarrow \mathrm{H}^1(F, A)_p.$$

If K/F is a Galois extension with $G = \mathrm{Gal}(K/F)$, then we the inflation map (that is also injective)

$$\mathrm{H}^1(G, \mathscr{F}(m_K)) \longrightarrow \mathrm{H}^1(F, \mathscr{F}(m_{\bar{F}})).$$

Combining these two, we have

$$\mathrm{H}^1(G, \mathscr{F}(m_K)) \longrightarrow \mathrm{H}^1(F, \mathscr{F}(m_{\bar{F}})) \longrightarrow \mathrm{H}^1(F, A)_p.$$

Theorem 4.1. *Suppose A has supersingular reduction and K/F is deeply ramified, then the natural maps*

$$\mathrm{H}^1(G, \mathscr{F}(m_K)) \longrightarrow \mathrm{H}^1(F, \mathscr{F}(m_{\bar{F}})) \longrightarrow \mathrm{H}^1(F, A)_p$$

are isomorphisms. In particular, the cohomology group $H^1(G, A(K))_p$ is of infinite corank over $\mathbb{Z}_p$.

Proof. The first isomorphism is from Theorem 3.1 and the second is from the fact that every point in $\bar{A}(\bar{\mathbb{F}})$ has order prime to p (A has supersingular reduction), and hence in (4.2), $\mathrm{H}^1(F, \bar{A}(\bar{\mathbb{F}})) = 0$.

Let A^t be the dual abelian variety of A. Since $A^t(F)$ is a $\mathbb{Z}_p$-module of infinite rank (see [8]), then Tate's local duality implies that the cohomology group $H^1(F, A)_p$ is of infinite corank over $\mathbb{Z}_p$. □

Proof. (of Theorem 1.1) Theorem 4.1 and Proposition 2.16. □

References

[1] J. Coates and R. Greenberg: Kummer theory for abelian varieties over local fields, Invent. Math. **124**(1996), 129-174

[2] B. Mazur: Rational points of abelian varieties with values in towers of number fields, Invent. Math. **18**(1972), 183-266.

[3] J.-P. Serre: Corps Locaux. Hermann, 1968

[4] S. Sen: Ramification in p-adic Lie extensions, Invent. Math. **17**(1972), 44-50

[5] K.-S. Tan: A Generalized Mazur's theorem and its applications, to appear in Transactions of AMS.

[6] K.-S. Tan: Selmer groups over $\mathbb{Z}_p^d$-extensions, manuscript 2010.

[7] J. Tate: p-divisible group In: "Proceeding of a conference on local field (Driebergen, 1966)", Springer(1967), 158-183

[8] J. F. Voloch: Diophantine approximation on abelian variety in characteristic p, American J. of Math. 117(1995), 1089-1095