1-1-2014

The Strong Cm Lifting Problem & The Relabelling Action on The Equicharacteristic Universal Deformation Space of A P-Divisible Smooth Formal Groups Over an Algebraic Closure of a Field With P Elements

Taisong Jing
University of Pennsylvania, jingtaisong@gmail.com

The Strong Cm Lifting Problem & The Relabelling Action on The Equicharacteristic Universal Deformation Space of A P-Divisible Smooth Formal Groups Over an Algebraic Closure of a Field With P Elements

Abstract
It is known that an abelian variety over a finite field may not admit a lifting to an abelian variety with complex multiplication in characteristic 0. In the first part of the thesis, we study the strong CM lifting problem (sCML): can we kill the obstructions to CM liftings by requiring the whole ring of integers in the CM field act on the abelian variety? We give counterexamples to question (sCML), and prove the answer to question (sCML) is affirmative under the following assumptions on the CM field L: for every place v above p in the maximal totally real subfield L_0, either v is inert in L, or v is split in L with absolute ramification index e(v)p is a smooth formal scheme equipped with a naturally defined action by the automorphism group of the formal group via ``changing the label on the closed fiber''. In the second part of the thesis, an algorithm to compute this relabelling action is described, and some asymptotic properties of the action are obtained as the automorphism of the formal group approaches identity.

Degree Type
Dissertation

Degree Name
Doctor of Philosophy (PhD)

Graduate Group
Mathematics

First Advisor
Ching-Li Chai

Keywords
Complex multiplication, Deformation, Formal group, Lifting

Subject Categories
Mathematics

THE STRONG CM LIFTING PROBLEM &

THE RELABELLING ACTION ON THE

EQUICHARACTERISTIC UNIVERSAL DEFORMATION SPACE

OF P-DIVISIBLE SMOOTH FORMAL GROUPS OVER $\overline{\mathbb{F}}_p$

Taisong Jing

A DISSERTATION

in

Mathematics

Presented to the Faculties of the University of Pennsylvania in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

2014

Ching-Li Chai, Professor of Mathematics
Supervisor of Dissertation

David Harbater, Professor of Mathematics
Graduate Group Chairperson

Dissertation Committee:
Ching-Li Chai, Professor of Mathematics
Ted Chinburg, Professor of Mathematics
Tony Pantev, Professor of Mathematics

THIS THESIS IS DEDICATED TO

my grandfather, Huatai Jing,

for understanding me most thoroughly

and

supporting me most firmly in the world

Acknowledgments

Foremost, I would like to express my sincere gratitude to my advisor Professor Ching-Li Chai for his continuous support to my Ph.D. study and research. This thesis work would not have been written without his patience, encouragement, enthusiasm, immense knowledge, and numerous hours spent on discussion with me. I could not have imagined having a better advisor for my Ph.D. study.

Besides my advisor, I would like to thank the faculty at the University of Pennsylvania, especially Steven S. Shatz, Ted Chinburg, Florian Pop, David Harbater, and Tony Pantev, for what they taught me during the past five years. I would also like to thank Professor Frans Oort for his questions and encouragement during his visits to the University of Pennsylvania. I would like to thank Janet Burns, Monica Pallanti, and Paula Scarborough for making the department like a family to me.

I am grateful to my fellow graduate students Zhaoting Wei, Ying Zhang, Hilaf Hasson, Ryan Eberhart, and Adam Topaz for their help in mathematics and otherwise. My life would not have been much fun without the pleasant memories on movies with Shanshan Ding and Paul Levande, chats with Edvard Fagerholm, and

many other activities with Haomin Wen and Tong Li.

Final thanks go to my parents, Weidong Jing and Chunling Zhang, for their love, and Fang Liu, for new delight in my life.

ABSTRACT

THE STRONG CM LIFTING PROBLEM &

THE RELABELLING ACTION ON THE EQUICHARACTERISTIC

UNIVERSAL DEFORMATION SPACE OF P-DIVISIBLE SMOOTH FORMAL

GROUPS OVER $\overline{\mathbb{F}}_p$

Taisong Jing

Ching-Li Chai

It is known that an abelian variety over a finite field may not admit a lifting to an abelian variety with complex multiplication in characteristic 0. In the first part of the thesis, we study the strong CM lifting problem (sCML): can we kill the obstructions to CM liftings by requiring the whole ring of integers in the CM field act on the abelian variety? We give counterexamples to question (sCML), and prove the answer to question (sCML) is affirmative under the following assumptions on the CM field L: for every place v above p in the maximal totally real subfield L_0, either v is inert in L, or v is split in L with absolute ramification index $e(v) < p-1$. The equicharacteristic universal deformation space of a p-divisible smooth formal group over an algebraic closure of F_p is a smooth formal scheme equipped with a naturally defined action by the automorphism group of the formal group via "changing the label on the closed fiber". In the second part of the thesis, an algorithm to compute this relabelling action is described, and some asymptotic properties of the action are obtained as the automorphism of the formal group approaches identity.

Contents

Part I

The Strong CM Lifting Problem

Chapter 1

Introduction to Part I

In this article we study the following question concerning lifting abelian varieties over a finite field to characteristic 0:

> *Strong CM lifting* (sCML): Let $(A, \mathcal{O}_L \hookrightarrow \mathrm{End}(A))$ be a g-dimensional abelian variety over $\mathbb{F}_q$ with an action by the whole ring of integers in the CM field L of degree $2g$. Does there exist a local domain R of characteristic 0 with residue field $\mathbb{F}_q$, an abelian scheme $\mathcal{A}$ over R equipped with a CM structure $L \hookrightarrow \mathrm{End}^0(\mathcal{A}) := \mathrm{End}(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Q}$, such that $\mathcal{A}_{\mathbb{F}_q}$ is L-linearly isomorphic to A?

We give counterexamples to question (sCML) and show that it has an affirmative answer under the following additional assumptions on L: for every place v above p in the maximal totally real subfield L_0, either v is inert in L, or v is split in L with absolute ramification index $e(v) < p - 1$.

History. If we drop the assumption that $\mathcal{O}_L$ acts on A and only require $\mathrm{End}^0(A)$ contains L, the resulted CM lifting question, denoted by (CML) in [1], was first addressed by F. Oort in [18] (Thm. B). A sharper version proved in [1] (3.5.6) said that if $g \geq 2$, in any isogeny class of abelian varieties over k with p-rank at most $g-2$, there exists an abelian variety that does not admit a CM lifting to characteristic 0. Moreover, there are effective controls on the finite fields over which such examples can be constructed. Therefore (CML) does not hold in general. The question (sCML) can be considered as a first step in studying which abelian variety over $\mathbb{F}_q$ admits a CM lifting.

Approach. The question of CM lifting is local and geometric in nature; i.e., it is equivalent to consider a parallel CM lifting question about the p-divisible groups attached to the abelian variety over $\overline{\mathbb{F}}_p$. A p-divisible group is said to be an F-linear CM p-divisible group if it admits an action by a commutative semisimple $\mathbb{Q}_p$-algebra F such that $[F : \mathbb{Q}_p]$ is equal to the height of the p-divisible group; if moreover $\mathcal{O}_F$ acts on the p-divisible group, then we say it is an $\mathcal{O}_F$-linear CM p-divisible group. As an analogy to the notion of CM type for a CM abelian variety over $\mathbb{C}$, an F-linear isogeny invariant called *p-adic CM type* can be assigned to an F-linear CM p-divisible group in characteristic 0. The p-adic CM type turns out to determine the F-linear isogeny class of the CM p-divisible group; if we only consider $\mathcal{O}_F$-linear CM p-divisible groups over a complete discrete valuation ring of characteristic 0 with residue field $\overline{\mathbb{F}}_p$, then the p-adic CM type even determines

the $\mathcal{O}_F$-linear isomorphism class. Similar to the definition of reflex field for a CM type, we have the notion of reflex field for a p-adic CM type, which is the smallest possible field over whose ring of integers there exists an $\mathcal{O}_F$-linear CM p-divisible group with the prescribed p-adic CM type.

The question of CM lifting is reduced to the following question on lifting subgroups of certain CM p-divisible groups:

> Let $F := L \otimes_{\mathbb{Q}} \mathbb{Q}_p$, Φ be a subset of $\mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$, and F' be the reflex field of (F, Φ). Let $\mathcal{X}_\Phi$ be the unique $\mathcal{O}_F$-linear CM p-divisible group over $R_0 := \mathcal{O}_{B(\overline{\mathbb{F}}_p)\cdot F'}$, where $B(\overline{\mathbb{F}}_p) := W(\overline{\mathbb{F}}_p) \otimes \mathbb{Q}$. A subgroup of the closed fiber $(\mathcal{X}_\Phi)_{\overline{\mathbb{F}}_p}$ is said to be *potentially liftable*, if there exists a finite extension R/R_0 such that the subgroup lifts to a finite locally free subgroup scheme of $(\mathcal{X}_\Phi)_R$. What are the potentially liftable subgroups of $(\mathcal{X}_\Phi)_{\overline{\mathbb{F}}_p}$?

Complete lists of potentially liftable subgroups for all Φ running over the subsets of $\mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$ that are compatible with the involution ι on F induced from the complex conjugation would allow us to answer the question (CML) completely. If we content ourselves with $\mathcal{O}_F$-stable potential liftable subgroups, then we can answer the question (sCML) completely.

Main results. We first point out a constraint on the field of definition of a potential liftable subgroup. This constraint comes from the residue field of the reflex field assocated to the p-adic CM type (4.1.1). If the reflex field has a "small" residue

field for all p-adic CM types compatible with ι, then we obtain counterexamples to (sCML) (4.1). We also deduce a classification result about when this obstruction coming from small residue field can happen (4.1.2).

On the other hand, we will show that for a certain class of CM types Φ, all $\mathcal{O}_F$-stable subgroups of $(\mathcal{X}_\Phi)_{\overline{\mathbb{F}}_p}$ are potentially liftable; see (6.1.2), (6.1.3), (7.2.1), and (7.2.3). This leads to a lot of examples of abelian varieties over k with $\mathcal{O}_L$-action such that they admit CM liftings over characteristic 0 with actions by orders (usually smaller than $\mathcal{O}_L$) in L. As a corollary, we prove that the answer to the question (sCML) is affirmative when every place v of L_0 above p is inert in L; see (6.1.5) and (7.2.5).

A complete answer to the question on potential liftable subgroups of $(\mathcal{X}_\Phi)_{\overline{\mathbb{F}}_p}$ requires us to consider all finite subgroups of the geometric generic fiber of $\mathcal{X}$, and compute the reductions over $\overline{\mathbb{F}}_p$ of their scheme-theoretic closures. We do not know any such attempts in the past except for some very special cases, e.g., when $\dim \mathcal{X}$ or $\operatorname{codim} \mathcal{X}$ is 1. In the thesis, we will study an example of $\mathcal{O}_F$-linear CM p-divisible group $\mathcal{X}_\Phi$ with dimension 2 and height 4 over a complete discrete valuation ring with residue field $\overline{\mathbb{F}}_p$, where F is a p-adic local field of degree 4 with inertia degree 2 and absolute ramification index 2, satisfying in addition that $\mathrm{Gal}(F/\mathbb{Q}_p) \cong \mathbb{Z}/4$. The answer is surprising to us: whether a finite subgroup of the geometric generic fiber of $\mathcal{X}_\Phi$ has an $\mathcal{O}_F$-stable reduction is completely determined by its order. Namely, if the order is p^{2n}, then the reduction is equal to $(\mathcal{X}_\Phi)_{\overline{\mathbb{F}}_p}[\pi_0^n]$, i.e., the kernel of

multiplication on $(\mathcal{X}_\Phi)_{\overline{\mathbb{F}}_p}$ by π_0^n, where π_0 is a uniformizer of $\mathcal{O}_F$; if the order is p^{2n+1}, then the reduction is a certain subgroup G between $(\mathcal{X}_\Phi)_{\overline{\mathbb{F}}_p}[\pi_0^n]$ and $(\mathcal{X}_\Phi)_{\overline{\mathbb{F}}_p}[\pi_0^{n+1}]$, and we have a precise description on G; see (Theorem 8.1.1). As a corollary, if L is a degree 4 CM field such that $L_p \cong F$, then up to prime-to-p L-linear isogeny over $\overline{\mathbb{F}}_p$ there are only *three* abelian varieties $(A/\mathbb{F}_q, L \hookrightarrow \mathrm{End}^0(A))$ that admit L-linear CM liftings to characteristic 0.

The computations in the example above indicates that the subgroups of the geometric generic fiber of $\mathcal{X}_\Phi$ seem to "try very hard" to have an $\mathcal{O}_F$-stable reduction, though in characteristic 0 they may be far from being $\mathcal{O}_F$-stable. Based on this observation, we can ask the following question.

> Let Φ be a primitive p-adic CM type for F. Is there a general condition on the p-adic CM type Φ, such that there exists an integer $d(\Phi)$ (equal to 1 in the example above) which only depends on Φ, satisfying that for any finite locally free subgroup scheme $\mathcal{G}$ of an $\mathcal{O}_F$-linear CM p-divisible group with p-adic CM type Φ over a complete discrete valuation ring in mixed characteristic, the closed fiber of $\mathcal{G}$ contains an $\mathcal{O}_F$-stable subgroup with index uniformly bounded by $p^{d(\Phi)}$?

This is true when $\#\Phi = 1$ or $[F : \mathbb{Q}_p]-1$. In these cases, an $\mathcal{O}_F$-linear CM p-divisible group with p-adic CM type Φ in mixed characteristic has dimension or codimension 1, and all finite locally free subgroup schemes have $\mathcal{O}_F$-stable reductions; in other words, $d(\Phi) = 0$ in these cases. The main example we study in this article is the

first example that does not belong to these cases. We do not know any further examples or necessary constraints on Φ so far.

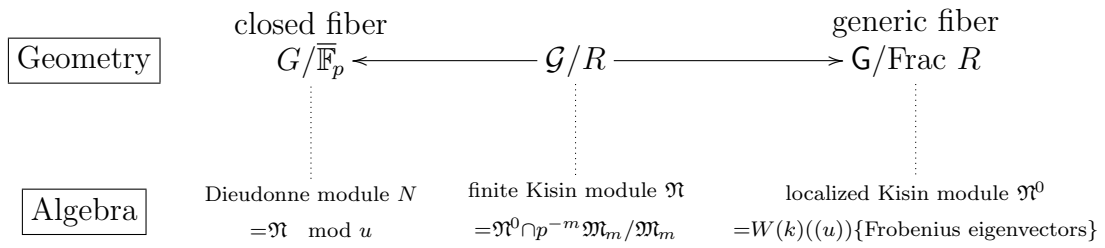
In the example of the $\mathcal{O}_F$-linear CM p-divisible group $\mathcal{X}_\Phi$ with dimension 2 and height 4, as a corollary of the computation on the reductions of its finite locally free subgroup schemes, we obtain a complete list of the closed fibers of all F-linear CM p-divisible groups in mixed characteristic with the same p-adic CM type as $\mathcal{X}_\Phi$. This leads to a counterexample to (sCML). Furthermore, in this new counterexample the reflex field is equal to F and hence its residue field is *not* "small". Therefore this counterexample does not fall in the framework of chapter 4. In other words, the obstruction coming from small residue field of the reflex field does not exhaust all the obstructions to strong CM liftings.

Tools. The main tool we employ in computations is the theory of Kisin modules from p-adic Hodge theory. For each p-adic CM type Φ for F, we construct via Kisin modules a class of $\mathcal{O}_F$-linear CM p-divisible groups with p-adic CM type Φ over the ring of integers in any finite extension of the reflex field; see (5.1). An important unresolved problem in integral p-adic Hodge theory is that the theory does not behave well under base change. However, this base change problem for $\mathcal{O}_F$-linear CM p-divisible groups has a satisfactory solution; see (3.1.1). We would like to thank C.-L. Chai for that observation. Therefore we are able to tell whether the constructions are compatible with base change; see (5.1.8). For each positive integer m, the p^m-torsion points on the geometric generic fiber of the constructed p-divisible

group become rational over a certain finite abelian extension of the base ring. We can explicitly write down the Kisin module after such a base change with the help of the theory of Lubin-Tate formal group law. These constructions and computations serve as the foundation of our approach on the strong CM lifting problem, but they are interesting in their own right as well.

One advantage of using Kisin modules is that, for a p-divisible group or its finite locally free subgroup scheme over a complete discrete valuation ring of mixed characteristic, we can write down the Dieudonne module of the closed fiber in a direct way from its Kisin module. To be more specific, a Kisin module is a $W(\kappa)[[u]]$-module equipped with a Frobenius ϕ satisfying certain additional conditions, where κ is a perfect field of characteristic p. We can associate a p-divisible group or a finite locally free subgroup scheme in mixed characteristic to a Kisin module, and roughly speaking the Dieudonne module of the closed fiber is the quotient module by "modulo u"; for a precise statement, see (3.2) or [1] (B.4.17). The localized $W(\kappa)((u))$-module of the Kisin module carries the information on the generic fiber. For a finite locally free subgroup scheme of $\mathcal{X}$, this localized $W(\kappa)((u))$-module is generated by certain "Frobenius eigenvectors" that corresponds to the torsion points; see (5.2.4). Hence, in order to lift a certain subgroup of $(\mathcal{X}_\Phi)_{\overline{\mathbb{F}}_p}$, it suffices to find an appropriate collection of torsion points such that the attached $W(\kappa)((u))$-module contains a lifting of the Dieudonne module of the subgroup; see (6.4.3). This computation is possible because of our knowledge on the torsion points, based

on the explicit information on their coordinates provided by the Lubin-Tate theory; see (5.3.5). If G is p^m-torsion, and $\mathfrak{M}_m$ is the Kisin module after base change to the extension of R_0 over which the p^m-torsion points of $(\mathcal{X}_\Phi)_{\overline{\mathbb{Q}}_p}$ become rational, the idea described above is shown in the following diagram:



Part I of the thesis is organized as follows. We first give a counterexample to (sCML) in chapter 2. After some preliminaries on CM p-divisible groups and Kisin modules in chapter 3, the obstruction that causes this counterexample will be explained and classified in chapter 4. In chapter 5.1, we construct a specific class of CM p-divisible groups and compute their torsion points via Kisin modules and Frobenius eigenvectors. In chapter 6 and 7, we establish positive results on (sCML). In chapter 8, we compute the first complete list of potentially liftable subgroups in the nontrivial cases, and deduce a new counterexample to (sCML) that does not fall in the previous framework.

Chapter 2

A Counterexample

Throughout this article, let p be a prime number, q be a power of p, and $k := \overline{\mathbb{F}}_p$. For a perfect field κ of characteristic p, let $W(\kappa)$ be the ring of Witt vectors over κ, and let $B(\kappa) := W(\kappa)[\frac{1}{p}]$. Denote the Frobenius automorphism on $B(\kappa)$ by σ. For a p-adic local field F, we denote its maximal unramified subextension of $\mathbb{Q}_p$ by F^{ur}, and its residue field by κ_F. Let L be a CM field of degree $2g$, L_0 be its maximal totally real subfield, and ι be the complex conjugation.

We first give a counterexample to (sCML). In this subsection, we consider the example where $p = 3$, $L = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$. The maximal totally real subfield $L_0 = \mathbb{Q}(\sqrt{5})$, in which p is inert. Denote the completion of L at its unique place above p by F. Pick and fix an isomorphism of F^{ur} with $B(\mathbb{F}_{p^2})$ in $B(k)$. The degree 4 extension $F \cong F^{\mathrm{ur}}[\pi]/(\pi^2 + p)$ is Galois. The involution on F induced by complex conjugation on L sends π to $-\pi$ and acts trivially on $B(\mathbb{F}_{p^2})$; we still denote this

involution by ι. Define $\tau : F \to F$ such that $\tau|_{B(\mathbb{F}_{p^2})} = \sigma$, $\tau(\pi) = \pi$. The Galois group $\mathrm{Gal}(F/\mathbb{Q}_p) = \langle\tau|\tau^2 = 1\rangle \times \langle\iota|\iota^2 = 1\rangle$.

Let B be an abelian surface over k with $\mathcal{O}_L$-action, such that the Dieudonne module M attached to $B[p^\infty]$ with $\mathcal{O}_F$-action is as follows: $M = W(k)[\pi]/(\pi^2 + p)e_1 \oplus W(k)[\pi]/(\pi^2 + p)e_2$, where the $\mathcal{O}_F$-action is $\pi \cdot e_i = \pi e_i, a \cdot e_1 = ae_1, a \cdot e_2 = a^\sigma e_2$ for $a \in W(\mathbb{F}_{p^2})$, and the $\mathcal{O}_F$-linear Frobenius and Verschiebung maps are defined by $Fe_1 = Ve_1 = e_2, Fe_2 = Ve_2 = pe_1$. See (3.1) for the existence of such an abelian surface. We claim B does *not* have an L-linear CM lifting to characteristic 0.

Suppose R is complete discrete valuation ring of characteristic 0 with residue field $k = \overline{\mathbb{F}}_p$, E is its fraction field, and fix $\overline{\mathbb{Q}}_p$ to be an algebraic closure of E. Let $\mathcal{A}$ be a CM abelian scheme with sufficiently many complex multiplications by L over R, and $\mathcal{X} := \mathcal{A}[p^\infty]$ be the associated p-divisible group. The p-divisible group $\mathcal{X}$ is an F-linear CM p-divisible group; see (3.1) for the definitions and basic properties. Then there exists a subset Φ of $\mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$ such that $\mathrm{Lie}(\mathcal{X}) \otimes_E \overline{\mathbb{Q}}_p$ splits into $\prod_{i\in\Phi}(\overline{\mathbb{Q}}_p)_i$ as an F-module, where the index of $(\overline{\mathbb{Q}}_p)_i$ indicates the action of F on $\overline{\mathbb{Q}}_p$ is given by the embedding i. This Φ is called the *p-adic CM type* of $\mathcal{X}$, and it is *compatible with* ι in the sense that $\Phi \coprod \Phi \circ \iota = \mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$; for more on its properties, see (3.1). Because of the structure of $\mathrm{Gal}(F/\mathbb{Q}_p)$, Φ is invariant under either τ or $\tau\iota$. Therefore the reflex field F' for (F, Φ) is a ramified quadratic extension over $\mathbb{Q}_p$, and the residue field $\kappa_{F'} = \mathbb{F}_p$.

It has been observed in [1] (3.8) that a "small" residue field of the reflex field for (F, Φ) will prevent a CM lifting over characteristic 0 with p-adic CM type Φ. For the convenience of the readers, we include a sketch of their argument and deduce a constraint on the reduction $\mathcal{X}_k$. Let $\mathcal{Y}$ be an $\mathcal{O}_F$-linear CM p-divisible group over $\mathcal{O}_{F'}$ with p-adic CM type Φ; for its existence, see [1] 3.7.3 (1). Let $\rho : \mathrm{Gal}((F')^{ab}/F') \to \mathcal{O}_F^\times$ be the Galois representation associated to $\mathcal{Y}$. If another Galois representation $\rho' : \mathrm{Gal}((F')^{ab}/F') \to \mathcal{O}_F^\times$ agrees with ρ when restricted to $I_{F'}^{ab}$, then we say ρ' is an *unramified twist* of ρ. An unramified twist of ρ is also the Galois representation associated to an $\mathcal{O}_F$-linear CM p-divisible group over $\mathcal{O}_{F'}$ (see [1] 1.4.3.2). Take a splitting of $\mathrm{Gal}((F')^{ab}/F') \cong \widehat{\mathbb{Z}} \times I_{F'}^{ab}$, where $I_{F'}^{ab}$ is the maximal abelian quotient of the inertia subgroup $I_{F'}$, then after twisting ρ with the unramified character $\chi : \mathrm{Gal}((F')^{ab}/F') \xrightarrow{\mathrm{pr}_1} \widehat{\mathbb{Z}} \xrightarrow{(\rho|_{\widehat{\mathbb{Z}}})^{-1}} \mathcal{O}_F^\times$, we may assume ρ carries $I_{F'}^{ab}$ onto its entire image. In particular, this implies for any positive integer m, the field generated by the p^m-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}_p}}$ is a totally ramified finite extension of F'. We denote this extension by F'_m.

With the same p-adic CM type, $\mathcal{Y} \times_{\mathrm{Spec}\,\mathcal{O}_{F'}} \mathrm{Spec}\,R$ and $\mathcal{X}$ are F-linearly isogeneous, hence there exists a finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{Y} \times_{\mathrm{Spec}\,\mathcal{O}_{F'}} \mathrm{Spec}\,R$ such that $\mathcal{X}$ is F-linearly isomorphic to $(\mathcal{Y} \times_{\mathrm{Spec}\,\mathcal{O}_{F'}} \mathrm{Spec}\,R)/\mathcal{G}$. Suppose $\mathcal{G}$ is of p^m-torsion. Without loss of generality we may assume E contains F'_m. Then there exists a finite locally free subgroup G_1 of $\mathcal{Y} \times_{\mathrm{Spec}\,\mathcal{O}_{F'}} \mathrm{Spec}\,F'_m$ such that $G_1 \times_{\mathrm{Spec}\,F'_m} \mathrm{Spec}\,E \cong \mathcal{G} \times_{\mathrm{Spec}\,R} \mathrm{Spec}\,E$. Take $\mathcal{G}_1$ to be the scheme-theoretic clo-

sure of G_1 in $\mathcal{Y} \times_{\operatorname{Spec} \mathcal{O}_{F'}} \operatorname{Spec} \mathcal{O}_{F'_m}$, and let $\mathcal{Y}_1 := (\mathcal{Y} \times_{\operatorname{Spec} \mathcal{O}_{F'}} \operatorname{Spec} \mathcal{O}_{F'_m})/\mathcal{G}_1$. Then $\mathcal{X}$ is F-linearly isomorphic to $\mathcal{Y}_1 \times_{\operatorname{Spec} \mathcal{O}_{F'_m}} \operatorname{Spec} R$.

Since F'_m is totally ramified over F', its residue field $\kappa_{F'_m} = \kappa_{F'} = \mathbb{F}_p$. Over the closed fiber, $X := \mathcal{X}_k$ is F-linearly isomorphic to $(\mathcal{Y}_1 \times_{\operatorname{Spec} \mathcal{O}_{F'_m}} \operatorname{Spec} \kappa_{F'_m}) \times_{\operatorname{Spec} \kappa_{F'_m}} \operatorname{Spec} k$. Now suppose the closed fiber $X := \mathcal{X}_k$ has a compatible $\mathcal{O}_F$-action. This implies that $\mathcal{G}_1 \times_{\operatorname{Spec} \mathcal{O}_{F'_m}} \operatorname{Spec} k$ is invariant under the $\mathcal{O}_F$-action on $(\mathcal{Y} \times_{\operatorname{Spec} \mathcal{O}_{F'}} \operatorname{Spec} \mathcal{O}_{F'_m}) \times_{\operatorname{Spec} \mathcal{O}_{F'_m}} \operatorname{Spec} k$, therefore $\mathcal{G}_1 \times_{\operatorname{Spec} \mathcal{O}_{F'_m}} \operatorname{Spec} \kappa_{F'_m}$ is invariant under the $\mathcal{O}_F$-action on $(\mathcal{Y} \times_{\operatorname{Spec} \mathcal{O}_{F'}} \operatorname{Spec} \mathcal{O}_{F'_m}) \times_{\operatorname{Spec} \mathcal{O}_{F'_m}} \operatorname{Spec} \kappa_{F'_m}$, too. So $\mathcal{Y}_1 \times_{\operatorname{Spec} \mathcal{O}_{F'_m}} \operatorname{Spec} \kappa_{F'_m}$ is an $\mathcal{O}_F$-linear CM p-divisible group and its base change to $\operatorname{Spec} k$ is $\mathcal{O}_F$-linearly isomorphic to X. In other words, X together with its $\mathcal{O}_F$-structure descents to $\mathbb{F}_p$.

Now we claim $B[p^\infty]$ together with its $\mathcal{O}_F$-structure does *not* descent to $\mathbb{F}_p$. In fact, the Lie algebra $\operatorname{Lie}(B[p^\infty]) \cong ke_1 \oplus k\pi e_1$, where the actions of $\mathcal{O}_{F^{ur}}/p = \mathbb{F}_{p^2}$ on the two summands are both induced from the chosen embedding $F^{ur} \hookrightarrow B(k)$. Such an $\mathbb{F}_{p^2}$-action does not descent to $\mathbb{F}_p$. Thus B does not have an L-linear CM lifting, and we obtain a counterexample to the question (sCML).

The key point of this counterexample is that the residue field of the reflex field F' does not contain the residue field of F. This implies that if B has an L-linear CM lifting, then $B[p^\infty]$ together with the $\mathcal{O}_F$-structure descents to a "small" field, and there will be an extra symmetry on the representation of $\mathcal{O}_F$ on $\operatorname{Lie}(B[p^\infty])$. The importance of the representation $\mathcal{O}_F \to \operatorname{End}_k(\operatorname{Lie}(B[p^\infty]))$ was noticed and studied in §4 of [1] in terms of *Lie types*. We take the next section to review the

basic facts from the CM theory of p-divisible groups, and then in §4 we will classify the counterexamples caused by the extra symmetry described above.

Chapter 3

Preliminaries

3.1 CM p-divisible groups

In this subsection we review some facts on CM p-divisible groups. Let R be either a complete discrete valuation ring of mixed characteristic $(0, p)$, or a field of characteristic p. Let X be a p-divisible group over R, and F be a commutative semisimple $\mathbb{Q}_p$-algebra of dimension $\mathrm{ht}(X)$, where $\mathrm{ht}(X)$ is the height of X. We say X is a F-linear (resp. $\mathcal{O}_F$-linear) CM p-divisible group, if $F \hookrightarrow \mathrm{End}^0(X)$ (resp. $\mathcal{O}_F \hookrightarrow \mathrm{End}(X)$). If X is an F-linear CM p-divisible group over R, then relative to the decomposition $F = \prod F_i$ as a finite product of p-adic local fields, X is isogeneous to $\prod X_i$, where X_i is an F_i-linear CM p-divisible group over R.

If F is a p-adic local field, then an F-linear CM p-divisible group X over a field of characteristic p is isoclinic; see [1] 3.7.1.6.

Let F be a finite dimensional commutative semisimple $\mathbb{Q}_p$-algebra, and $(X, \alpha : \mathcal{O}_F \to \mathrm{End}(X))$ be an $\mathcal{O}_F$-linear CM p-divisible group over a field κ of characteristic p, then $\mathrm{Lie}(X)$ is a finitely generated $\mathcal{O}_F \otimes_{\mathbb{Z}} \kappa$-module. Let $[\mathrm{Lie}(X)]$ be its class in the Grothendieck group $R_\kappa(\mathcal{O}_F)$ of the category of finitely generated $\mathcal{O}_F \otimes_{\mathbb{Z}} \kappa$-modules, this class is called the *Lie type* of the $\mathcal{O}_F$-linear CM p-divisible group X.

When $\kappa = k$ let us look at the structure of the Grothendieck group $R_k(\mathcal{O}_F)$. Suppose $F = \prod F_i$ as a finite product of p-adic local fields, then $R_k(\mathcal{O}_F) = R_k(\mathcal{O}_{F_i})$, so we may assume F is a p-adic local field. Let κ_F be the residue field of F, e_F be the ramification index of $F/\mathbb{Q}_p$. Then we have $\mathcal{O}_F \otimes_{\mathbb{Z}} k \cong \prod_{i \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)} \mathcal{O}_F \otimes_{\mathcal{O}_{F^{\mathrm{ur}}}, i} k$, and each $\mathcal{O}_F \otimes_{\mathcal{O}_{F^{\mathrm{ur}}}, i} k \cong k[t]/t^{e_F}$. For each $i \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$ there exists a canonical isomorphism $\epsilon_i \colon R_k(\mathcal{O}_F \otimes_{\mathcal{O}_{F^{\mathrm{ur}}}, i} k) \xrightarrow{\cong} \mathbb{Z}$ that sends each effective class to its dimension over k. They induce a canonical isomorphism

$$R_k(\mathcal{O}_F \otimes_{\mathbb{Z}} k) \xrightarrow{\cong} \prod_{i \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)} R_k(\mathcal{O}_F \otimes_{\mathcal{O}_{F^{\mathrm{ur}}}, i} k) \xrightarrow[\cong]{\prod \epsilon_i} \prod_{i \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)} \mathbb{Z}$$

A class δ in $R_k(\mathcal{O}_F)$ is called a *Lie type*, if for any $i \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$ the component δ_i satisfies $0 \leq \epsilon_i(\delta) \leq e_F$. Denote the set of Lie types in $R_k(\mathcal{O}_F)$ by $\mathrm{LT}(\mathcal{O}_F)$. Define $\epsilon : R_k(\mathcal{O}_F) \to \mathbb{Z}$ to be the homomorphism

$$\epsilon \colon \delta \mapsto \sum_{i \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)} \epsilon_i(\delta)$$

We call $\epsilon(\delta)$ the *dimension* of δ, and $\frac{\epsilon(\delta)}{[F:\mathbb{Q}_p]}$ the *slope* of δ. Two Lie types are said to be *isogeneous* if they have the same slope. These definitions naturally generalize to

the situation when F is a finite product of p-adic local fields. When $\delta = [\mathrm{Lie}(X)]$, these definitions are all compatible with the corresponding definitions for the p-divisible group X; see [1] (4.2.6) (i), (ii) and (iii).

For each Lie type $\delta \in R_k(\mathcal{O}_F)$, up to $\mathcal{O}_F$-linear isomorphism there exists a unique $\mathcal{O}_F$-linear CM p-divisible group $(X, \alpha : \mathcal{O}_F \to \mathrm{End}_k(X))$ over k with $[\mathrm{Lie}(X)] = \delta$; see [1] (4.2.6) (iv).

Let F be a finite dimensional commutative semisimple $\mathbb{Q}_p$-algebra. If $F = \prod F_i$ as a finite product of p-adic local fields, then $\mathrm{Hom}(F, \overline{\mathbb{Q}}_p) = \coprod \mathrm{Hom}(F_i, \overline{\mathbb{Q}}_p)$. A *p-adic CM type* Φ for F is a subset of $\mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$, and the *reflex field* F' of Φ is the p-adic local field fixed by the open subgroup $\{g \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) | g\Phi = \Phi\}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Suppose R is a complete discrete valuation ring of characteristic 0 with residue characteristic p, and Frac R is embedded in $\overline{\mathbb{Q}}_p$. For an F-linear CM p-divisible group $\mathcal{X}$ over R, there exists a p-adic CM type Φ for F such that $\mathrm{Lie}(\mathcal{X}) \otimes_R \overline{\mathbb{Q}}_p \cong \prod_{i \in \Phi} (\overline{\mathbb{Q}}_p)_i$ as $F \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p$-modules, where the index of $(\overline{\mathbb{Q}}_p)_i$ indicates the action of F on $\overline{\mathbb{Q}}_p$ is given by $i : F \to \overline{\mathbb{Q}}_p$; this Φ is called the *p-adic CM type* of $\mathcal{X}$. The cardinality of Φ is equal to the dimension of $\mathcal{X}$.

The p-adic CM type of F-linear CM p-divisible groups is invariant under isogenies. Conversely, if the residue field of R is algebraically closed and two F-linear CM p-divisible groups over R have the same p-adic CM type, then they are F-linearly isogeneous. There exists an $\mathcal{O}_F$-linear CM p-divisible group $(\mathcal{X}, \alpha : \mathcal{O}_F \to \mathrm{End}_R(\mathcal{X}))$ over R with p-adic CM type Φ if and only if Frac R contains the re-

flex field F'. If we assume the residue field of R is algebraically closed, then the $\mathcal{O}_F$-linear CM p-divisible group with p-adic CM type Φ over R is unique up to an $\mathcal{O}_F$-linear isomorphism; see [1] (3.7.3) and (3.7.4).

Suppose F is a p-adic local field. Define a map from the set of p-adic CM types to $R_k(\mathcal{O}_F)$:

$$\xi : 2^{Hom(F,\overline{\mathrm{Frac}\ R})} \to R_k(\mathcal{O}_F)$$

such that under the identification $R_k(\mathcal{O}_F) \cong \prod_{i\in \mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)} R_k(\mathcal{O}_F \otimes_{\mathcal{O}_{F^{\mathrm{ur}}},i} k) \xrightarrow[\cong]{\prod \epsilon_i} \prod_{i\in \mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)} \mathbb{Z}$, the component $\epsilon_i(\xi(\Phi))$ is equal to $\#\{\varphi \in \Phi |\, \varphi|_{F^{\mathrm{ur}}} = i\}$. If R is a complete discrete valuation ring of characteristic 0 with residue field of characteristic p, and $\mathcal{X}$ is an $\mathcal{O}_F$-linear CM p-divisible group over R with p-adic CM type Φ, then its reduction $(\mathcal{X}_\Phi)_k$ is an $\mathcal{O}_F$-linear CM p-divisible group with Lie type $\xi(\Phi)$; see [1] (4.2.3). These definitions and properties naturally generalize to the situation when F is a finite product of p-adic local fields.

Proposition 3.1.1. *Let κ be a perfect field of characteristic p, and R be a complete discrete valuation ring of characteristic 0 with residue field κ. Suppose $\mathcal{X}_1$ and $\mathcal{X}_2$ are $\mathcal{O}_F$-linear CM p-divisible groups over R with the same p-adic CM type Φ. Let X_1 and X_2 be their closed fibers over κ, respectively. Then for any $\mathcal{O}_F$-linear isomorphism $\gamma : X_1 \to X_2$, there exists a unique $\mathcal{O}_F$-linear isomorphism $\tilde{\gamma} : \mathcal{X}_1 \to \mathcal{X}_2$ such that $\tilde{\gamma}_\kappa = \gamma$.*

Proof. Let $\alpha_i : \mathcal{O}_F \hookrightarrow \mathrm{End}(\mathcal{X}_i)$ be the $\mathcal{O}_F$-structure on $\mathcal{X}_i$ for $i = 1, 2$. For every map $\mathrm{Spec}\, R' \to \mathrm{Spec}\, R$, let $(\alpha_i)_{R'} : \mathcal{O}_F \hookrightarrow \mathrm{End}((\mathcal{X}_i)_{R'})$ be the induced $\mathcal{O}_F$-structure

on $(\mathcal{X}_i)_{R'}$. Let $\tilde{R}$ be the ring of integers in the compositum Frac $R \cdot B(\overline{\kappa})$, then there exists an $\mathcal{O}_F$-linear isomorphism $\tilde{\theta} : (\mathcal{X}_1)_{\tilde{R}} \to (\mathcal{X}_2)_{\tilde{R}}$ because they have the same p-adic CM type Φ. We first show any $\mathcal{O}_F$-linear isomorphism between $(X_1)_{\overline{\kappa}}$ and $(X_2)_{\overline{\kappa}}$ over the closed fiber has a unique lifting to an $\mathcal{O}_F$-linear isomorphism between $(\mathcal{X}_1)_{\tilde{R}}$ and $(\mathcal{X}_1)_{\tilde{R}}$. Let $\beta : (X_1)_{\overline{\kappa}} \to (X_2)_{\overline{\kappa}}$ be an $\mathcal{O}_F$-linear isomorphism over the closed fiber. Then $\beta \circ (\theta^{-1}|_{\kappa})$ is an $\mathcal{O}_F$-linear automorphism of $(X_2)_{\overline{\kappa}}$. Since $(\alpha_2)_{\overline{\kappa}}(\mathcal{O}_F)$ is equal to its own centralizer in $\mathrm{End}((X_2)_{\overline{\kappa}})$, there exists $b \in \mathcal{O}_F$ such that $\beta \circ \theta_{\overline{\kappa}}^{-1} = (\alpha_2)_{\overline{\kappa}}(b)$. Then $(\alpha_2)_{\tilde{R}}(b) \circ \theta$ is a lifting of β to $\tilde{R}$. By the faithfulness of the specialization functor $\mathcal{Y} \rightsquigarrow \mathcal{Y}_{\overline{\kappa}}$ for p-divisible groups over the Noetherian local ring $\tilde{R}$ (see [1] (1.4.2.3)), this lifting is unique.

Let $\Gamma : (\mathcal{X}_1)_{\tilde{R}} \to (\mathcal{X}_2)_{\tilde{R}}$ be the lifting of $\gamma_{\overline{\kappa}}$. We claim Γ descents to an $\mathcal{O}_F$-linear isomorphism $\tilde{\gamma} : \mathcal{X}_1 \to \mathcal{X}_2$. In fact, it suffices to check the restriction $\Gamma_n : \mathcal{X}_1[p^n]_{\tilde{R}} \to \mathcal{X}_2[p^n]_{\tilde{R}}$ descents to R for each positive integer n. Since the reduction $\Gamma_n|_k$ is defined over a finite extension of κ, Γ_n is actually defined over a finite Galois étale extension of R. Again by the faithfulness of the specialization functor for p-divisible groups over $\tilde{R}$, it suffices to check the condition of finite Galois descent over the closed fiber, which is satisfied because $\gamma_{\overline{\kappa}}$ over $\overline{\kappa}$ descends to γ over κ. □

Remark 3.1.2. The closed fibers X_1 and X_2 are indeed $\mathcal{O}_F$-linearly isomorphic because they have the same Lie type. We would like to thank C.-L. Chai for his observation on (3.1.1).

Suppose L is a CM field of degree $2g$, and L_0 is its maximal totally real subfield,

and ι is the complex conjugation. Let S_0 and S be the set of places above p in L_0 and L, respectively. Then for each place $v \in S_0$, $L_v := L \otimes_{L_0} L_{0,v}$ is a 2-dimensional commutative $L_{0,v}$-algebra, and the involution in $\mathrm{Aut}(L_v/L_{0,v})$ is induced by ι. For any field κ of characteristic p, the Grothendieck group $R_\kappa(\mathcal{O}_L)$ is naturally isomorphic to $\prod_{v\in S_0} R_\kappa(\mathcal{O}_{L_v})$. If A is a g-dimensional abelian variety over κ with $\mathcal{O}_L$-action, then $\mathrm{Lie}(A)$ is a finitely generated module over $\mathcal{O}_L \otimes_{\mathbb{Z}} \kappa$, and we define the class $[\mathrm{Lie}(A)]$ in $R_\kappa(\mathcal{O}_L)$ to be the *Lie type* of A. The Lie type of the abelian variety A is equal to the Lie type of its attached p-divisible group $A[p^\infty]$ via the natural isomorphism $R_\kappa(\mathcal{O}_L) \xrightarrow{\cong} R_\kappa(\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}_p)$, and the latter is further naturally isomorphic to $\prod_{v\in S_0} R_\kappa(\mathcal{O}_{L,v}) \cong \prod_{w\in S} R_\kappa(\mathcal{O}_{L,w})$. When $\kappa = k$, we define a class in $R_k(\mathcal{O}_L)$ to be a *Lie type*, if for each $w \in S$ its component in $R_k(\mathcal{O}_{L,w})$ is a Lie type in the sense of (3.1). Denote the set of Lie types in $R_k(\mathcal{O}_L)$ by $\mathrm{LT}(\mathcal{O}_L, p)$.

Suppose A is a g-dimensional abelian variety over k with complex multiplication by L. The decomposition $L \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{v\in S_0} L_v$ induces an L-linear isogeny $A[p^\infty] \sim \prod_{v\in S_0} A[v^\infty]$, and each $A[v^\infty]$ is an L_v-linear CM p-divisible group over κ. If we denote the CM structure $L \hookrightarrow \mathrm{End}^0_k(A)$ by α^0, then the dual abelian variety $A^\vee$ has an L-action $(\alpha^0)^\vee \circ \iota$ via the composition of the dual action with the complex multiplication, and (A, α^0) is L-linearly isogeneous to $(A^\vee, (\alpha^0)^\vee \circ \iota)$. If we look at the attached p-divisible groups, it implies for each place $v \in S_0$, the L_v-linear CM p-divisible group $A[v^\infty]$ has a symmetric Newton polygon, which is equivalent to saying $\dim A[v^\infty]$ is equal to $[L_{0,v} : \mathbb{Q}_p]$. If we know the whole ring of integers $\mathcal{O}_L$

operates on A, then $A[v^\infty]$ is an $\mathcal{O}_{L_v}$-linear CM p-divisible group with dimension $[L_{0,v} : \mathbb{Q}_p]$. Conversely, if for every $v \in S_0$, X_v is an $\mathcal{O}_{L_v}$-linear CM p-divisible group over k with dimension $[L_{0,v} : \mathbb{Q}_p]$, then there exists an abelian variety A over k with $\mathcal{O}_L$-action such that $A[p^\infty]$ is $\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}_p$-linearly isomorphic to $\prod_{v \in S_0} X_v$.

Let $F_0 = \prod_{i=1}^{n} F_{0,i}$ be a finite dimensional commutative semisimple $\mathbb{Q}_p$-algebra, where each $F_{0,i}$ is a p-adic local field. Let $F := \prod_{i=1}^{n} F_i$, where F_i is a 2-dimensional commutative semisimple $F_{0,i}$-algebra. Let ι be the involution in $\mathrm{Aut}(F/F_0)$ such that $\iota|_{F_i}$ is nontrivial for all $i = 1, 2, \cdots, n$. We say a p-adic CM type Φ for F is *compatible* with ι, if $\Phi \coprod \Phi \circ \iota = \mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$.

Analogous to the question (CML) and (sCML) for abelian varieties (see chapter for the statement), we can formulate the following questions (CML) and (sCML) for p-divisible groups:

> (CML) (resp. (sCML)) *relative to (F, F_0)* for $(X, F \hookrightarrow \mathrm{End}^0(X)$ (resp. $(X, \mathcal{O}_F \hookrightarrow \mathrm{End}(X))$: Let F, F_0, ι be as above. Let X be an F-linear CM p-divisible group (resp. $\mathcal{O}_F$-linear CM p-divisible group) over k. Does there exist an F-linear CM p-divisible group $\mathcal{X}$ over a complete discrete valuation ring of characteristic 0 with residue field k, such that the p-adic CM type of $\mathcal{X}$ is compatible with ι, and the closed fiber of $\mathcal{X}$ is F-linearly isomorphic to X?

If we drop the requirement that the p-adic CM type is compatible with ι, then the answer to (sCML) is trivially affirmative. The compatibility condition with ι on

the p-adic CM type is for the purpose of algebraization; see (3.1.3) below.

Proposition 3.1.3. *The answer to question* (CML) *for* $(A, L \hookrightarrow End^0(A))$ *(resp.* (sCML) *for* $(A, \mathcal{O}_L \hookrightarrow End(A))$*) is affirmative if and only if the answer to question* (CML) *(resp.* sCML*) relative to* $(L_p, L_{0,p})$ *for* $(A[p^\infty]_k, L_p \hookrightarrow End^0(A[p^\infty]_k))$ *(resp.* $(A[p^\infty]_k, \mathcal{O}_{L,p} \hookrightarrow End(A[p^\infty]_k))$*) is affirmative.*

Proof. First of all, the question (sCML) for abelian varieties is equivalent to the apparently weaker version when $\mathbb{F}_q$ is replaced by k by deformation theory; see [1] (4.1.9).

Second, in the question (sCML) for abelian varieties over k, we may assume the base ring of the CM lifting is a complete discrete valuation ring of characteristic 0 with residue field k. To see this, let D be a local domain of characteristic 0 with residue field k, and $\mathcal{A}$ be a CM lifting over D of A. Since $\mathcal{A}$ is of finite type over D, we may assume D is Noetherian. By taking the completion along a minimal prime of characteristic 0, we may assume D is a complete local Noetherian domain. For such D, the residue field of every maximal ideal $\mathfrak{m}$ in $D[\frac{1}{p}]$ is a finite extension of $B(k)$ ([9] (7.1.9)), therefore by a base change to Spec $D/(\mathfrak{m} \cap D)$ if necessary, we may assume D is a 1-dimensional complete local Noetherian domain of characteristic 0 with residue field k. Then by a base change to the normalization of Spec D and restricting to an irreducible component of characteristic 0, we may assume D is a complete discrete valuation ring R of characteristic 0 with residue field k, and we have produced a CM lifting over R of A.

Because of the two facts above, the necessity is obvious. For sufficiency, let A be an abelian variety over k with complex multiplication by $\mathcal{O}_L$. Suppose R is a complete discrete valuation ring of characteristic 0 with residue field k, and $\mathcal{X}_p$ is an L_p-linear CM lifting of $A[p^\infty]$ with p-adic CM type compatible with ι. By Serre-Tate theorem, there exists a formal abelian scheme $\mathcal{A}$ over R to serve as an L-linear CM lifting of A, and the p-adic CM type Φ of $\mathcal{A}$ is compatible with the complex conjugation ι, i.e., $\Phi \coprod \Phi \circ \iota = \mathrm{Hom}(L, \overline{\mathbb{Q}}_p)$. By [1] (2.2.3) $\mathcal{A}$ is algebraizable, and the sufficiency direction is proved. □

At the end of this section we state several questions related to (CML) and (sCML) for p-divisible groups relative to (F, F_0).

Definition 3.1.4. Let R_0 be a local domain of characteristic 0 with residue field κ_0 of characteristic p. Let $\mathcal{X}$ be a p-divisible group over R_0. We say a finite subgroup G of $\mathcal{X}_{\kappa_0}$ is *potentially liftable*, if there exists a local domain R that is finite over R_0 with residue field κ, and a finite locally free subroup scheme $\mathcal{G}$ of $\mathcal{X}_R$, such that $\mathcal{G}_\kappa = G_\kappa$.

Based on this definition, we can ask the following question on potentially liftable subgroups of CM p-divisible groups:

> Let Φ be a p-adic CM type for F, and F' be the reflex field. Define $R_0 := \mathcal{O}_{F' \cdot B(k)}$. Let $\mathcal{X}_\Phi$ be an $\mathcal{O}_F$-linear CM p-divisible group over R_0 with p-adic CM type Φ. What are the potentially liftable subgroups of $(\mathcal{X}_\Phi)_k$?

A complete list of potentially liftable subgroups for all Φ that are compatible with ι allows us to answer (CML) for p-divisible groups relative to (F, F_0) completely; if we content ourselves with all the $\mathcal{O}_F$-stable potentially liftable subgroups, then we can answer (sCML) for p-divisible groups relative to (F, F_0) completely.

Another related question concerns the interaction between the p-adic CM type of an F-linear CM p-divisible group in characteristic 0 and the Lie type of its reduction in characteristic p.

> Let Φ be a p-adic CM type for F. Consider the family of F-linear CM p-divisible groups $\mathcal{X}$ with p-adic CM type Φ over a complete discrete valuation ring of characteristic 0 with residue field k, such that $\mathcal{O}_F$ operates on the closed fiber $\mathcal{X}_k$ via the induced CM structure $F \hookrightarrow \mathrm{End}^0(\mathcal{X}_k)$. Let $\mathrm{LTI}(F, \Phi)$ be the set of Lie types of $\mathcal{X}_k$ when $\mathcal{X}$ runs over the family above. What can we say about $\mathrm{LTI}(F, \Phi)$?

When $F = L_p$, suppose $\Phi = \coprod_{v \in S_0} \Phi_v$ under the disjoint union $\mathrm{Hom}(L_p, \overline{\mathbb{Q}}_p) = \coprod_{v \in S_0} \mathrm{Hom}(L_v, \overline{\mathbb{Q}}_p)$. It is clear that $\prod_{v \in S_0} \mathrm{LTI}(L_v, \Phi_v)$ is contained in the $\mathrm{LTI}(L_p, \Phi)$. Note that Φ is compatible with ι if and only if for each $v \in S_0$, Φ_v is compatible with ι. The answer to question (sCML) for $(X, \mathcal{O}_{L,p} \hookrightarrow \mathrm{End}(X))$ is affirmative if for each $v \in S_0$, the v-component $[\mathrm{Lie}(A[v^\infty])] \in R_k(\mathcal{O}_{L_v})$ of $[\mathrm{Lie}(A)] \in R_k(\mathcal{O}_L)$ falls into at least one of the sets $\mathrm{LTI}(L_v, \Phi_v)$'s, when Φ runs over the p-adic CM types for L_v compatible with ι.

3.2 Kisin modules

We take this subsection to review some facts on the theory of Kisin modules, which will be used extensively in this paper. Let κ be a perfect field of characteristic p. Let $\mathfrak{S} := W(\kappa)[[u]]$, and let $\phi : \mathfrak{S} \to \mathfrak{S}$ be the endomorphism of $\mathfrak{S}$ such that $\phi(u) = u^p$, and $\phi|_{W(\kappa)} = \sigma$. Let $\mathfrak{S}^0 := \mathfrak{S}[\frac{1}{u}] = W(\kappa)((u))$. For any $\mathfrak{S}$-module $\mathfrak{M}$, let $\mathfrak{M}^0 := \mathfrak{S}^0 \otimes_{\mathfrak{S}} \mathfrak{M}$. Let $E/B(\kappa)$ be a finite (totally ramified) extension, π be a uniformizer in $\mathcal{O}_E$, and $E(u) = u^e + a_{e-1}u^{e-1} + \cdots + a_1 u + a_0$ be the Eisenstein monimal polynomial of π over $\mathcal{O}_E$; in particular, e is equal to the ramification index of $E/B(\kappa)$, $p|a_i$ for all $i = 0, 1, \cdots, e-1$, and $a_0 = pc$ with $c \in W(\kappa)^\times$.

Let $\mathrm{BT}^{\phi}_{/\mathfrak{S}}$ (resp. $(\mathrm{Mod}/\mathfrak{S})$) be the category of finitely generated $\mathfrak{S}$-modules $\mathfrak{M}$ that are free (resp. that are killed by a power of p and have projective dimension 1), and are equipped with a ϕ-linear endomorphism $\phi_{\mathfrak{M}} : \mathfrak{M} \to \mathfrak{M}$, such that the cokernel of $1 \otimes \phi_{\mathfrak{M}} : \phi^*\mathfrak{M} = \mathfrak{S} \otimes_{\phi,\mathfrak{M}} \mathfrak{M} \to \mathfrak{M}$ is killed by $E(u)$. The objects in $\mathrm{BT}^{\phi}_{/\mathfrak{S}}$ (resp. $(\mathrm{Mod}/\mathfrak{S})$) are called *Kisin modules* (resp. *finite Kisin modules*). We give $\mathrm{BT}^{\phi}_{/\mathfrak{S}}$ and $(\mathrm{Mod}/\mathfrak{S})$ the structure of exact categories (in the sense of Quillen) induced from the abelian category of $\mathfrak{S}$-modules. The conditions in the definition guarantee that there exists a unique $\mathfrak{S}$-homomorphism $\psi_{\mathfrak{M}} : \mathfrak{M} \to \phi^*\mathfrak{M}$ such that $(1 \otimes \phi_{\mathfrak{M}}) \circ \psi_{\mathfrak{M}} = E(u)\mathrm{Id}$. We say $\mathfrak{M}$ is *connected* if when n is sufficiently large,

$$\psi^n_{\mathfrak{M}} := \phi^{(n-1)*}\psi_{\mathfrak{M}} \circ \phi^{(n-2)*}\psi_{\mathfrak{M}} \circ \cdots \circ \phi^*\psi_{\mathfrak{M}} \circ \psi_{\mathfrak{M}} : \mathfrak{M} \to \phi^{n*}\mathfrak{M}$$

has image contained in $(u, p)\phi^{n*}\mathfrak{M}$. The full subcategory of connected objects of $\mathrm{BT}^{\phi}_{/\mathfrak{S}}$ (resp. $(\mathrm{Mod}/\mathfrak{S})$) are denoted by $\mathrm{BT}^{\phi,f}_{/\mathfrak{S}}$ (resp. $(\mathrm{Mod}/\mathfrak{S})^c$).

Let p-div/$\mathcal{O}_E$ (resp. p-Gr/$\mathcal{O}_E$) be the category of p-divisible groups (resp. finite locally free group schemes with order equal to a power of p) over $\mathcal{O}_E$, and let $(p\text{-div}/\mathcal{O}_E)^f$ (resp. $(p\text{-Gr}/\mathcal{O}_E)^c$) be the full subcategory of connected objects. By [12] (2.2.22), when $p > 2$ there exists equivalences of exact categories:

$$p\text{-Div}_{\text{Kis}} : \text{BT}^{\phi}_{/\mathfrak{S}} \to p\text{-div}/\mathcal{O}_E, \quad p\text{-Gr}_{\text{Kis}} : \text{Mod}/\mathfrak{S} \to p\text{-Gr}/\mathcal{O}_E$$

When $p = 2$, it was proved in [11] (1.2.8) that there exists an equivalence between the subcategories:

$$p\text{-Div}_{\text{Kis}} : \text{BT}^{\phi,f}_{/\mathfrak{S}} \to (p\text{-div}/\mathcal{O}_E)^f, \quad (p\text{-Gr}_{\text{Kis}})^c : (\text{Mod}/\mathfrak{S})^c \to (p\text{-Gr}/\mathcal{O}_E)^c$$

For a Kisin module $\mathfrak{M}$ in $\text{BT}^{\phi}_{/\mathfrak{S}}$, let $\mathcal{X}$ be the associated p-divisible group over $\mathcal{O}_E$ under p-Div$_{\text{Kis}}$, then $\text{rank}_{\mathfrak{S}}\mathfrak{M} = \text{ht}\mathcal{X}$, where ht$\mathcal{X}$ is the height of $\mathcal{X}$; it is a consequence of the isomorphism (1.2.9) in [11]. The Lie algebra $\text{Lie}(\mathcal{X}) \cong \phi^*\mathfrak{M}/\psi\mathfrak{M}$, see [1] (B.4.16).

Let $\mathcal{X}$ be a p-divisible group over $\mathcal{O}_E$, and assume it is connected when $p = 2$. Let $\mathfrak{M}$ be the attached Kisin module. Let X be the closed fiber of $\mathcal{X}$, and let M be the attached Dieudonne module. It was proved in [1] B.4 that M is canonically isomorphic to $\mathfrak{M}/u\mathfrak{M}$, with the σ-linear Frobenius endomorphism $F : M \to M$ given by $\phi_{\mathfrak{M}} \mod u$, and the Verschiebung homomorphism $V : M \to M^{\sigma}$ given by $\frac{1}{c}\psi_{\mathfrak{M}} \mod u$.

Suppose $\mathfrak{M}^{\vee}$ is the Kisin module attached to the Serre dual $\mathcal{X}^{\vee}$. The description of $\mathfrak{M}^{\vee}$ was given in §3 of [13]. Namely, $\mathfrak{M}^{\vee}$ is naturally isomorphic

to $\mathrm{Hom}_{\mathfrak{S}}(\mathfrak{M}, \mathfrak{S})$, with $\phi_{\mathfrak{M}^\vee}(T) := \frac{1}{c}(1 \otimes T) \circ \psi_{\mathfrak{M}}$ for $T \in \mathfrak{M}^\vee$, and $\psi_{\mathfrak{M}^\vee}(T) := cT \circ (1 \otimes \phi_{\mathfrak{M}})$. To be more explicit, let $(e_1, e_2, \cdots, e_n)$ be an $\mathfrak{S}$-basis of $\mathfrak{M}$, and suppose $\phi_{\mathfrak{M}}(e_1, e_2, \cdots, e_n) = (e_1, e_2, \cdots, e_n)A$, where A is an $n \times n$ matrix with entries in $\mathfrak{S}$. Let $(e_1^\vee, e_2^\vee, \cdots, e_n^\vee)$ be the dual $\mathfrak{S}$-basis of $\mathfrak{M}^\vee$, then $\phi_{\mathfrak{M}^\vee}(e_1^\vee, e_2^\vee, \cdots, e_n^\vee) = (e_1^\vee, e_2^\vee, \cdots, e_n^\vee) \cdot \frac{1}{c}E(u)(A^{-1})^t$.

For a Kisin module $\mathfrak{M}$ in $(\mathrm{Mod}/\mathfrak{S})^c$, the condition that $\mathfrak{M}$ is killed by a power of p implies $\mathfrak{M}^0$ has finite length over $\mathfrak{S}^0$. If $\mathrm{length}_{\mathfrak{S}^0}\mathfrak{M}^0 = d$, then the associated finite locally free group scheme $\mathcal{G}$ over $\mathcal{O}_E$ has order p^d.

To see this, first by a devissage argument it suffices to prove the case when $\mathfrak{M}$ is killed by p. The condition that the projective dimension of $\mathfrak{M}$ (as an $\mathfrak{S}$-module) is equal to one then implies that $\mathfrak{M}$ is a free $\kappa[[u]]$-module of finite rank. Let $\mathcal{G}$ be the associated finite locally free group scheme over $\mathcal{O}_E$. It suffices to prove the order of $\mathcal{G}$ is equal to $p^{\mathrm{rank}_{\kappa[[u]]}\mathfrak{M}}$. Applying (3.2), we are reduced to proving the order of a finite p-torsion group G over κ is equal to $p^{\mathrm{rank}_\kappa M}$, where M is the attached Dieudonne module. Without loss of generality, we may and do assume κ is algebraically closed. Therefore G has a filtration with each subquotient isomorphic to $\mathbb{Z}/p\mathbb{Z}$, μ_p, or α_p. Then it becomes clear since each of them has order p and the rank of the attached Dieudonne module over κ is equal to one, too.

If $\mathcal{X}_1 \to \mathcal{X}_2$ is an isogeny between two p-divisible groups over $\mathcal{O}_E$, then the attached $\mathfrak{S}$-module homomorphism $\mathfrak{M}_1 \to \mathfrak{M}_2$ is injective, and $\mathrm{Coker}(\mathfrak{M}_1 \to \mathfrak{M}_2)$ is the Kisin module in $(\mathrm{Mod}/\mathfrak{S})^c$ attached to $\mathrm{Ker}(\mathcal{X}_1 \to \mathcal{X}_2)$.

Let $\mathfrak{M}$ be a finitely generated $\mathfrak{S}$-module $\mathfrak{M}$ which is killed by a power of p. The projective dimension of $\mathfrak{M}$ is equal to 1 if and only if u is regular for $\mathfrak{M}$. In fact, by a straightforward devissage argument we can show that $\mathfrak{M}$ has finite projective dimension, then the statement above follows from Auslander-Buchsbaum Theorem. As a corollary, the projective dimension of a submodule $\mathfrak{N}$ of $\mathfrak{M}$ is also equal to 1, and the projective dimension of the quotient $\mathfrak{M}/\mathfrak{N}$ is equal to 1 if and only if $\mathfrak{N}$ is *saturated* in $\mathfrak{M}$ in the following sense:

Definition 3.2.1. Let $\mathfrak{M}$ be a finitely generated $\mathfrak{S}$-module. A submodule $\mathfrak{N} \subset \mathfrak{M}$ is said to be *saturated* (in $\mathfrak{M}$) if $\mathfrak{N} = \mathfrak{N}^0 \cap \mathfrak{M}$.

In combination with the equivalence between the category of finite Kisin modules and finite locally free group schemes with order equal to a power of p, we deduce

Corollary 3.2.2. *Let $\mathfrak{M}$ be a finite Kisin module, and $\mathcal{G}$ be the associated finite locally free group scheme over $\mathcal{O}_E$. Then a finite Kisin submodule $\mathfrak{N} \subset \mathfrak{M}$ corresponds to a finite locally free subgroup scheme $\mathcal{H} \subset \mathcal{G}$ if and only if $\mathfrak{N}$ is saturated in $\mathfrak{M}$.*

If we know a submodule of a finite Kisin module is saturated, we can simplify the condition to check whether it is a Kisin submodule.

Proposition 3.2.3. *Let $\mathfrak{M}$ be a finite Kisin module, and $\mathfrak{N} \subset \mathfrak{M}$ be a saturated submodule. Then $\mathfrak{N}$ is a finite Kisin submodule if and only if $\mathfrak{N}$ is invariant under $\phi_{\mathfrak{M}}$.*

Proof. It suffices to check under the assumption in the proposition, the cokernel of $1 \otimes \phi_{\mathfrak{M}}|_{\phi^*\mathfrak{N}} : \phi^*\mathfrak{N} \to \mathfrak{N}$ is killed by $E(u)$. Since the cokernel $1 \otimes \phi_{\mathfrak{M}} : \phi^*\mathfrak{M} \to \mathfrak{M}$ is killed by $E(u)$, for any $x \in \mathfrak{N}$ at least we know there exists $a \in \phi^*\mathfrak{M}$ such that $(1 \otimes \phi_{\mathfrak{M}})(a) = E(u)x$. We need to show $a \in \phi^*\mathfrak{N}$.

If we base change to $\mathfrak{S}^0$, $(1 \otimes \phi_{\mathfrak{M}})^0 : (\phi^*\mathfrak{M})^0 \to \mathfrak{M}^0$ is surjective because $\mathfrak{M}^0$ is killed by p^m for some m and $E(u)$ is a unit in $\mathfrak{S}^0/p^m$. On the other hand, both $(\phi^*\mathfrak{M})^0$ and $\mathfrak{M}^0$ are $\mathfrak{S}^0$-modules of finite length and their lengths are equal, so a surjective $\mathfrak{S}^0$-homomorphism between such two modules must be an isomorphism. In particular, this tells $(1\otimes\phi_{\mathfrak{M}})^0$ is injective, and so is its restriction to $(\phi^*\mathfrak{N})^0 \to \mathfrak{N}^0$. Again because the two modules have equal lengths, the restriction $(1 \otimes \phi_{\mathfrak{M}})^0|_{(\phi^*\mathfrak{N})^0}$ is an isomorphism. In particular, for any given $x \in \mathfrak{N}$, there exists $b \in (\phi^*\mathfrak{N})^0$ such that $(1 \otimes \phi_{\mathfrak{M}})(b) = E(u)x$.

In summary, we have $E(u)x = (1 \otimes \phi_{\mathfrak{M}})(a) = (1 \otimes \phi_{\mathfrak{M}})(b)$. By the injectivity of $1 \otimes \phi_{\mathfrak{M}}$, we have $a = b \in \phi^*\mathfrak{M} \cap \phi^*\mathfrak{N}^0 = \phi^*(\mathfrak{M} \cap \mathfrak{N}^0) = \phi^*\mathfrak{N}$. □

Chapter 4

An obstruction on the Lie type for a CM Lifting to a certain p-adic CM type

4.1 Counterexamples to (sCML)

With the notion of Lie types for $\mathcal{O}_F$-linear CM p-divisible groups, it is straightforward to summarize the argument in §2 into the following proposition.

Proposition 4.1.1. *Let $F = \prod_{i=1}^{n} F_i$ be a finite dimensional commutative semisimple $\mathbb{Q}_p$-algebra, where each F_i is a p-adic local field. Let Φ be a p-adic CM type for F, and F' be the reflex field for (F, Φ). Let κ_{F_i} be the residue field of F_i, and $\kappa_{F'}$ be the residue field of F'. Suppose R is a complete discrete valuation ring of characteristic*

0 *with residue field* k*, and* $\mathcal{X}$ *is an* F*-linear CM* p*-divisible group over* R *with p-adic CM type* Φ*. If* $\mathcal{X}_k$ *has a compatible* $\mathcal{O}_F$*-action, then the class of* $[Lie(\mathcal{X}_k)]$ *in the Grothendieck group* $R_k(\mathcal{O}_F)$ *is in the image of homomorphism* $R_{\kappa_{F'}}(\mathcal{O}_F) \to R_k(\mathcal{O}_F)$ *induced by the inclusion* $\kappa_{F'} \hookrightarrow k$*.*

In particular, if there exists $1 \leq i \leq n$ *such that* κ_{F_i} *is not contained in* $\kappa_{F'}$*, then there exists an* $\mathcal{O}_F$*-linear CM* p*-divisible group* X' *over* k *such that* X' *does not admit an* F*-linear CM lifting over characteristic 0 with p-adic CM type* Φ*.* $\square$

In other words, if Φ is a p-adic CM type such that the residue field of the reflex field is "small", then there is an extra symmetry on the Lie types when we consider the reduction of CM p-divisible groups with p-adic CM type Φ. In terms of question (LTI) for p-divisible groups (see (3.1)), the statement of Proposition (4.1.1) can be written as $\mathrm{LTI}(\Phi, F) \subset \mathrm{Im}(R_{\kappa_{F'}}(\mathcal{O}_F) \to R_k(\mathcal{O}_F))$.

Let (F, F_0) be a pair as in (3.1). Based on Proposition (4.1.1), if there exists an $\mathcal{O}_F$-linear CM p-divisible group X over k such that $[\mathrm{Lie}(X)]$ is not in $\mathrm{Im}(R_{\kappa_{F'}}(\mathcal{O}_F) \to R_k(\mathcal{O}_F))$ for all p-adic CM types Φ for F that are compatible with ι, then X is a counterexample to question (sCML) relative to (F, F_0) for p-divisible groups. Concerning question (sCML) for abelian varieties, if $(L_p, L_{0,p})$ is equal to one of the following pairs (F, F_0), then the answer to question (sCML) for abelian varieties is negative.

- $F = B(\mathbb{F}_{p^2})[\pi]/(\pi^2 - p)$, $F_0 = B(\mathbb{F}_{p^2})$. The Grothendieck group $R_k(\mathcal{O}_F)$ is naturally isomorphic to $\mathbb{Z}^{\mathrm{Hom}(B(\mathbb{F}_{p^2}), \overline{\mathbb{Q}}_p)}$. For all p-adic CM types Φ for F

compatible with ι, one can check $\kappa_{F'} = \mathbb{F}_p \subsetneqq \kappa_F = \mathbb{F}_{p^2}$. Let X be an $\mathcal{O}_F$-linear CM p-divisible group over k with Lie type equal to $(2,0)$ or $(0,2)$, then X does not have an F-linear CM lifting over characteristic 0 with p-adic CM type compatible with ι.

- Suppose $p \equiv 3 \mod 4$, and $F = B(\mathbb{F}_{p^2})[\pi]/(\pi^4 - p)$, $F_0 = B(\mathbb{F}_{p^2})(\pi^2) \subset F$. The Grothendieck group $R_k(\mathcal{O}_F)$ is naturally isomorphic to $\mathbb{Z}^{\mathrm{Hom}(B(\mathbb{F}_{p^2}),\overline{\mathbb{Q}}_p)}$. For all p-adic CM types Φ for F compatible with ι, one can check $\kappa_{F'} = \mathbb{F}_p \subsetneqq \kappa_F = \mathbb{F}_{p^2}$. Let X be an $\mathcal{O}_F$-linear CM p-divisible group over k with Lie type equal to $(4,0)$, $(3,1)$, $(1,3)$, or $(0,4)$, then X does not have an F-linear CM lifting over characteristic 0 with p-adic CM type compatible with ι.

When $p > 2$, the following proposition says that the list above gives all the "essential" counterexamples to question (sCML) caused by the extra symmetry in Proposition (4.1.1)[1].

Proposition 4.1.2. *Suppose $p > 2$. Let L be a CM field, L_0 be its maximal totally real subfield. Let ι be the complex conjugation on L. Let S_0 be the set of places of L_0 above p.*

(a) *Let $v \in S_0$, and $L_v := L \otimes_{L_0} L_{0,v}$. Let κ_v be the residue field of L_v when L_v is a field, or the residue field of $L_{0,v}$ when $L_v \cong L_{0,v} \times L_{0,v}$. Suppose for all p-adic CM types for L_v that are compatible with ι, the residue field of the reflex field does*

[1]We have found another counterexample to question (sCML) that does not come from this extra symmetry. This example will come out in a future article.

not contain κ_v, then there are only two possibilities for $(L_v, L_{0,v})$:

(1) $F = B(\mathbb{F}_{p^2})[\pi]/(\pi^2 - p)$, $F_0 = B(\mathbb{F}_{p^2})$.

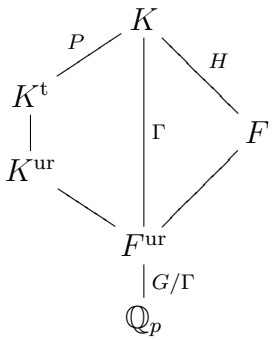
(2) $p \equiv 3 \mod 4$, $F = B(\mathbb{F}_{p^2})[\pi]/(\pi^4 - p)$, $F_0 = B(\mathbb{F}_{p^2})(\pi)$.

(b) *Let $X = \prod_{v \in S_0} X[v^\infty]$ be an $\mathcal{O}_{L,p}$-linear CM p-divisible group over k, where each $X[v^\infty]$ is an $\mathcal{O}_{L,v}$-linear CM p-divisible group. For a p-adic CM type Φ for L_p, let κ'_Φ be the residue field of the reflex field F'_Φ. If for all p-adic CM types Φ for L_p that are compatible with ι, $[Lie(X)]$ is not contained in $\mathrm{Im}(R_{\kappa'_\Phi}(\mathcal{O}_L) \to R_k(\mathcal{O}_L))$, then there exists a place $v \in S_0$, such that $(L_v, L_{0,v})$ and the $\mathcal{O}_{L_v}$-linear CM p-divisible group $X[v^\infty]$ are in the list given in* (4.1).

Proof. We first prove (b) assuming (a). If $[\mathrm{Lie}(X)]$ is not contained in the image of $R_{\kappa'_\Phi}(\mathcal{O}_L) \to R_k(\mathcal{O}_L)$, then there exists $v \in S_0$ such that $[\mathrm{Lie}(X[v^\infty])]$ is not contained in $\mathrm{Im}(R_{\kappa'_\Phi}(\mathcal{O}_{L_v}) \to R_k(\mathcal{O}_{L_v}))$. Note that $\Phi = \prod_{v \in S_0} \Phi_v$ where each Φ_v is a p-adic CM type for L_v. Let κ'_{Φ_v} be the residue field of the reflex field of Φ_v, then $\kappa'_{\Phi_v} \subset \kappa'_\Phi$. Therefore $[\mathrm{Lie}(X[v^\infty])]$ is not contained in $\mathrm{Im}(R_{\kappa'_{\Phi_v}}(\mathcal{O}_{L_v}) \to R_k(\mathcal{O}_{L_v}))$, either. In particular, this implies κ'_{Φ_v} does not contain κ_v. Note that Φ is compatible with ι if and only if each Φ_v is compatible with ι. Hence when Φ runs over the p-adic CM types for L_p that is compatible with ι, Φ_v also runs over the the p-adic CM types for L_v that is compatible with ι. Therefore v satisfies the assumptions in (a), and (b) is proved.

Now we prove (a). Let $F := L_v$, and $F_0 := L_{0,v}$. Let $n := [\kappa_F : \mathbb{F}_p]$, $e := [F : F^{\mathrm{ur}}]$. Fix an embedding of F in $\overline{\mathbb{Q}}_p$. Let K be the Galois closure of F in $\overline{\mathbb{Q}}_p$, and

let K^{t} be the maximal tamely ramified subextension of K, K^{ur} be the maximal unramified extension of K. Denote $d := [K^{\mathrm{ur}} : F^{\mathrm{ur}}]$. Let ζ_e be a fixed primitive e-th root of unity in $\overline{\mathbb{Q}}_p$. Let $G := \mathrm{Gal}(K/\mathbb{Q}_p)$, $\Gamma := \mathrm{Gal}(K/F^{\mathrm{ur}})$, $H := \mathrm{Gal}(K/F)$, $P := \mathrm{Gal}(K/K^{\mathrm{t}})$. The various fields and Galois groups are shown in the following diagram:



The set $\mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$ is naturally identified with G/H. If we fix an embedding of $F^{\mathrm{ur}} \cong B(\mathbb{F}_{p^n}) \hookrightarrow \overline{\mathbb{Q}}_p$, then $\mathrm{Hom}_{F^{\mathrm{ur}}}(F, \overline{\mathbb{Q}}_p)$ is identified with Γ/H.

We first show F/F_0 must ramify. If F/F_0 splits, we write $F \cong F_{0,1} \times F_{0,2}$, where the second index indicates the two copies of F_0. The set $\mathrm{Hom}(F, \overline{\mathbb{Q}}_p) = \mathrm{Hom}(F_{0,1}, \overline{\mathbb{Q}}_p) \coprod \mathrm{Hom}(F_{0,2}, \overline{\mathbb{Q}}_p)$. Take one embedding $i \in \mathrm{Hom}(F_{0,1}, \overline{\mathbb{Q}}_p)$ and let $\Phi := \{i\} \coprod (\mathrm{Hom}(F_{0,2}, \overline{\mathbb{Q}}_p) \backslash \{i \circ \iota\})$. The reflex field $F' = F_0$, hence $\kappa_{F'} = \kappa_F$, contradiction.

If F/F_0 is inert, then ι induces an involution on $\mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$. There is a natural fiberation $\mathrm{Res} : \mathrm{Hom}(F, \overline{\mathbb{Q}}_p) \to \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$ by restriction. Identify $\mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$ with the $\mathrm{Gal}(F^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathbb{Z}/n$-torsor $\{1, 2, \cdots, n\}$, then ι sends i to $i + \frac{n}{2}$ modulo n. Take $\Phi' := \{1, 2, \cdots, \frac{n}{2}\}$, and $\Phi := \mathrm{Res}^{-1}(\Phi')$, then Φ is compatible with ι. If $g \in G$ stabilizes Φ, g must induce identity on $\mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$. This implies $\kappa_{F'} \supset \kappa_F$,

contradiction.

Now we may and do assume F/F_0 ramifies. Next we show F is tamely ramified over F^{ur}. Because F and F_0 are completions of a CM field and its maximal totally real subfield, and the involution ι is induced by the complex conjugation, we deduce that the action of ι on G/H commutes with the left action by G. Since $F_0^{\mathrm{ur}} = F^{\mathrm{ur}}$, ι induces an involution on Γ/H.

We say a subset $\Lambda \subset \Gamma/H$ is *compatible with* ι if $\Lambda \coprod \iota\Lambda = \Gamma/H$. Define $\mathcal{S} :=$ the set of subsets of Γ/H that are compatible with ι. Then Γ acts on $\mathcal{S}$ because the action of Γ commutes with ι. We claim the action of Γ on $\mathcal{S}$ is transitive. Otherwise, let $\mathcal{S}' \coprod \mathcal{S}''$ be two disjoint Γ-orbits on $\mathcal{S}$, and take Λ', Λ'' from $\mathcal{S}', \mathcal{S}''$ respectively. Let σ be the Frobenius automorphism on F^{ur}, and θ be a lift of σ in G. Define $\Phi := \Lambda' \coprod \theta\Lambda'' \coprod \theta^2\Lambda'' \coprod \cdots \coprod \theta^{n-1}\Lambda''$, then Φ is compatible with ι. The assumption that $\kappa_{F'} \not\supseteq \kappa_F$ implies the existence of $g \in G\backslash\Gamma$ such that $g\Phi = \Phi$. Suppose $g\Gamma = \theta^s\Gamma$ where $1 \leq s \leq n-1$, then $\Lambda' = g^{-1}\theta^s\Lambda''$. This contradicts the fact that Λ' and Λ'' are in different Γ-orbits.

Note that $\#\mathcal{S} = 2^{\frac{e}{2}}$. We have assumed $p > 2$, hence as a normal p-subgroup of Γ, $P = \mathrm{Gal}(K/K^{\mathrm{t}})$ must act trivially on $\mathcal{S}$. In other words, it stablizes each $\Lambda \in \mathcal{S}$. We claim this forces $P = \langle 1 \rangle$. Otherwise, take $g \neq 1$ in P. Because the action of Γ on Γ/H is faithful, there exists $x \in \Gamma/H$ such that $gx \neq x$. Therefore there exists $\Lambda \in \mathcal{S}$ that contains both x and $\iota(g(x))$. Since g stabilizes Λ, this implies $g(x)$ and $\iota(g(x))$ are both in Λ, contradiction. This proves that F is tamely ramified over

F^{ur}.

Now we may and do F is a tamely ramified extension over F^{ur}. There exists a Teichmuller lift $\omega \in W(\mathbb{F}_{p^n})^\times$ such that $F = B(\mathbb{F}_{p^n})[\pi]/(\pi^e - \omega p)$. Under our assumption, the Galois closure $K = B(\mathbb{F}_{p^{nd}})^\times[\pi]/(\pi^e - \omega p)$, where d is the smallest positive integer such that: (a) $e|p^{nd} - 1$; (b) there exists an e-th root of ω^{p-1} in $W(\mathbb{F}_{p^{nd}})^\times$.

Let τ be the automorphism on K that fixes $B(\mathbb{F}_{p^n d})$ and sends π to $\zeta_e \pi$. Let $\sigma : K \to K$ be the automorphism that induces Frobenius on $B(\mathbb{F}_{p^{nd}})$ and sends π to $\gamma\pi$. Then $G = \langle \sigma, \tau | \sigma^{nd} = 1, \tau^e = 1, \sigma\tau\sigma^{-1} = \tau^p \rangle$, and we may identify G/H with the complete set of representatives $\{\tau^i \sigma^j | 0 \le i \le e-1, 0 \le j \le n-1\}$. Since $F_0^{\mathrm{ur}} = F^{\mathrm{ur}}$ and $[F : F_0] = 2$, we have $F_0 = B(\mathbb{F}_{p^n})(\pi^2)$, hence the action of ι on G/H sends $\tau^i\sigma^j$ to $\tau^{i+\frac{e}{2}}\sigma^j$. Now the question has turned to a concrete property on a metacyclic group G with clearly described group structure. It is a routine exercise to conclude that all the possibilities are what we have stated in the proposition. $\square$

Chapter 5

The construction of a special class of $\mathcal{O}_F$-linear CM p-divisible groups and their torsion points

Let F be a p-adic local field, $\Phi \subset Hom(F, \overline{\mathbb{Q}_p})$ be a nonempty p-adic CM type for F valued in $\overline{\mathbb{Q}_p}$, and F' be the reflex field. Let $E \supset F'$ be a p-adic local field, and $e(E)$ be its ramification index over $\mathbb{Q}_p$. Each uniformizer $\pi \in \mathcal{O}_E$ and positive integer m give a subgroup $(1 + \pi^m \mathcal{O}_E) \times \pi^{\mathbb{Z}}$ of $E^\times$. Let $E(\pi, r)$ be the corresponding totally ramified extension of E via local class field theory. With any pair of (E, π_E) where E contains F' and π_E is a uniformizer in $\mathcal{O}_E$, we will construct the Kisin module of an $\mathcal{O}_F$-linear CM p-divisible group $\mathcal{X}$ with p-adic CM type Φ over $\mathcal{O}_E$, such that for any $m \geq 1$ the p^m-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}_p}}$ are rational over $E(-\pi_E, me(E))$.

5.1 The construction of Kisin modules

We first give a generalized definition of the reflex norm of the p-adic CM type (F, Φ) and some other related notions to serve as the ingredients of the construction.

Definition 5.1.1. Let Γ be a commutative ring, N be a finitely generated free Γ-module of rank n. For $x \in \mathrm{End}_\Gamma(N)$, define the *determinant* $\det(x) \in \Gamma$ to be the induced endomorphism on $\Lambda^n N$ under the natural identification $\mathrm{End}_\Gamma(\Lambda^n N) \xrightarrow{\cong} \Gamma$. If $x \in N$, define the *characteristic polynomial* $P_{x,N}(t)$ to be $\det(t - x \otimes 1)$ for $t - x \otimes 1 \in \mathrm{End}_{\Gamma[t]}(M \otimes_\Gamma \Gamma[t])$.

Let M be a finitely generated projective Γ-module. There exists a finitely generated free Γ-module N such that M is a direct summand of N: $N = M \oplus M'$. For $x \in \mathrm{End}_\Gamma(M)$, let $\tilde{x}$ be the extension of x to $\mathrm{End}_\Gamma(N)$ by setting $\tilde{x}|_{M'} = \mathrm{Id}$. Define the *determinant* $\det(x) \in \Gamma$ to be $\det(\tilde{x})$. If $x \in N$, define the *characteristic polynomial* $P_{x,M}(t)$ to be $\det(t - \tilde{x} \otimes 1)$ for $t - \tilde{x} \otimes 1 \in \mathrm{End}_{\Gamma[t]}(M \otimes_\Gamma \Gamma[t])$.

Proposition 5.1.2. ([6] 1.2) *The definition of determinant and characteristic polynomial for an endomorphism on a finitely generated projective module does not depend on the choice of N and M'.*

In particular, if K is a field and Γ is a finite dimensional commutative semi-simple K-algebra, then every finitely generated Γ-module V is projective, hence we can define $\det(x)$ and $P_{x,V}(t)$ for every $x \in \mathrm{End}_\Gamma M$. The following proposition can be viewed as an analogy of the fact that the degree of a characteristic polynomial

for a linear transformation on a vector space is equal to the dimension of the vector space.

Proposition 5.1.3. *Let K be a field, Γ be a finite dimensional commutative semi-simple K-algebra, and V be a finitely generated Γ-module. For any $x \in End_\Gamma V$,*

$$\dim_K \Gamma[[t]]/P_{x,V}(t) = \dim_K V$$

Proof. Suppose $\Gamma = K_1 \times K_2 \times \cdots \times K_n$, then $V = V_1 \oplus V_2 \oplus \cdots \oplus V_n$, where M_i is a finite dimensional K-vector space. Write the Γ-endomorphism x as $(x_1, x_2, \cdots, x_n)$ under the isomorphism $\mathrm{End}_\Gamma(V) \cong \mathrm{End}_{K_1}(V_1) \times \mathrm{End}_{K_2}(V_2) \times \cdots \mathrm{End}_{K_n}(V_n)$. Then $P_{x,V}(t) = (P_{x_1,V_1}(t), P_{x_2,V_2}(t), \cdots, P_{x_n,V_n}(t))$. Hence

$$\dim_K \Gamma[[t]]/P_{x,V}(t) = \sum_{i=1}^{n} \dim_K K_i[[t]]/P_{x_i,V_i}(t) = \sum_{i=1}^{n} [K_i : K] \dim_{K_i} V_i = \dim_K V$$

□

Definition 5.1.4. Let K be a field, $\mathcal{K}$ be a finite dimensional commutative semisimple K-algebra, Φ be a subset of $\mathrm{Hom}(\mathcal{K}, \overline{K})$. Let $\mathcal{K}' \subset \overline{K}$ be the reflex field. Let E be a finite extension of $\mathcal{K}'$, and A be an intermediate field between E and K. Let $V_{\Phi,E}$ be an $E \otimes_K \mathcal{K}$-module such that $V_{\Phi,E} \otimes_E \overline{K} \cong \prod_{\varphi \in \Phi} (\overline{K})_\varphi$, where the subscript φ indicates the $\mathcal{K}$-action on the corresponding component.

For $x \in E^\times$, define its reflex norm with respect to Φ as the determinant of x viewed as an $A \otimes_K \mathcal{K}$-endomorphism on the $A \otimes_K \mathcal{K}$-module $V_{\Phi,E}$, denoted by $N_{\Phi,E,A\otimes_K\mathcal{K}}(x)$. Define $P_{\Phi,x,A\otimes_K\mathcal{K}}(u) \in A \otimes_{\mathbb{Q}_p} F[u]$ to be the characteristic polynomial of x.

Remark 5.1.5. (a) When $A = K$ and $\mathcal{K}$ is a finite extension of K, we recover the usual definition of the reflex norm $E^\times \to K^\times$.

(b) If $\Phi_1 \coprod \Phi_2 = \Phi_3$ and E contains the reflex field of Φ_1 and Φ_2, then $V_{\Phi_1,E} \oplus V_{\Phi_2,E} \cong V_{\Phi_3,E}$ as a direct sum as $E \otimes_K \mathcal{K}$-modules. In particular, this implies $N_{\Phi_1,E,A\otimes_K\mathcal{K}}(x)N_{\Phi_2,E,A\otimes_K\mathcal{K}}(x) = N_{\Phi_3,E,A\otimes_K\mathcal{K}}(x)$, and $P_{\Phi_1,x,A\otimes_K\mathcal{K}}(u)P_{\Phi_1,x,A\otimes_K\mathcal{K}}(u) = P_{\Phi_3,x,A\otimes_K\mathcal{K}}(u)$. When $\Phi = \mathrm{Hom}(\mathcal{K}, \overline{K})$ is the set of all the homomorphisms of $\mathcal{K}$ into $\overline{K}$, the corresponding reflex norm of $x \in E^\times$ is simply $\mathrm{Nm}_{E/A}(x)$, and its characteristic polynomial is the characteristic polynomial of x over A.

(c) For a finite extension E'/E, one can check $N_{\Phi,E,A\otimes_K\mathcal{K}} \circ \mathrm{Nm}_{E'/E} = N_{\Phi,E',A\otimes_K\mathcal{K}}$.

Now let $K = \mathbb{Q}_p$, $\mathcal{K} = F$ be a p-adic local field, Φ be a p-adic CM type for F, F' be the reflex field, and E is an extension over F'. Let $A = B(\kappa_E)$. Let π_E be a uniformizer in $\mathcal{O}_E$. Let $E(u)$ be the minimal Eisenstein polynomial of π_E over $B(\kappa_E)$. Define $c := \frac{\mathrm{Nm}_{E/B(\kappa_E)}(-\pi_E)}{p}$, then cp is the constant term of $E(u)$. Let Φ^c be the complement of Φ in $\mathrm{Hom}(F, \overline{\mathbb{Q}_p})$, then $E(u) = P_{\Phi,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u) \cdot P_{\Phi^c,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u)$.

Define $\mathfrak{M}$ to be the rank 1 free $W(\kappa_E)[[u]] \otimes_{\mathbb{Z}_p} \mathcal{O}_F$-module $W(\kappa_E) \otimes_{\mathbb{Z}_p} \mathcal{O}_F e$. There is a natural identification

$$1 \otimes \phi : \phi^*\mathfrak{M} = W(\kappa_E)[[u]] \otimes_{\phi, W(\kappa_E)[[u]]} (W(\kappa_E)[[u]] \otimes_{\mathbb{Z}_p} \mathcal{O}_F e) \xrightarrow{\cong} W(\kappa_E)[[u]] \otimes_{\mathbb{Z}_p} \mathcal{O}_F e$$

Define the ϕ-linear endomorphism $\phi_{\mathfrak{M}} : \mathfrak{M} \to \mathfrak{M}$ by $\phi_{\mathfrak{M}}(e) := \frac{1}{c} P_{\Phi^c,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u)e$, and define the $W(\kappa_E)[[u]]$ homomorphism $\psi_{\mathfrak{M}} : \mathfrak{M} \to \phi^*\mathfrak{M}$ by $\psi_{\mathfrak{M}}(e) = (1 \otimes \phi)^{-1}(cP_{\Phi,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u))e$.

Proposition 5.1.6. *The p-divisible group associated to the Kisin module $\mathfrak{M}$ constructed above is an $\mathcal{O}_F$-linear CM p-divisible group over $\mathcal{O}_E$ with p-adic CM type Φ.*

Proof. Everything is clear from the definition of $\mathfrak{M}$ except for the statement on the p-adic CM type. The Lie algebra $\mathrm{Lie}(\mathcal{X})$ is naturally isomorphic to

$$\phi^*\mathfrak{M}/\psi_{\mathfrak{M}}\mathfrak{M} \underset{\mu}{\overset{\cong}{\to}} W(\kappa_E)[[u]] \otimes_{\mathbb{Z}_p} \mathcal{O}_F/(P_{\Phi,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u))$$

Define a F-linear homomorphism on $\overline{\mathbb{Q}}_p \otimes_{\mathbb{Z}_p} \mathcal{O}_F$-modules

$$\begin{aligned} L : \overline{\mathbb{Q}}_p \otimes_{\mathcal{O}_E} (W(\kappa_E)[[u]] \otimes_{\mathbb{Z}_p} \mathcal{O}_F/(P_{\Phi,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u))) &\to \prod_{i\in\Phi} (\overline{\mathbb{Q}}_p)_i \\ 1 \otimes (f(u) \otimes y) &\mapsto (f(\pi_E)\cdot i(y))_i \end{aligned}$$

Here the index i for $\overline{\mathbb{Q}}_p$ indicates the F-action is given by $i : F \to \overline{\mathbb{Q}}_p$. The F-linear homomorphism L is well-defined because of Cayley-Hamilton Theorem. It is surjective because by Dedekind's theorem the embeddings of F in $\overline{\mathbb{Q}}_p$ are linearly independent. Count the $\mathbb{Q}_p$-dimension of the left hand side by (5.1.3): $\dim_{\overline{\mathbb{Q}}_p} \overline{\mathbb{Q}}_p \otimes_{\mathcal{O}_E} (W(\kappa_E)[[u]] \otimes_{\mathbb{Z}_p} \mathcal{O}_F/(P_{\Phi,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u))) = \dim_E(B(\kappa_E)[[u]] \otimes_{\mathbb{Q}_p} F/(P_{\Phi,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u))) = \#\Phi$. Hence L is an F-linear isomorphism and the Proposition follows. □

It is an immediate corollary of (3.2) that

Proposition 5.1.7. *The Dieudonné module of the closed fiber $\mathcal{X}_k$ of the p-divisible group constructed above is given by $M := W(\kappa_E)\otimes_{\mathbb{Z}_p}\mathcal{O}_F e$, $Fe = \frac{p}{N_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(-\pi_E)} e$, $Ve = N_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(-\pi_E) \otimes e$.* □

The construction is compatible with base change in the following sense.

Proposition 5.1.8. *Suppose $E' \supset E \supset F'$ are p-adic local fields. Let κ_E and $\kappa_{E'}$ be the residue field of E, E', respectively. Let $E^* := B(\kappa_{E'}) \cdot E$. Suppose $\pi_{E'}, \pi_E$ are uniformizers in E', E such that $Nm_{E'/E^*}(-\pi_{E'}) = -\pi_E$. Let $\mathfrak{M}, \mathfrak{M}'$ be the Kisin modules constructed above with (E, π_E) and $(E', \pi_{E'})$, respectively. If we denote the p-divisible group associated to $\mathfrak{M}, \mathfrak{M}'$ by $\mathcal{X}, \mathcal{X}'$, then $\mathcal{X}'$ is $\mathcal{O}_F$-linearly isomorphic to $\mathcal{X} \times_{Spec\, \mathcal{O}_E} Spec\, \mathcal{O}_{E'}$ via a canonical isomorphism.*

Proof. Let X and X' be the closed fiber of $\mathcal{X}$ and $\mathcal{X}'$ over κ_E and $\kappa_{E'}$, respectively. By (3.1.1), we only need to show $X \times_{\operatorname{Spec} \kappa_E} \operatorname{Spec} \kappa_{E'}$ is $\mathcal{O}_F$-linearly isomorphic to X'. It suffices to prove in the situations when E'/E is totally ramified or unramified. When E'/E is totally ramified, $E^* = E$. Proposition 5.1.7 it suffices to show $N_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p} F}(-\pi_E) = N_{\Phi,E',B(\kappa_E)\otimes_{\mathbb{Q}_p} F}(-\pi_{E'})$, which follows from the condition $\operatorname{Nm}_{E'/E}(-\pi_{E'}) = -\pi_E$. When E'/E is unramified, $\pi_{E'} = \pi_E$ and $E' = B(\kappa'_E) \cdot E$. One can show for any $x \in \mathcal{O}_E \subset \mathcal{O}_{E'}$, we have $N_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p} F}(x) = N_{\Phi,B(\kappa'_E)\cdot E,B(\kappa'_E)\otimes_{\mathbb{Q}_p} F}(x)$, this finishes the proof. □

The following proposition is also a direct application of (3.1.1).

Proposition 5.1.9. *Let E be a p-adic local field that contains F', κ_E be the residue field of E, and π_E be a uniformizer of $\mathcal{O}_E$. Let $\mathfrak{M}$ be the Kisin module constructed with (E, π_E). Let κ be an extension of κ_E, and $E^* := B(\kappa) \cdot E$. Define $\mathfrak{M}^* := \mathfrak{M} \otimes_{W(\kappa_E)} W(\kappa)$, and $\phi_{\mathfrak{M}^*}$ to be the natural extension of $\phi_{\mathfrak{M}}$. Let $\mathcal{X}$ and $\mathcal{X}^*$ be*

the p-divisible group attached to $\mathfrak{M}$ and $\mathfrak{M}^*$. Then $\mathcal{X}^*$ is $\mathcal{O}_F$-linearly isomorphic to $\mathcal{X} \times_{Spec\,\mathcal{O}_E} Spec\,\mathcal{O}_{E^*}$ via a canonical isomorphism.

5.2 Torsion points

Let κ be a perfect field of characteristic p, and E be a finite totally ramified extension over $B(\kappa)$. Let π_E be a uniformizer in $\mathcal{O}_E$, and $E(u)$ be its minimal Eisenstein polynomial over $B(\kappa)$. Assume the constant term of $E(u)$ is equal to pc, where $c \in W(\kappa)^\times$. Let $\mathcal{X}$ be a p-divisible group over $\mathcal{O}_E$ (connected if $p = 2$), and let $\mathfrak{M}$ be the attached Kisin module. By the theory of Kisin modules, to find a torsion point on $\mathcal{X}$ is equivalent to solve a certain equation on $p^{-\infty}\mathfrak{M}/\mathfrak{M}$ as follows.

Lemma 5.2.1. *Let $m \geq 1$ be a positive integer. Then there is a natural one-to-one correspondence between the p^m-torsion points on $\mathcal{X}$ and the set*

$$\{x \in p^{-m}\mathfrak{M}/\mathfrak{M} | \phi_{\mathfrak{M}}(x) = \frac{1}{c}E(u)x\}$$

Proof. When $p > 2$, the equivalence between finite Kisin modules and finite locally free group schemes killed by a power of p covers the etale group scheme $\mathbb{Z}/p^m$. The attached Kisin module $\mathfrak{M}(\mathbb{Z}/p^m)$ is isomorphic to $(\mathfrak{S}/p^m) \cdot e$, with $\phi_\mu e = \frac{1}{c}E(u)e, \psi_\mu e = c \otimes e$. Then the statement follows directly from the identification between $\mathrm{Hom}(\mathbb{Z}/p^m, \mathcal{X}[p^m])$ and $\mathrm{Hom}_{\mathfrak{S}/p^m}(\mathfrak{M}(\mathbb{Z}/p^m), p^{-m}\mathfrak{M}/\mathfrak{M})$. When $p = 2$, we can take a detour via their Cartier dual by the identification $\mathrm{Hom}(\mathbb{Z}/p^m, \mathcal{X}[p^m]) \cong \mathrm{Hom}(\mathcal{X}^*[p^m], \mu_{p^m})$. The details are left as exercises. □

Let $\mathcal{X}$ be the p-divisible group over $\mathcal{O}_E$ associated to the Kisin module $\mathfrak{M}$ constructed in (5.1). By CM theory we know the p^m-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ generate an abelian extension of E. Let $\mathrm{Gal}(E^{\mathrm{ab}}/E)$ and I_E^{ab} be the abelianized absolute Galois group of E and its inertia subgroup. If we would expect the Galois representation $\rho : \mathrm{Gal}(E^{\mathrm{ab}}/E) \to \mathcal{O}_F^\times$ attached to $\mathcal{X}$ to bring I_E^{ab} onto the image of ρ, then there exists a splitting $\mathrm{Gal}(E^{ab}/E) \cong \hat{\mathbb{Z}} \times I_E^{\mathrm{ab}}$ such that the first component acts on $\mathcal{X}[p^m]$ trivially, and the action of the second component is compatible with the reflex norm $\mathcal{O}_E^\times \xrightarrow{N_{\Phi,E}} \mathcal{O}_F^\times \twoheadrightarrow \mathcal{O}_F^\times/p^m$ via local class field theory. In particular, $1 + p^m\mathcal{O}_E^\times$ acts trivially on $\mathcal{X}[p^m]$. This hope guides us to search for the solution to $\phi_{\mathfrak{M}}(x) = \frac{1}{c}E(u)x$ in the Kisin module after a base change to a class field of E.

The theory of Lubin-Tate formal group law provides us with information on the explicit Eisenstein polynomial of a class field of E. Let us take a brief review on the set up of Lubin-Tate theory. Let E be a p-adic local field and π be a uniformizer. Let κ_E be the residue field, and $N := [\kappa_E : \mathbb{F}_p]$. Let $h(x)$ be a degree p^N polynomial in $\mathcal{O}_E[[x]]$ such that $h(x) \equiv \pi x + \text{terms of degree } \geq 2$ and $h(x) \equiv x^{p^N} \mod \pi$. For any positive integer r, let $h^{(r)}(x) := h \circ h \circ \cdots \circ h$ be the r-th iteration of $h(x)$. Since $x|h(x)$, we deduce $h^{(r-1)}(x)|h^{(r)}(x)$. Define $h_r(x) := \frac{h^{(r)}(x)}{h^{(r-1)}(x)}$. It is clear that $h_r(x)$ is an Eisenstein polynomial of degree $p^{Nr} - p^{N(r-1)}$ over E. There exists a unique one dimensional formal group law $F_h(X, Y)$ over $\mathcal{O}_E$ such that $F_h \circ h = h \circ F_h$. For any $a \in \mathcal{O}_E$, there exists a unique element $[a]_h \in \mathcal{O}_E[[x]]$ such that $[a]_h(x) = ax + \text{terms of degree} \geq 2$ and $F_h \circ [a]_h = [a]_h \circ F_h$; in particular

$h = [\pi]_h$. The p-divisible group $\mathcal{X}_h$ attached to F_h is an $\mathcal{O}_E$-linear one dimensional CM p-divisible group over $\mathcal{O}_E$, and the roots of $h^{(r)}(x)$ are the coordinates of π^r-torsion points on $\mathcal{X}_h$. The field $E(\pi, r)$ generated by these coordinates is an abelian extension of E with Galois group $\mathcal{O}_E^\times/\pi^r$, and it corresponds to the open subgroup $(1 + \pi^r\mathcal{O}_E) \times \pi^{\mathbb{Z}}$ of $E^\times$ via local class field theory.

Lemma 5.2.2. *Let r be a positive integer. For any $y_1, y_2 \in \mathcal{O}_E[[x]]$ such that $y_1 \equiv y_2 \mod \pi$, we have $h^{(r)}(y_1) \equiv h^{(r)}(y_2) \mod \pi^{r+1}$.*

Proof. Let $\log_F(x)$ be the logarithm of the Lubin-Tate formal group law $F_h(X, Y)$, it satisfies a functional equation $\log_F(x) = g(x) + \frac{1}{\pi}\log_F(x^{p^N})$ for some $g(x) = x + \text{terms of degree} \geq 2$; see [8] (I.8.3.6). For any $\alpha(x) \in \mathcal{O}_E[[x]]$ and $\beta(x) \in E[[x]]$ and any positive integer k, we have $\log_F(\alpha(x)) \equiv \log_F(\beta(x)) \mod \pi^k$ if and only if $\alpha(x) \equiv \beta(x) \mod \pi^k$ by [8] (I.2.2). Since $\log_F \circ h^{(r)} = \pi^r \circ \log_F$, it suffices to check $\log_F(y_1) \equiv \log_F(y_2) \mod \pi$. Let ν be a valuation on E such that $\nu(\pi) = 1$. It follows from the functional equation that $\log_F(x) = \sum_{i=0}^{\infty} a_i x^i$, where $p^{Nj}|i$ if $\nu(a_i) = -j$. This guarantees $a_i y_1^i \equiv a_i y_2^i \mod \pi$ when $y_1 \equiv y_2 \mod \pi$, and the lemma now follows. □

Corollary 5.2.3. *For any positive integer r, $h^{(r-1)}(x^{p^N}) \equiv h^{(r-1)}(x)h_r(x) \mod \pi^r$.*

□

Let $\mathcal{X}$ be the p-divisible group over $\mathcal{O}_E$ associated to the Kisin module $\mathfrak{M}$ constructed in (5.1). Now we are ready to compute the coordinates of the torsion

points on the geometric generic fiber of $\mathcal{X}$ in the sense of Lemma 5.2.1, after a base change to an abelian extension of E. First let us make some notations:

- Let F' be the reflex field of the p-adic CM type (F, Φ), E be a finite extension of F', π_E be a uniformizer in $\mathcal{O}_E$, and κ_E be the residue field. Let $e(E)$ be the absolute ramification index of E. Define $n := [\kappa_F \cap \kappa_E : \mathbb{F}_p]$, $N := [\kappa_E : \mathbb{F}_p]$.

- Let $h(x)$ be a degree p^N polynomial in $\mathcal{O}_E[[x]]$ such that $h(x) \equiv -\pi_E x +$ terms of degree ≥ 2 and $h(x) \equiv x^{p^N} \mod \pi$. Let $h^{(r)}(x) := h \circ h \circ \cdots \circ h$, and $h_r(x) := \frac{h^{(r)}(x)}{h^{(r-1)}(x)}$ for all positive integers r.

- Let m be a positive integer, and $M := me(E)$. Let π_m be a root of the Eisenstein polynomial $h_M(x)$. Let $E_m := E(\pi_m) = E(-\pi_E, M)$ be the abelian extension of E given by Lubin-Tate theory.

- Let $E(u)$ and $E_m(u)$ be the minimal Eisenstein polynomial of π_E and π_m over $B(\kappa_E)$, and let cp and $c_m p$ be the constant terms of $E(u)$ and $E_m(u)$.

- Let $\mathfrak{M}$ and $\mathfrak{M}_m$ be the Kisin modules constructed as in (5.1) with (E, π_E) and (E_m, π_m), and let $\mathcal{X}$ and $\mathcal{X}_m$ be the associated p-divisible groups.

- Define $v := (N_{\Phi, E(u), B(\kappa_E)\otimes_{\mathbb{Q}_p} F(u)}(h^{(M-1)}(u)))^{\phi^{N-1}+\phi^{N-2}+\cdots+\phi+1} e \in \mathfrak{M}_m$; see (5.1.4) for the definition of $\Lambda_{\Phi, E, B(\kappa_E)\otimes_{\mathbb{Q}_p} F}(h^{(M-1)}(u))$.

- For any subgroup A of the finite abelian group $p^{-m}\mathcal{O}_F/\mathcal{O}_F$, define $\mathfrak{N}_A^0$ to be the $\mathfrak{S}^0$-module $\mathfrak{S}^0\{\eta \cdot v | \eta \in A\}$, define $\mathfrak{N}_A$ to be the saturated finite Kisin

module $\mathfrak{N}_A^0 \cap (p^{-m}\mathfrak{M}_m/\mathfrak{M}_m)$. Let $\mathcal{G}_A$ be the p^m-torsion finite locally free subgroup scheme of $\mathcal{X}_m$ attached to $\mathfrak{N}_A$.

- For each $\tau \in \mathrm{Hom}(B(\kappa_E) \cap F, \overline{\mathbb{Q}}_p)$, choose an embedding $i_\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$ such that $i_\tau|_{B(\kappa_E)\cap F} = \tau$. Let $\Phi_\tau := \{i \in \Phi | i|_{B(\kappa_E)\cap F} = \tau\}$. Define $S_\tau := \{\alpha \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/B(\kappa_E))/\mathrm{Gal}(\overline{\mathbb{Q}}_p/E) | \alpha^{-1} \circ i_\tau \in \Phi_\tau\}$. Define a homomorphism $\phi : \mathcal{O}_{B(\kappa_E)\cdot i_\tau(F)}[[u]] \to \mathcal{O}_{B(\kappa_E)\cdot i_{\sigma\tau}(F)}[[u]]$, such that $\phi|_{W(\kappa_E)} = \sigma$, $\phi|_{i_\tau(F)} = i_{\sigma\tau} \circ i_\tau^{-1}$, and $\phi(u) = u^p$. Define $\tilde{f}_{\tau,m}(u) := \prod_{\alpha\in S_\tau} (\alpha_* h_M)(u)$, $\tilde{g}_{\tau,m}(u) := \prod_{\alpha\in S_\tau} (\alpha_* h^{(M-1)})(u)$, and $g_{\tau,m}(u) := \tilde{g}_{\tau,m}(u)^{\phi^{N-n}+\phi^{N-2n}+\cdots+\phi^n+1}$.

Proposition 5.2.4. *Notations are as above, then:*

(a) The element v in $\mathfrak{M}_m$ satisfies $\phi_{\mathfrak{M}_m}(v) \equiv \frac{1}{c_m} E_m(u) v \mod p^m$. In $p^{-m}\mathfrak{M}/\mathfrak{M}$, all solutions x to $\phi_{\mathfrak{M}_m}(x) = \frac{1}{c_m} E_m(u) x$ have the form $\eta \cdot v$, where η runs over $p^{-m}\mathcal{O}_F/\mathcal{O}_F$.

(b) There exists an $\mathcal{O}_F$-linear isomorphism between $\mathcal{X} \times_{Spec\,\mathcal{O}_E} Spec\,\mathcal{O}_{E_m}$ and $\mathcal{X}_m$, and all the p^m-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are rational over E_m.

(c) The mapping $A \mapsto \mathcal{G}_A$ is a one-to-one correspondence from the subgroups of $p^{-m}\mathcal{O}_F/\mathcal{O}_F$ to the p^m-torsion finite locally free subgroup schemes of $\mathcal{X}_m$, and we have $\#\mathcal{G}_A = \#A$.

(d) Under the identification of

$$\mathfrak{M}_m := W(\kappa_E) \otimes_{\mathbb{Z}_p} \mathcal{O}_F[[u]]e \xrightarrow{\cong} \bigoplus_{\tau\in Hom(B(\kappa_E)\cap F, B(\kappa_E))} \mathcal{O}_{B(\kappa_E)\cdot i_\tau(F)}[[u]]e_\tau$$

we have a concrete description of $\phi_{\mathfrak{M}_m}$ and v:

$$\phi_{\mathfrak{M}_m} e_\tau = \tilde{f}_{\sigma\tau,m}(u) e_{\sigma\tau}, \qquad v = \sum_{\tau \in Hom(B(\kappa_E)\cap F, B(\kappa_E))} (\prod_{i=0}^{n-1} g_{\sigma^{-i}\tau,m}(u)^{\phi^i}) e_\tau$$

Remark 5.2.4.1. It follows from CM theory and local class field theory that all the p^m-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are rational over a certain totally ramified abelian extension of E, i.e., the fixed field of the kernel of the associated Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}_p/E) \to \mathcal{O}_F^\times \Rightarrow (\mathcal{O}_F/p^m)^\times$. The computation here on torsion points via Kisin modules allows us to tell this kernel explicitly: it corresponds to the subgroup $(1+\pi_E^M \mathcal{O}_E) \times (-\pi_E)^{\mathbb{Z}} \subset E^\times$ via the reciprocity map $E^\times \to \mathrm{Gal}(\overline{\mathbb{Q}}_p/E)$ in local class field theory.

Proof. With the element v defined as above, we can compute $\phi_{\mathfrak{M}_m} v =$

$$\begin{aligned}
& (N_{\Phi,E(u),B(\kappa_E)\otimes_{\mathbb{Q}_p}F(u)}(h^{(M-1)}(u)))^{\phi^N+\phi^{N-1}+\cdots+\phi} \cdot \tfrac{1}{c_m} \cdot P_{\Phi^c,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u) e \\
= \; & N_{\Phi,E(u),B(\kappa_E)\otimes_{\mathbb{Q}_p}F(u)}(h^{(M-1)}(u^{p^N}))(N_{\Phi,E(u),B(\kappa_E)\otimes_{\mathbb{Q}_p}F(u)}(h^{(M-1)}(u)))^{\phi^{N-1}+\cdots+\phi} \cdot \\
& \tfrac{1}{c_m} \cdot P_{\Phi^c,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u) e \\
\equiv \; & N_{\Phi,E(u),B(\kappa_E)\otimes_{\mathbb{Q}_p}F(u)}(h_M(u))(N_{\Phi,E(u),B(\kappa_E)\otimes_{\mathbb{Q}_p}F(u)}(h^{(M-1)}(u)))^{\phi^{N-1}+\cdots+\phi+1} \cdot \\
& \tfrac{1}{c_m} \cdot P_{\Phi^c,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u) e \mod p^m \\
= \; & N_{\Phi,E(u),B(\kappa_E)\otimes_{\mathbb{Q}_p}F(u)}(\mathrm{Nm}_{E_m(u)/E(u)}(u-\pi_m)) \cdot \\
& \tfrac{1}{c_m} \cdot P_{\Phi^c,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u) v \\
= \; & P_{\Phi,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u) \cdot \tfrac{1}{c_m} \cdot P_{\Phi^c,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u) v \\
= \; & \tfrac{1}{c_m} E_m(u) v
\end{aligned}$$

Since $\phi_{\mathfrak{M}_m}$ commutes with the $\mathcal{O}_F$-action on $\mathfrak{M}_m$, (a) now follows. In particular, we have found $\#(\mathcal{O}_F/p^m) = m[F:\mathbb{Q}_p]$ different p^m-torsion points in $\mathcal{X}_m$. Since

$\mathrm{ht}(\mathcal{X}_m) = [F : \mathbb{Q}_p]$, all the p^m-torsion points on $(\mathcal{X}_m)_{\overline{\mathbb{Q}}_p}$ are rational over E_m. By the construction of $h_M(x)$ and π_m, we can check $\mathrm{Nm}_{E_m/E}(-\pi_m) = -\pi_E$. By Proposition 5.1.8 we know $\mathcal{X} \times_{\mathrm{Spec}\,\mathcal{O}_E} \mathrm{Spec}\,\mathcal{O}_{E_m}$ is $\mathcal{O}_F$-linearly isomorphic to $\mathcal{X}_m$ and (b) is proved.

The correspondence in (c) is obviously bijective. To check $\#\mathcal{G}_A = \#A$, recall we have proved in Proposition 3.2 that $\#\mathcal{G}_A = p^{\mathrm{length}_{\mathfrak{S}^0}\mathfrak{N}_A^0}$, and it is clear that $\#A = p^{\mathrm{length}_{\mathbb{Z}}A}$. If we look at the natural filtration $0 \subset \mathfrak{N}_A^0[p] \subset \mathfrak{N}_A^0[p^2] \subset \cdots \subset \mathfrak{N}_A^0[p^m] = \mathfrak{N}_A^0$, each subquotient $\mathfrak{N}_A^0[p^i]/\mathfrak{N}_A^0[p^{i-1}]$ is equal to $k((u))\{\overline{\eta \cdot v_m} | \eta \in A[p^i]\}$. Its dimension over $k((u))$ is equal to $\dim_{\mathbb{F}_p} A[p^i]/A[p^{i-1}]$. This implies

$$\mathrm{length}_{\mathfrak{S}^0}\mathfrak{N}_A^0 = \sum_{i=1}^{m} \dim_{k((u))} \mathfrak{N}_A^0[p^i]/\mathfrak{N}_A^0[p^{i-1}] = \sum_{i=1}^{m} \dim_{\mathbb{F}_p} A[p^i]/A[p^{i-1}] = \mathrm{length}_{\mathbb{Z}}A$$

To see (d), with the definition of S_τ, one can check

$$N_{\Phi,E(u),B(\kappa_E)\otimes_{\mathbb{Q}_p}F(u)}(f(u)) = (\prod_{\alpha\in S_\tau} \alpha_* f(u))_\tau$$

Then (d) follows from a careful examination of the definition of v under the identification $\mathfrak{M}_m \xrightarrow{\cong} \bigoplus_{\tau\in\mathrm{Hom}(B(\kappa_E)\cap F, B(\kappa_E))} \mathcal{O}_{B(\kappa_E)\cdot i_\tau(F)}[[u]]e_\tau$. □

Remark 5.2.5. Let d be a positive integer and $\sqrt[d]{\pi_m}$ be a d-th root of π_m. The minimal Eisenstein polynomial of $\sqrt[d]{\pi_m}$ over $B(\kappa_E)$ is $E_m(u^d)$, and its constant term is equal to pc_m. Let $\mathfrak{M}_{m,d}$ be the Kisin module constructed in (5.1) with $(E_m(\sqrt[d]{\pi_m}), \sqrt[d]{\pi_m})$. Its associated p-divisible group is naturally isomorphic to the base change of $\mathcal{X}_m$ to $\mathcal{O}_E[\sqrt[d]{\pi_m}]$. If we replace u with u^d in the definition of v

and denote it by $v(u^d)$, then all the solutions x to $\phi_{\mathfrak{M}_{m,d}}(x) = \frac{1}{c_m}E_m(u^d)x$ in $p^{-m}\mathfrak{M}_{m,d}/\mathfrak{M}_{m,d}$ have the form $\eta \cdot v(u^d)$, where η runs over $p^{-m}\mathcal{O}_F/\mathcal{O}_F$.

5.3 Some technical lemmas

We establish a few lemmas on properties of the polynomial $h^{(M-1)}(u)$. The properties will be stated in terms of Newton polygons.

Let us review the basic notions about Newton polygons: let (F, ν) be a discrete valuation field, $\mathcal{O}_F$ be the valuation ring. Let $f(t) = \sum_{i=r}^{d} a_i t^i \in F[t, t^{-1}]$, where $a_r, a_d \neq 0$. The *Newton polygon* $\mathrm{NP}(f)$ of $f(t)$ is the convex hull of $\bigcup_{i=r}^{d}(i, \nu(a_i)) + \mathbb{R}_+^2$, where $\mathbb{R}_+^2 := \{(x, y) \in \mathbb{R}^2 | x \geq 0, y \geq 0\}$. We define the *slopes* of $\mathrm{NP}(f)$ as the slopes of the segments on the boundary of the polygon to the left of $x = d$. If λ is a slope of $\mathrm{NP}(f)$, we define the *multiplicity* of λ as the length of the projection to x-axis of the corresponding segment.

If $f(t)$ is a polynomial over F, the valuation v on F uniquely extends to the splitting field of f. The slopes of a polynomial's Newton polygon are related with the valuations of its roots in the following way.

Proposition 5.3.1. *Suppose $f(t)$ is a monic polynomial with a nonzero constant term. If the valuations of all the nonzero roots of f are equal to $-\lambda_1 < -\lambda_2 < \cdots < -\lambda_k$ with multiplicities $a_1, a_2, \cdots, a_k$, respectively, then the slopes of $NP(f)$ are $\lambda_1 > \lambda_2 > \cdots > \lambda_k$ with lengths $a_1, a_2, \cdots, a_k$, respectively.*

Recall that the Minkowski sum of two sets S_1 and S_2 in a vector space is defined as $S_1 + S_2 := \{v_1 + v_2 | v_i \in S_i\}$. We have an immediate corollary from Proposition 5.3.1.

Corollary 5.3.2. *The Newton polygon NP(fg) is equal to the Minkowski sum NP(f) + NP(g).*

Let K be a field. For each formal power series $g(t) \in K((t))$, there exists a unique integer r such that $g(t) = x^r g_0(t)$ and $g_0(t) \in K[[t]]^\times$. We define this integer r to be the *order* of $g(t)$, denoted by $\mathrm{ord}_u g(t)$, or simply $\mathrm{ord}_u g$ for short. The following lemma will be extensively used in the future computations.

Lemma 5.3.3. *Let F be a p-adic local field with residue field κ_F, and π be a uniformizer in $\mathcal{O}_F$. Suppose $f(t) = \sum_{i=r}^{d} a_i t^i \in F[t, t^{-1}]$, where $a_r, a_d \neq 0$. Let $h := \min\{\nu(a_i) | r \leq i \leq d\}$. Let c_{il} be the unique elements in κ_F for $i = r, r+1, \cdots, d$ and $l = h, h+1, \cdots$ such that $a_i = \sum_{l=h}^{\infty} \pi^j \langle c_{il} \rangle$, where $\langle x \rangle$ is the Teichmuller lift for $x \in \kappa_F$. Define $g_j(t) := \sum_{i=r}^{d} \langle c_{ij} \rangle t^i$. Suppose the slopes of NP(f) are $\lambda_1 > \lambda_2 > \cdots \lambda_s$ with multiplicities $\alpha_1, \alpha_2, \cdots, \alpha_s$, respectively. Then we have the following estimates:*

$$ord_u g_l \geq d - \sum_{j=1}^{k-1} \alpha_j - (i - \sum_{j=1}^{k-1} \alpha_j), \quad if h - \sum_{j=1}^{k-1} \lambda_j \alpha_j < l < h - \sum_{j=1}^{k} \lambda_j \alpha_j, k = 1, 2, \cdots$$

$$ord_u g_l = d - \sum_{j=1}^{k} \alpha_j, \qquad if\, l = h - \sum_{j=1}^{k} \lambda_j \alpha_j, k = 0, 1, 2, \cdots$$

Proof. By the definitions of $g_j(u)$ we can write $f(t) = \sum_{j=h}^{\infty} \pi^j g_j(t)$. For each $l \geq h$, there exists a positive integer k such that $h - \sum_{j=1}^{k-1} \lambda_j \alpha_j \leq l < h - \sum_{j=1}^{k} \lambda \alpha_j$. First

suppose $h - \sum_{j=1}^{k-1} \lambda_j \alpha_j < l < h - \sum_{j=1}^{k} \lambda \alpha_j$. If $n = \min\{i | c_{i,l} \neq 0\}$, then $\nu(a_n) \leq i$. Because the point $P_n = (n, v(a_n))$ is inside the Newton polygon, we deduce that n is larger than or equal to the x-coordinate of the intersection of $\mathrm{NP}(f)$ with $y = i$. The x-coordinate of the intersection is equal to $d - \sum_{j=1}^{k-1} \alpha_j - (i - \sum_{j=1}^{k-1} \alpha_j)$ from the information on the slopes of $NP(f)$. Therefore $\mathrm{ord}_u g_l \geq d - \sum_{j=1}^{k-1} \alpha_j - (i - \sum_{j=1}^{k-1} \alpha_j)$. Second, suppose $l = h - \sum_{j=1}^{k} \alpha_j$ where k is a non-negative integer. Let $n_0 := d - \sum_{j=1}^{k} \alpha_j$. Because $(d - \sum_{j=1}^{k} \alpha_j, l)$ is a vertex on $\mathrm{NP}(f)$, $\nu(a_{n_0})$ must be equal to l, and any other n such that $\nu(a_n) = l$ must be larger than $d - \sum_{j=1}^{k} \alpha_j$. This proves the estimates on the orders of $g_l(u)$. □

Now we study the Newton polygons of the polynomials $h^{(M-1)}(u)$ and $h_M(u)$ that we have defined over E in (5.2). Choose the valuation ν on E such that $\nu(\pi_E) = 1$.

Proposition 5.3.4. *The following statements are true:*

(a) The vertices of $NP(h_M(u))$ are $(p^{MN} - p^{(M-1)N}, 0)$, $(0, 1)$, and the slope of $NP(h_M(u))$ is $-\frac{1}{(p^{MN} - p^{(M-1)N})}$ with multiplicity $p^{MN} - p^{(M-1)N}$.

(b) The vertices of $NP(h^{(M-1)}(u))$ are $(p^{(M-1)N}, 0), (p^{(M-2)N}, 1), \cdots, (1, M-1)$, the slopes of $NP(h^{(M-1)}(u))$ are $-\frac{1}{(p^{(M-1)N} - p^{(M-2)N})} > -\frac{1}{(p^{(M-2)N} - p^{(M-3)N})} > \cdots > -\frac{1}{(p^N - 1)}$, with multiplicites $p^{(M-1)N} - p^{(M-2)N}, p^{(M-2)N} - p^{(M-3)N}, \cdots, p^N - 1$, respectively.

(c) For any positive integer D, there exists $\widehat{h^{(M-1)}}(u) \in \mathcal{O}_E[u, u^{-1}]$ such that

$h^{(M-1)}(u)\widehat{h^{(M-1)}}(u) \equiv 1 \mod \pi_E^D$, *the vertices of* $NP(\widehat{h^{(M-1)}}(u))$ *are* $(-p^{(M-1)N}, 0)$, $(-Dp^{(M-1)N} + (D-1)p^{(M-2)N}, D-1)$, *and the slope of* $NP(\widehat{h^{(M-1)}}(u))$ *is equal to* $-\frac{1}{(p^{(M-1)N}-p^{(M-2)N})}$ *with multiplicity* $(D-1)(p^{(M-1)N} - p^{(M-2)N})$.

Proof. From the definition of $h_M(u)$ we know it is an Eisenstein polynomial of degree $(1-p^{-N})p^{MN}$, hence all its roots have valuation $\frac{1}{(1-p^{-N})p^{MN}}$, this proves (a) by Proposition 5.3.1. Since $h^{(M-1)}(u) = u\prod_{i=1}^{M-1} h_i(u)$, there are exactly $p^{iN} - p^{(i-1)N}$ roots of $h^{(M-1)}(u)$ with valuation $\frac{1}{p^{iN}-p^{(i-1)N}}$, this proves (b) by Corollary 5.3.2. Then apply Lemma 5.3.3 we deduce there exist $A_i(u) \in \mathcal{O}_E[u, u^{-1}]^\times$ for $i = 0, 1, \cdots, M-1$ such that $h^{(M-1)}(u) = \sum_{i=0}^{M-1} \pi_E^i A_i(u)$, and $\mathrm{ord}_u A_i = p^{(M-1-i)Nd}$. Note that $(h^{(M-1)}(u))^{-1}$ exists in the p-adic completion of $\mathcal{O}_E((u))$ as

$$(h^{(M-1)}(u))^{-1} = A_0^{-1}(1 + \sum_{k=1}^{\infty} A_0^{-1}A_k\pi_E^k)^{-1} = \sum_{k=0}^{\infty} \pi_E^k(\sum_{\substack{i_1+i_2+\cdots+i_t=k \\ i_j>0}} A_0^{-(t+1)}A_{i_1}\cdots A_{i_t})$$

If we define $\widehat{h^{(M-1)}}(u) := \sum_{k=0}^{D-1} \pi_E^k(\sum_{\substack{i_1+i_2+\cdots+i_t=k \\ i_j>0}} (-1)^t A_0^{-(t+1)}A_{i_1}\cdots A_{i_t})$, then $\widehat{h^{(M-1)}}$ is defined in $\mathcal{O}_E[u, u^{-1}]$. Let us estimate the order of $A_0^{-(t+1)}A_{i_1}\cdots A_{i_t}$. If $i_1 \geq 2$, then after replacing $(i_1, i_2, \cdots, i_t)$ with $(1, i_1 - 1, i_2, \cdots, i_t)$, the order will change by

$$-\mathrm{ord}_u A_0 + \mathrm{ord}_u A_1 + \mathrm{ord}_u A_{i_1-1} - \mathrm{ord}_u A_{i_1} < -p^{MN}(1-2p^{-N}) \leq 0$$

For the same reason, if $i_j > 1$ then after splitting i_j into 1 and $i_j - 1$, the order of $A_0^{-(t+1)}A_{i_1}\cdots A_{i_t}$ also decreases. Hence, among the indices $(i_1, i_2, \cdots, i_t)$ such that $i_1 + i_2 + \cdots + i_t = k$, the order of $A_0^{-(t+1)}A_{i_1}\cdots A_{i_t}$ is the lowest only when $t = k$ and $i_1 = i_2 = \cdots = i_k = 1$. Therefore $\mathrm{ord}_u(\sum_{\substack{i_1+i_2+\cdots+i_t=k \\ i_j>0}} A_0^{-(t+1)}A_{i_1}\cdots A_{i_t}) =$

$\mathrm{ord}_u A_0^{-(k+1)} A_1^k = -(k+1)p^{MN} + kp^{(M-1)N}$. (c) now follows. $\square$

Now suppose E is an unramified p-adic local field. Define the endomorphism ϕ on $E(u)$ such that $\phi|_E = \sigma$, and $\phi(u) = u^p$. If $i > 0$ and $f(u) \in E(u)$ can be written as $f_0(u^d)$ such that $p^i | d$, then $f(u)$ is contained in the image of $\phi^i : E(u) \to E(u)$, therefore $f(u)^{\phi^{-i}}$ is well-defined.

Lemma 5.3.5. *Suppose E is an unramified extension over $\mathbb{Q}_p$ and we take $\pi_E = p$. Let d, D be positive integers and suppose $D \leq M$. Suppose we have integers $x_1 > x_2 > \cdots > x_r > y_1 > y_2 > \cdots > y_s$, such that $p^{y_s} d$ is an integer. Let $l \leq r$ be the largest integer such that $x_l > y_1 + N$; we treat $l = 0$ if such an x_l does not exist. Then there exists $g_k \in E[u]$ for $k = 0, 1, \cdots, D-1$ such that* $h^{(M-1)}(u^d)^{\phi^{x_1} + \cdots + \phi^{x_r} - \phi^{x_1 - N} - \cdots - \phi^{x_l - N} - \phi^{y_1} - \cdots - \phi^{y_s}} \equiv \sum_{k=0}^{D-1} p^k g_k \mod p^D$ *with*

$$ord_u g_k \geq \begin{cases} dp^{(M-1)N}((1-p^{-N})(p^{k+1} + \cdots p^l) + p^{x_{l+1}} + \cdots + p^{x_r} - p^{y_1} - \cdots - p^{y_s}) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if} \quad 0 \leq k \leq l-1 \\ dp^{(M-1)N}(p^{x_{k+1}} + \cdots + p^{x_r} - p^{y_1} - \cdots - p^{y_s}) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if} \quad l \leq k \leq r-1 \\ dp^{(M-1)N}(-(k-r+1)p^{y_1} - \cdots - p^{y_s}) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if} \quad k \geq r \end{cases}$$

Proof. Replace $h^{(M-1)}(u^d)^{-1}$ by $h^{\widehat{(M-1)}}(u^d)$. Recall that $h^{(M-1)}(u^d)^{\phi^N - 1} \equiv h_M(u^d)$

mod p^M, we deduce

$$\begin{aligned} & h^{(M-1)}(u^d)^{\phi^{x_1}+\cdots+\phi^{x_r}-\phi^{x_1-N}-\cdots-\phi^{x_l-N}-\phi^{y_1}-\cdots-\phi^{y_s}} \\ \equiv\ & h_M(u^d)^{\phi^{x_1-N}+\phi^{x_2-N}+\cdots+\phi^{x_l-N}} h^{(M-1)}(u^d)^{\phi^{x_{l+1}}+\cdots+\phi^{x_r}} \widehat{h^{(M-1)}}(u^d)^{\phi^{y_1}+\cdots+\phi^{y_s}} \\ & \mod p^D \end{aligned}$$

By the definition of ϕ, for any $f(x) \in E[u, u^{-1}]$, the slopes of $\mathrm{NP}(f(u^d)^{\phi^i})$ are equal to the quotient of the slopes of $\mathrm{NP}(f)$ by $p^i d$. Hence by Lemma (5.3.4) the slopes of

$$\mathrm{NP}(h_M(u^d)^{\phi^{x_1-N}+\phi^{x_2-N}+\cdots+\phi^{x_l-N}} h^{(M-1)}(u^d)^{\phi^{x_{l+1}}+\cdots+\phi^{x_r}} \widehat{h^{(M-1)}}(u^d)^{\phi^{y_1}+\cdots+\phi^{y_s}})$$

are:

$$-\tfrac{1}{p^{x_1}(p^{(M-1)N}-p^{(M-2)N})d} > -\tfrac{1}{p^{x_2}(p^{(M-1)N}-p^{(M-2)N})d} > \cdots >$$

$$-\tfrac{1}{p^{x_r}(p^{(M-1)N}-p^{(M-2)N})d} > -\tfrac{1}{p^{y_1}(p^{(M-1)N}-p^{(M-2)N})d} > \cdots$$

The multiplicity of each slope $-\frac{1}{p^{x_i}(p^{(M-1)N}-p^{(M-2)N})d}$ is $p^{x_i}(p^{(M-1)N}-p^{(M-2)N})d$, and the multiplicity of $-\frac{1}{p^{y_1}(p^{(M-1)N}-p^{(M-2)N})d}$ is $(D-1)p^{y_1}(p^{(M-1)N}-p^{(M-2)N})d$. Then the statement follows by a direct application of Lemma 5.3.3. □

Chapter 6

Strong CM lifting to a p-adic CM type induced from an unramified local field

6.1 Main results of the Chapter

Definition 6.1.1. Let Γ_0 be a complete discrete valuation ring of characteristic 0 and residue characteristic p. Let κ_0 be the residue field of R_0. Let $\mathcal{X}$ be a p-divisible group over Γ_0. A finite subgroup G of $\mathcal{X}_{\kappa_0}$ is said to be *potentially liftable*, if there exists a finite extension Γ over Γ_0 with residue field κ, and a finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{X}_R$, such that $\mathcal{G}_\kappa = G_\kappa$.

Let F be a p-adic local field, π be a uniformizer in $\mathcal{O}_F$, e be the absolute

ramification index, κ_F be the residue field, and let $n := [\kappa_F : \mathbb{F}_p]$. In this section we prove the following theorem:

Theorem 6.1.2. *Let a be an integer such that $1 \leq a \leq n-1$. Let $i_0 \in Hom(F^{ur}, \overline{\mathbb{Q}}_p)$, $\Phi' := \{i_0, i_0 \circ \sigma, \cdots, i_0 \circ \sigma^{a-1}\} \subset Hom(F^{ur}, \overline{\mathbb{Q}}_p)$, and let Φ be the p-adic CM type on F induced from Φ'. Let $\mathcal{X}$ be the $\mathcal{O}_F$-linear CM p-divisible group over $W(k)$ with p-adic CM type Φ. Then every $\mathcal{O}_F$-stable subgroup G of $\mathcal{X}_k$ is potentially liftable.*

Theorem (6.1.2) has the following consequences:

Corollary 6.1.3. *Notations are as in (6.1.2). Then every $\mathcal{O}_F$-linear CM p-divisible group over k with dimension ae admits an F-linear CM lifting to characteristic 0 with p-adic CM type Φ.*

Proof. Every $\mathcal{O}_F$-linear CM p-divisible group Y over k with dimension ae is L-linearly isogeneous to $\mathcal{X}_k$, hence there exists an $\mathcal{O}_F$-stable subgroup G of $\mathcal{X}_k$ such that Y is $\mathcal{O}_F$-linearly isomorphic to $\mathcal{X}_k/G$. By Theorem (6.1.2), there exists a finite totally ramified extension R over $W(k)$ and a finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{X}_R$, such that $\mathcal{G}_k = G$. Then $\mathcal{X}_R/\mathcal{G}$ is an F-linear CM lifting of Y with p-adic CM type Φ. □

Remark 6.1.4. In the context of question (LTI) for p-divisible groups (see (3.1)), Corollary (6.1.3) implies $\mathrm{LTI}(F, \Phi) = \{$the set of Lie types of dimension $ae\}$. So the F-linear isogeny constraint is the only constraint on $\mathrm{LTI}(F, \Phi)$; cf. (3.1).

Corollary 6.1.5. *We have the following positive results on (sCML):*

(a) *Let K_0 be a p-adic local field, K be a degree 2 unramified extension of K_0. Then the answer to question (sCML) relative to (K, K_0) for p-divisible groups is affirmative.*

(b) *Let L be a CM field, and L_0 be its maximal totally real subfield. If for every place v of L_0 above p, v is inert in L, then for the CM field L the answer to question (sCML) for abelian varieties is affirmative.*

Proof. (b) follows from (a) by Proposition (3.1.3), so it suffices to prove (a). Let ι be the involution in $\mathrm{Aut}(K/K_0)$. Let e_K be the absolute ramification index of K, n_K be the inertia degree of K. The set of embeddings $\mathrm{Hom}(K^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$ is isomorphic to $\{1, 2, \cdots, n_K\}$ as $\mathrm{Gal}(K^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathbb{Z}/n_K$-torsors. The involution on $\{1, 2, \cdots, n_K\}$ induced by ι sends i to $i + \frac{n_K}{2} \mod n_K$. Take a p-adic CM type for K^{ur} to be $\Phi' := \{1, 2, \cdots, \frac{n_K}{2}\}$, and let Φ be the p-adic CM type for K induced from Φ'. Then Φ is compatible with ι, i.e., $\Phi \coprod \Phi \circ \iota = \mathrm{Hom}(K, \overline{\mathbb{Q}}_p)$. Now if Y is an $\mathcal{O}_K$-linear CM p-divisible group with dimension $[K_0 : \mathbb{Q}_p] = \frac{n_K}{2} \cdot e_K$, then by Corollary (6.1.3) we deduce that Y admits a K-linear CM lifting with p-adic CM type Φ compatible with ι. This proves (a). □

Here is the plan to prove Theorem (6.1.2). We have constructed the Kisin module of $\mathcal{X}$ in (5.1). For each $m \geq 1$, after a base change to the totally ramified abelian extension such that the p^m-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are rational, we have also computed the finite Kisin modules attached to the p^m-torsion finite locally free subgroup schemes in Proposition (5.2.4). If such a finite Kisin module reduces to

an $\mathcal{O}_F$-stable Dieudonné module by (3.2), then the associated finite locally free subgroup scheme is the lifting of an $\mathcal{O}_F$-stable subgroup.

6.2 Examples of potentially liftable subgroups

To illustrate the approach to prove Theorem (6.1.2), in this subsection we consider the example when $F = B(\mathbb{F}_{p^4})$ is unramified over $\mathbb{Q}_p$ of degree 4. Take an identification of $\mathrm{Hom}(F, B(k))$ with $\{1, 2, 3, 4\}$ as $\mathrm{Gal}(F/\mathbb{Q}_p) \cong \mathbb{Z}/4$-torsors. Take a p-adic CM type $\Phi = \{2, 3\}$. The reflex field F' is equal to F. Take $h(x) = px + x^{p^4}$, it satisfies the requirement in the theory of Lubin-Tate formal group laws as in (5.2). Follow the notations in (5.2), the Eisenstein polynomial $h_2(x) := \frac{h^{(2)}(x)}{h(x)} = \mathrm{p} + (px + x^{p^4})^{p^4-1}$ defines a totally ramified abelian extension F_2 over F with Galois group $\cong \mathcal{O}_F/p^2$. Note that the constant term of $h_2(x)$ is equal to p. Let π_2 be a root of $h_2(x)$, and take $R = \mathcal{O}_{F_2 \cdot B(k)} = W(k)[\pi_2]$. Let $\mathcal{X}$ be the $\mathcal{O}_F$-linear CM p-divisible group over R with p-adic CM type Φ, so the p^2-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are rational over Frac R. Let X be the closed fiber of $\mathcal{X}$. We will show some examples of liftable $\mathcal{O}_F$-stable subgroups of X.

The Kisin module attached to $\mathcal{X}$ is isomorphic to $\mathfrak{M} \cong \bigoplus_{i=1}^{4} W(k)[[u]]e_i$, where $\mathcal{O}_F$ acts on the i-th component by the embedding i. For simplicity we identify $\mathcal{O}_F$ with its image in $W(k)$ under the first embedding. By (5.2.4 (d)), the ϕ-linear homomorphism $\phi_{\mathfrak{M}}$ is defined as $\phi_{\mathfrak{M}} e_i = e_{i+1}$ if $i = 1, 2$, and $\phi_{\mathfrak{M}} e_i = h_2(u) e_{i+1}$ if $i = 3, 4$. Here we have identified e_{j+4} with e_j.

By Proposition (5.2.4(d)), the solutions to $\phi_{\mathfrak{M}}(x) = h_2(u)x$ in $p^{-2}\mathfrak{M}/\mathfrak{M}$ have the form $\eta \cdot v$ where $\eta \in p^{-2}\mathcal{O}_F/\mathcal{O}_F$, and

$$v := h(u)^{\phi^3+\phi^2}e_1 + h(u)^{\phi^3+1}e_2 + h(u)^{\phi+1}e_3 + h(u)^{\phi^2+\phi}e_4$$

where ϕ is the endomorphism on $W(k)$ that induces σ on $W(k)$ and sends u to u^p. Note that by our definition, the coefficients of $h(u)$ are in fact integers in $\mathbb{Z}$, therefore $h(u)^{\phi} = h(u^p)$.

The finite Kisin modules attached to p^2-torsion subgroup schemes of $\mathcal{X}$ are given by $\mathfrak{N}_A := W(k)((u))\{\eta \cdot v | \eta \in A\} \cap p^{-2}\mathfrak{M}/\mathfrak{M}$ where A runs over all the subgroups of $p^{-2}\mathcal{O}_F/\mathcal{O}_F$. The Dieudonné module of the closed fiber is given by $\mathfrak{N}_A/(\mathfrak{N}_A \cap u(p^{-2}\mathfrak{M}/\mathfrak{M})) \cong (\mathfrak{N}_A + u(p^{-2}\mathfrak{M}/\mathfrak{M}))/u(p^{-2}\mathfrak{M}/\mathfrak{M})$, which we denote by "$\mathfrak{N}_A \mod u$" from now on for simplicity.

On the other hand, the Dieudonné module of $X := \mathcal{X}_k$ is isomorphic to $M := \mathfrak{M}/u\mathfrak{M} \cong \bigoplus_{i=1}^{4} M_i = \bigoplus_{i=1}^{4} W(k)e_i$, where $\mathcal{O}_F$ acts by the i-th embedding on the i-th component, $Fe_i = e_{i+1}$ for $i = 1, 2$, $Fe_i = pe_{i+1}$ for $i = 3, 4$, $Ve_{i+1} = pe_i$ for $i = 1, 2$, and $Ve_{i+1} = e_i$ for $i = 3, 4$. Let us look at a few examples of the Dieudonné modules attached to $\mathcal{O}_F$-stable subgroups of X, and show they are liftable.

Example 6.2.1. Let $N := p^{-1}M_3/M_3$, it is an $\mathcal{O}_F$-stable Dieudonné module. Consider $p^{-1}v =$

$$\begin{aligned} &p^{-1}((u^{p^4}+pu)^{\phi^3+\phi^2}e_1 + (u^{p^4}+pu)^{\phi^3+1}e_2 + (u^{p^4}+pu)^{\phi+1}e_3 + (u^{p^4}+pu)^{\phi^2+\phi}e_4) \\ &\equiv p^{-1}u^{p^7+p^6}e_1 + p^{-1}u^{p^7+p^4}e_2 + p^{-1}u^{p^5+p^4}e_3 + p^{-1}u^{p^6+p^5}e_4 \mod \mathfrak{M} \end{aligned}$$

Therefore $u^{-(p^5+p^4)}(p^{-1}v) \equiv p^{-1}e_3 \mod u$. Therefore if we take $A := \langle p^{-1} \rangle$, then $\mathfrak{N}_A \mod u = N$. Since the associated finite group scheme $\mathcal{G}_A$ has order p, we deduce that $\mathfrak{N}_A \mod u = N$. In fact, the reduction of any cyclic subgroup scheme of $\mathcal{X}$ with order p is equal to the finite subgroup of X associated to N.

Remark 6.2.2. We have actually shown a stronger fact $u^{-(p^5+p^4)}(p^{-2}v) \equiv p^{-1}e_3 \mod u^{p^6-p^4}\mathfrak{M}$. This fact will be useful later.

Example 6.2.3. Let $N := p^{-1}M_3/M_3 \oplus p^{-1}M_4/M_4$, it is an $\mathcal{O}_F$-stable Dieudonné module. For any $\eta_1 = p^{-1}\zeta_1$ with $\zeta_1 \in W(\mathbb{F}_{p^4})^\times$, we have

$$\eta_1 \cdot v \equiv p^{-1}\zeta_1 u^{p^7+p^6}e_1 + p^{-1}\zeta_1^{\sigma} u^{p^7+p^4}e_2 + p^{-1}\zeta_1^{\sigma^2} u^{p^5+p^4}e_3 + p^{-1}\zeta_1^{\sigma^3} u^{p^6+p^5}e_4 \mod \mathfrak{M}$$

We have seen $\mathfrak{N}_{\langle \eta_1 \rangle}/u\mathfrak{N}_{\langle \eta_1 \rangle} = p^{-1}M_3/M_3$, so we need another $\eta_2 \in p^{-2}\mathcal{O}_F/\mathcal{O}_F$ to produce a lifting of $p^{-1}e_4$. If $\zeta_2 \in W(\mathbb{F}_{p^4})^\times$ is $\mathbb{Z}_p$-linearly independent from ζ_1, then there exists $\lambda_1, \lambda_2 \in W(\mathbb{F}_{p^4})$ such that $\lambda_1\zeta_1 + \lambda_2\zeta_2 = 0$, $\lambda_1\zeta_1^{\sigma} + \lambda_2\zeta_2^{\sigma} = 1$. Thus modulo $\mathfrak{M}$ we have

$$\begin{aligned} & \lambda_1^{\sigma^3}(p^{-1}\zeta_1 \cdot v) + \lambda_2^{\sigma^3}(p^{-1}\zeta_2 \cdot v) \\ \equiv\ & p^{-1}(\lambda_1^{\sigma^3}\zeta_1 + \lambda_2^{\sigma^3}\zeta_2)u^{p^7+p^6}e_1 + p^{-1}(\lambda_1^{\sigma^3}\zeta_1^{\sigma} + \lambda_2^{\sigma^3}\zeta_2^{\sigma})u^{p^7+p^4}e_2 + p^{-1}u^{p^6+p^5}e_4 \end{aligned}$$

Therefore $u^{-(p^6+p^5)}(\lambda_1^{\sigma^3}(p^{-1}\zeta_1 \cdot v) + \lambda_2^{\sigma^3}(p^{-1}\zeta_2 \cdot v)) \equiv p^{-1}e_4 \mod u$. If we take $A := \langle p^{-1}\zeta_1 \rangle \times \langle p^{-1}\zeta_2 \rangle$, then $\mathfrak{N}_A \mod u = p^{-1}M_3/M_3 \oplus p^{-1}M_4/M_4 = N$.

Example 6.2.4. Let $N := p^{-1}M_2/M_2 \oplus p^{-1}M_3/M_3$, it is an $\mathcal{O}_F$-stable Dieudonné module. This time we base change to $\mathcal{X} \times_{\operatorname{Spec} W(k)[\pi_2]} \operatorname{Spec} W(k)[\sqrt[p]{\pi_2}]$ to carry out the computation[1], where $\sqrt[p]{\pi_2}$ is a p-th root of π_2. Let $\mathfrak{M}'$ be the Kisin module

[1]Note that every p^2-torsion subgroup of $\mathcal{X}' := \mathcal{X} \times_{\operatorname{Spec} W(k)[\pi_2]} \operatorname{Spec} W(k)[\sqrt[p]{\pi_2}]$ is the base

attached to $\mathcal{X} \times_{\operatorname{Spec} W(k)[\pi_2]} \operatorname{Spec} W(k)[\sqrt[p]{\pi_2}]$. By Remark (5.2.5), if we replace u with u^p in the formula for v and denote it by $v' := v(u^p)$, then the p^2-torsion points on $\mathcal{X}'$ correspond to $\eta \cdot v'$, where $\eta \in p^{-2}\mathcal{O}_F/\mathcal{O}_F$. Take $A := \langle p^{-2} \rangle$. By Example (6.2.1), we already have $u^{-(p^6+p^5)}(p^{-1}v')$ in $\mathfrak{N}_A$ as a lifting of $p^{-1}e_3$, and we need to find another element in $\mathfrak{N}_A$ to lift $p^{-1}e_2$. Consider

$$\begin{aligned} p^{-2}v' &= p^{-2}(h(u^p)^{\phi^3+\phi^2}e_1 + h(u^p)^{\phi^3+1}e_2 + h(u^p)^{\phi+1}e_3 + h(u^p)^{\phi^2+\phi}e_4) \\ &= p^{-2}(h(u)^{\phi^4+\phi^3}e_1 + h(u)^{\phi^4+\phi}e_2 + h(u)^{\phi^2+\phi}e_3 + h(u)^{\phi^3+\phi^2}e_4) \end{aligned}$$

By Corollary 5.2.3, $h(u)^{\phi^4-1} \equiv h_2(u) \mod p^2$, hence in $\mathfrak{N}_A^0$ we know $h(u)^{-\phi-1}(p^{-2}v')$ is equal to

$$\begin{aligned} & p^{-2}(h(u)^{\phi^4+\phi^3-\phi-1}e_1 + h_2(u)e_2 + h(u)^{\phi^2-1}e_3 + h(u)^{\phi^3+\phi^2-\phi-1}e_4) \\ \equiv\ & (p^{-2}u^{p^8+p^7-p^5-p^4} + p^{-1}(u^{p^7-p^5} + u^{p^8-p^5-p^4+p^3} - u^{p^8+p^7-p^5-2p^4+1} - \\ & u^{p^8+p^7-2p^5-p^4+p}))e_1 + (p^{-2}u^{p^8-p^4} + p^{-1}(1 - u^{p^8-2p^4+1}))e_2 + (p^{-2}u^{p^6-p^4} + \\ & p^{-1}(u^{-p^4+p^2} - u^{p^6-2p^4+1}))e_3 + (p^{-2}u^{p^7+p^6-p^5-p^4} + p^{-1}(u^{p^6-p^5-p^4+p^3} + \\ & u^{p^7-p^5-p^4+p^2} - u^{p^7+p^6-p^5-2p^4+1} - u^{p^7+p^6-2p^5-p^4+p}))e_4 \end{aligned}$$

This vector is not yet in $p^{-2}\mathfrak{M}/\mathfrak{M}$ since the coefficient of e_3 has a negative order in u. However, since $u^{-(p^6+p^5)}(p^{-1}v')$ is a lifting of $p^{-1}e_3$, we can use it to "strike out" the coefficient of $p^{-1}e_3$. Let $w := h(u)^{-\phi-1}(p^{-2}v') - (u^{-p^4+p^2} - u^{p^6-2p^4+1}) \cdot$

change of a p^2-torsion subgroup of $\mathcal{X}$, so to lift the associated subgroup of X to a finite locally free p^2-torsion subgroup scheme of $\mathcal{X} \times_{\operatorname{Spec} W(k)[\pi_2]} \operatorname{Spec} W(k)[\sqrt[p]{\pi_2}]$ is the same as to lift it to a finite locally free p^2-torsion subgroup scheme of $\mathcal{X}$. We make the base change here for the aim of convenience in computation.

$u^{-(p^6+p^5)}(p^{-1}v')$, then we have

$$\begin{aligned} w &= (h(u)^{-\phi-1}(p^{-2}v') - p^{-1}(u^{-p^4+p^2} - u^{p^6-2p^4+1})e_3) - \\ &\quad (u^{-p^4+p^2} - u^{p^6-2p^4+1})(u^{-(p^6+p^5)}(p^{-1}v') - p^{-1}e_3) \end{aligned}$$

We have seen the first term in the sum is in $p^{-2}\mathfrak{M}/\mathfrak{M}$ and it reduces to $p^{-1}e_2$ modulo u, and by Remark (6.2.2) we know the second term is divisible by $u^{p^7-p^5-p^4+p^2}$. Therefore we deduce $w \equiv p^{-1}e_2 \mod u$. This proves $\mathfrak{N}_A \mod u = p^{-1}M_2/M_2 \oplus p^{-1}M_3/M_3 = N$.

6.3 The correspondence between subgroups and Lie types

To prove Theorem (6.1.2), we need a description of the Dieudonné modules attached the $\mathcal{O}_F$-stable subgroups of an $\mathcal{O}_F$-linear CM p-divisible group. Such a description also allows us to write down the Lie type of the quotient $\mathcal{O}_F$-linear CM p-divisible group directly from the $\mathcal{O}_F$-stable subgroup. We take this subsection to set up some definitions on such a description.

Let F be a p-adic local field. Let X be an $\mathcal{O}_F$-linear CM p-divisible group with Lie type δ. In the natural isomorphism $R_k(\mathcal{O}_F) \cong \prod_{\tau\in\mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)} R_k(\mathcal{O}_F \otimes_{\mathcal{O}_{F^{\mathrm{ur}}},\tau} k) \xrightarrow{\prod \epsilon_\tau} \prod_{\tau\in\mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)} \mathbb{Z}$ (see (3.1)), denote the image of δ by $(\delta_\tau)_{\tau\in\mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)}$. The Dieudonné module attached to X_δ is

$$M_\delta \cong \bigoplus_{\tau\in\mathrm{Hom}(F,\overline{\mathbb{Q}}_p)} M_{\delta,\tau}$$

where $M_{\delta,\tau} \cong W(k) \otimes_{\tau,\mathcal{O}_F^{\mathrm{ur}}} \mathcal{O}_F e_\tau$ is a free $W(k) \otimes_{\tau,\mathcal{O}_{F^{\mathrm{ur}}}} \mathcal{O}_F$-module of rank 1. The Frobenius and Verschiebung maps satisfy $FM_{\delta,\tau} = \pi_F^{e-\delta_{\sigma\tau}} M_{\delta,\sigma\tau}$ and $VM_{\delta,\sigma\tau} = \pi_F^{\delta_{\sigma\tau}} M_{\delta,\tau}$.

If G is an $\mathcal{O}_F$-stable subgroup of X, then its attached Dieudonné module is $\bigoplus_{\tau\in\mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)} \pi_F^{-d_\tau} M_{\delta,\tau}/M_{\delta,\tau}$, where the d_τ's are non-negative integers. This module is stable under F and V, this implies

$$\delta_{\sigma\tau} - e_F \leq d_{\sigma\tau} - d_\tau \leq \delta_{\sigma\tau}, \text{ for all } \tau \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$$

Definition 6.3.1. Let $\delta = (\delta_\tau)_{\tau\in Hom(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)}$ be a Lie type. A vector of non-negative integers

$$\underline{d} = (d_\tau)_{\tau\in Hom(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)} \in \bigoplus_{\tau\in Hom(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)} \mathbb{N}_\tau$$

is defined to be *δ-admissible*, if $\delta_{\sigma\tau} - e \leq d_{\sigma\tau} - d_\tau \leq \delta_{\sigma\tau}$ for all τ. It is said to be *δ-admissible and reduced*, if moreover we have $\min d_\tau = 0$. Two δ-admissible $\underline{d}$ and $\underline{d'}$ are called *equivalent*, if $d_\tau - d'_\tau$ is a constant that does not depend on τ.

If $\underline{d} = (d_\tau)$ is δ-admissible, we denote $N_\delta(\underline{d}) := \bigoplus_{\tau\in Hom(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)} (\pi_F^{-d_\tau} M_{\delta,\tau}/M_{\delta,\tau})$ and let $G(\underline{d})$ be the associated finite subgroup scheme of X_δ. We also denote the Dieudonné module $M(\underline{d}) := \bigoplus_{\tau\in Hom(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)} \pi_F^{-d_\tau} M_{\delta,\tau}$, and let $X(\underline{d})$ be the associated p-divisible group over k. Clearly from the definition we have:

Proposition 6.3.2. *The mapping $[\underline{d}] \mapsto X(\underline{d})$ is a one-to-one correspondence between the equivalent classes of δ-admissible vectors and the $\mathcal{O}_F$-isomorphic classes of $\mathcal{O}_F$-linear p-divisible groups isogeneous to X_δ. Moreover, the Lie type $[Lie(X(\underline{d}))] = (\delta_\tau - d_\tau + d_{\sigma^{-1}\tau})_{\tau\in Hom(F^{ur},\overline{\mathbb{Q}}_p)} \in R_k(\mathcal{O}_F)$.*

6.4 The proof of Theorem (6.1.2)

In this subsection we prove Theorem (6.1.2). Notations are as in the beginning of the section. We first claim it suffices to prove in the case when F is unramified over $\mathbb{Q}_p$. To see this, recall that Φ is induced from the p-adic CM type Φ' for F^{ur}. Let $\mathcal{Y}$ be the $\mathcal{O}_{F^{ur}}$-linear p-divisible group over $W(k)$ with p-adic CM type Φ', then $\mathcal{X}$ is $\mathcal{O}_F$-linearly isomorphic to the Serre tensor construction $\mathcal{Y} \otimes_{\mathcal{O}_{F^{ur}}} \mathcal{O}_F$. Now suppose G is an $\mathcal{O}_F$-stable finite subgroup of $\mathcal{X}_k$. The following lemma (6.4.1) reduces the potential liftablity of G to an $\mathcal{O}_{F^{\mathrm{ur}}}$-stable finite subgroup of $\mathcal{Y}_k$.

Lemma 6.4.1. *Let F/F_0 be a totally ramified finite extension of degree d between p-adic local fields, and π be a uniformizer of F. Let Y be an $\mathcal{O}_{F_0}$-linear CM p-divisible group over k, and $X := Y \otimes_{\mathcal{O}_{F_0}} \mathcal{O}_F$ be the Serre tensor construction. Let $Y \hookrightarrow X$ be the canonical embedding, and Y_i be the image of Y under the endomorphism $\pi^i \in End(X)$ for $i = 0, 1, \cdots, d-1$. Then for every $\mathcal{O}_F$-stable finite subgroup $G \subset X$, there exists an $\mathcal{O}_{F_0}$-stable finite subgroup $G_i \subset X_i$ for $i = 0, 1, \cdots, d-1$, such that $G = \prod_{i=0}^{d-1} G_i$.*

Proof. The Dieudonné module N attached to Y splits into $\bigoplus_{\tau \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)} N_\tau$, where N_τ is a free $W(k) \otimes_{\tau, \mathcal{O}_F^{\mathrm{ur}}} \mathcal{O}_{F_0}$-module of rank 1. Let $M_\tau := \mathcal{O}_F \otimes_{\mathcal{O}_{F_0}} N_\tau$, then the Dieudonné module M attached to X is naturally isomorphic to $\bigoplus_{\tau \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)} M_\tau$. Let $N_{\tau,i} := \mathcal{O}_{F_0}\pi^i \otimes_{\mathcal{O}_{F_0}} N_\tau$ for $i = 0, 1, \cdots, d-1$, then the Dieudonné module attached to Y_i is $\bigoplus_{\tau \in \mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)} N_{\tau,i}$.

Since G is $\mathcal{O}_F$-stable, there exists a sequence of non-negative integers $(\underline{a_\tau})$ such

that the Dieudonné module attached to G is $\bigoplus_{\tau\in\mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)}\pi^{-a_\tau}M_\tau/M_\tau$. Let π_0 be a uniformizer of $\mathcal{O}_{F_0}$. Note that $\pi^{-a_\tau}M_\tau/M_\tau=\bigoplus_{i=0}^{d-1}\pi_0^{-[\frac{a_\tau+i}{d}]}N_{\tau,i}/N_{\tau,i}$. For each i, define $P_i:=\bigoplus_{\tau\in\mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}}_p)}\pi_0^{-[\frac{a_\tau+i}{d}]}N_{\tau,i}/N_{\tau,i}$ as a submodule in $p^{-\infty}N_{\tau,i}/N_{\tau,i}$. Since Y is $\mathcal{O}_F$-stable, we know the Frobenius endomorphism F sends $N_{\tau,i}$ to $\pi_0^{\delta_\tau}N_{\tau,i}$ for some integer δ_τ, hence on M we know F sends M_τ to $\pi^{d\delta_\tau}M_{\sigma\tau}$. Therefore $a_\tau-d\delta_\tau\le a_{\sigma\tau}$. This implies $[\frac{a_\tau+i}{d}]-\delta_\tau\le[\frac{a_{\sigma\tau}+i}{d}]$, hence P_i is a finite Dieudonné module.

Let G_i be the finite subgroup of X_i that corresponds to P_i. Then G_i is $\mathcal{O}_{F_0}$-stable, and $G=\prod_{i=0}^{d-1}G_i$. □

From now on we may and do assume that F is unramified over $\mathbb{Q}_p$. Take an identification between the $\mathrm{Gal}(F/\mathbb{Q}_p)\cong\mathbb{Z}/n$-torsors $\mathrm{Hom}(F,B(k))$ and $\{1,2,\cdots,n\}$, such that $\Phi=\{2,3,\cdots,a+1\}$. The reflex field F' of (F,Φ) is equal to F. Take $h(x)=px+x^{p^n}$, and construct $h^{(r)}(x),h_r(x)$ for all positive integers r as in (5.2). Let π_n be a root of $h_n(x)$, and $\sqrt[p^n]{\pi_n}$ be a p^n-th root of π_n. Define $R:=W(k)[\sqrt[p^n]{\pi_n}]$. Let $\mathfrak{M}$ be the Kisin module constructed in §5 over R using the uniformizer $\sqrt[p^n]{\pi_n}$, and let $\mathcal{X}$ be the associated p-divisible group. By (5.2.4) all p^n-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are already rational over Frac R. By Proposition (5.2.4) and Remark (5.2.4(d)), the p^n-torsion points on $\mathcal{X}$ are in one-to-one correspondence with $\{\eta\cdot v|\eta\in p^{-n}\mathcal{O}_F/\mathcal{O}_F\}$, where $v=\sum_{i=1}^{a}h^{(n-1)}(u^{p^n})^{\phi^{n-1}+\phi^{n-2}+\cdots+\phi^{n-a-1+i}+\phi^{i-2}+\phi^{i-3}+\cdots+1}e_i+\sum_{i=a+1}^{n}h^{(n-1)}(u^{p^n})^{\phi^{i-2}+\phi^{i-3}+\cdots+\phi^{i-a-1}}e_i$.

Let $X:=\mathcal{X}_k$ be the closed fiber, it is the $\mathcal{O}_F$-linear CM p-divisible group over k

with Lie type $\xi(\Phi)$. From the definition of Φ, if a vector of integers $\underline{d} = (d_i)_{i=1,2,\cdots,n}$ is $\xi(\Phi)$-admissible, then $0 \leq d_{i+1} - d_i \leq 1$ when $1 \leq i \leq a$, and $-1 \leq d_{i+1} - d_i \leq 0$ when $a+1 \leq i \leq n$. Define $q_i := \min\{i-1, n+1-i, a, n-a\}$ for each $i = 1, 2, \cdots, n$. One can easily check that for a positive integer r, there exists a reduced $\xi(\Phi)$-admissible $\underline{d} \in \mathbb{N}^n$ such that the i-th component d_i is equal to r if and only if $1 \leq r \leq q_i$.

Take a set of $\mathbb{Q}_p$-basis $\{\zeta_i | i = 1, 2, \cdots, n\}$ of $F^{\mathrm{ur}} = B(\mathbb{F}_{p^n})$, without loss of generality we may assume $\zeta_i \in W(\mathbb{F}_{p^n})^\times$. By Dedekind's Theorem the matrix $[\zeta_i^{\sigma^j}]_{0 \leq i,j \leq n-1}$ is non-degenerating. Hence we can rearrange the order of the rows such that for any $1 \leq l \leq n$, the submatrix formed by first l rows and l columns is non-degenerating. So there exists a unique vector $\underline{\lambda_l} = (\lambda_{l,0}, \lambda_{l,1}, \cdots, \lambda_{l,l})$ in $(W(k))^{l+1}$ such that $(\lambda_{l,0}, \lambda_{l,1}, \cdots, \lambda_{l,l}) \cdot [\zeta_i^{\sigma^j}]_{0 \leq i,j \leq l} = (0, 0, \cdots, 0, 1)$.

Definition 6.4.2. Suppose (s, r) is a pair of integers such that $1 \leq s \leq n, 1 \leq r \leq q_s$. Define

$$A_s^{(r)} := \begin{cases} \prod_{i=0}^{r+s-a-2} \langle p^{-r} \zeta_i \rangle, & \text{if } \ s \geq a+1 \\ \prod_{i=0}^{r-1} \langle p^{-(a+1-s+r)} \zeta_i \rangle, & \text{if } \ s \leq a \end{cases}$$

as subgroups of $p^{-n}\mathcal{O}_F / \mathcal{O}_F$.

Define integers

$$D(s,r) := \begin{cases} p^{n^2}(p^{s-1} - p^{s+r-a-2} - p^{s+r-a-3} - \cdots - p^{s-a-1}) \\ \qquad\qquad \text{if } \ a+1 \le s \le n, s+r \le n \\ p^{n^2}(p^{s-1} - p^{s-2} - p^{s-3} - \cdots - p^{s-a-1}) \\ \qquad\qquad \text{if } \ a+1 \le s \le n, s+r = n+1 \\ p^{n^2}(p^{s-1} - p^{r-1} - p^{r-2} - \cdots - p^{s-a-1}) \\ \qquad\qquad \text{if } \ 1 \le s \le a, r \le n-1-a \\ p^{n^2}(p^{s-1} - p^{s-2} - p^{s-3} - \cdots - p^{s-a-1}) \\ \qquad\qquad \text{if } \ 1 \le s \le a, r = n-a \end{cases}$$

From the definition it is clear that $D(s,r) > 0$.

For an element $x \in p^{-n}\mathfrak{M}^0/\mathfrak{M}^0$, we define $\mathrm{ord}_u x$ to be the smallest integer d such that $u^{-d}x \in p^{-n}\mathfrak{M}/\mathfrak{M}$ and $u^{-d}x \neq 0 \mod u$. If $\mathrm{ord}_u(x_1 - x_2) \ge D$, we write $x_1 \equiv x_2 \mod \mathrm{ord}_u \ge D$.

Proposition 6.4.3. *For each pair of (s,r) that satisfies the condition in (6.4.2), there exists $w_s^{(r)} \in \mathfrak{N}_{A_s^{(r)}}$ such that $w_s^{(r)} \equiv p^{-r}e_s \mod ord_u \ge D(s,r)$.*

Proof. We divide the problem into the case when $a+1 \le s \le n$ and $1 \le s \le a$.

(i) First suppose $a+1 \le s \le n$. Prove by induction on r. Suppose $1 \le r \le \min\{s-1, n+1-s, a, n-a\}$ and we have proved for smaller r's. Define

$$v^* := \sum_{k=0}^{s+r-a-2} \lambda_{s+r-a-2,k}^{\sigma^{a+2-r}} h^{(n-1)}(u^{p^n})^{-\phi^{s-2}-\cdots-\phi^{s-a-1}}(p^{-r}\zeta_k \cdot v)$$

Then by the choice of $\underline{\lambda_{s+r-a-2}}$ one can easily check that the coefficient of e_i in

$v^* - p^{-r}e_s$ vanishes for $a+2-r \le i \le s$. Now we examine the coefficients for e_i with $i \le a+1-r$ or $i \ge s+1$.

When $1 \le i \le a+1-r$, the coefficient of e_i is equal to the product of $p^{-r}(\sum_{k=0}^{s+r-a-2} \lambda_{s+r-a-2,k}^{\sigma^{a+2-r}} \zeta_k^{\sigma^i})$ with

$$h^{(n-1)}(u^{p^n})^{\phi^{n-1}+\cdots+\phi^{\max\{s-1,n-a-1+i\}}-\phi^{\min\{s-2,n-a-2+i\}}-\cdots-\phi^{\max\{s-a-1,i-1\}}+\phi^{\min\{s-a-2,i-2\}}+\cdots+1}$$

The number of $h^{(n-1)}(u^{p^n})^{\phi^j}$-factors with $j>0$ is equal to $(n-1)-\max\{s-1, n-a-1+i\}+1$. Because $r \le \min\{s-1, n+1-s, a, n-a\}$ implies $s-1 \le n-r$, and $i \le a+1-r$ implies $n-a-1+i \le n-r$, we have $(n-1)-\max\{s-1, n-a-1+i\}+1 \ge (n-1)-(n-r)+1 = r$. Hence by Lemma 5.3.5, we can write this coefficient as $p^{-r}(g_0 + pg_1 + p^2g_2 + \cdots + p^{r-1}g_{r-1})$, such that

$$\mathrm{ord}_u g_k \;\ge\; p^{n^2}(p^{\max\{s-1,n-a-1+i\}} - p^{\min\{s-2,n-a-2+i\}} - \cdots - p^{\max\{s-a-1,i-1\}})$$

If $s+r \le n$, then $n-a-1+i \ge n-r \ge s$, hence the above lower bound is

$$\ge p^{n^2}(p^s - p^{s-2} - \cdots - p^{s-a-1}) \ge p^{n^2}(p^{s-1} - p^{s+r-a-2} - \cdots - p^{s-a-1}) = D(s,r)$$

If $s+r = n+1$, that lower bound is $\ge d(p^{s-1} - p^{s-2} - \cdots - p^{s-a-1}) = D(s,r)$, too.

Similarly, when $i \ge s+r+1$, we can also prove the order of the coefficient of e_i has order $\ge D(s,r)$.

When $s+1 \le i \le s+r$, by Lemma 5.3.5, the coefficient of e_i is equal to

$$\begin{aligned} & p^{-r}(\sum_{k=0}^{s+r-a-2} \lambda_{s+r-a-2,k}^{\sigma^{a+2-r}} \zeta_k^{\sigma^i}) h^{(n-1)}(u^{p^n})^{\phi^{i-2}+\cdots+\phi^{s-1}-\phi^{i-a-2}-\cdots-\phi^{s-a-1}} \\ = \;& p^{-r}(g_0 + pg_1 + p^2g_2 + \cdots + p^{r-1}g_{r-1}) \end{aligned}$$

with estimates on the order of the g_k's as follows. If $k \leq i-s-1$, we have $\mathrm{ord}_u g_k \geq p^{n^2}(p^{s-1} - p^{i-a-2} - \cdots - p^{s-a-1}) \geq D(s,r)$. If $i-s \leq k \leq r-1$, we deduce $\mathrm{ord}_u g_k \geq p^{n^2}(-(k-(i-s)+1)p^{i-a-2} - p^{i-a-3} - \cdots - p^{s-a-1})$.

So far we have been able to write v^* as

$$p^{-r}e_s + \sum_{\substack{i \leq a+1-r \\ \text{or} \\ i \geq s+r+1}} v_i^* e_i + \sum_{s+1 \leq i \leq s+r} \sum_{j=0}^{r-1} h_{i,j} p^{-r+j} e_i$$

knowing:

(a) when $i \leq a+1-r$ or $i \geq s+r+1$, $\mathrm{ord}_u v_i^* \geq D(s,r)$.

(b1) when $s+1 \leq i \leq s+r$ and $j \leq i-s-1$, $\mathrm{ord}_u h_{i,j} \geq D(s,r)$.

(b2) when $s+1 \leq i \leq s+r$ and $i-s \leq j \leq r-1$, $\mathrm{ord}_u h_{i,j} \geq p^{n^2}(-(j-(i-s)+1)p^{i-a-2} - \cdots - p^{s-a-1})$.

Now we define

$$w_s^{(r)} := v^* - \sum_{(i,j)\text{as in (b2)}} h_{i,j} w_i^{(r-j)}$$

Note that $r-j \leq r-i+s \leq \min\{i-1, n+1-i, a, n-a\}$, so by induction hypothesis we have constructed $w_i^{(r-j)} \in \mathfrak{N}^0_{A_i^{(r-j)}} = W(k)((u))\{p^{-(r-j)}\zeta_t \cdot v | 0 \leq t \leq i+(r-j)-a-2\}$. Because $i+(r-j) \leq i+r-(i-s) \leq r+s$, and $r-j < r$, hence we have $\mathfrak{N}^0_{A_i^{(r-j)}} \subset \mathfrak{N}^0_{A_s^{(r)}}$. Thus this $w_s^{(r)}$ is indeed defined in $\mathfrak{N}^0_{A_s^{(r)}}$. Next we verify $\mathrm{ord}_u(w_s^{(r)} - p^{-r}e_s) \geq D(s,r)$. Write $w_s^{(r)} - p^{-r}e_s =$

$$\sum_{\substack{i \leq a+1-r \\ \text{or} \\ i \geq s+r+1}} v_i^* e_i + \sum_{\substack{s+1 \leq i \leq s+r \\ j \leq i-s-1}} h_{i,j} p^{-r+j} e_i - \sum_{\substack{s+1 \leq i \leq s+r \\ j \geq i-s}} h_{i,j}(w_i^{(r-j)} - p^{-r+j}e_i)$$

We have shown the first two terms in the above formula have orders higher than or equal to $D(s,r)$. For the last term, by induction hypothesis $\mathrm{ord}_u(w_i^{(r-j)} - p^{-r+j}e_i) \geq$

$D(i, r-j)$, and we have shown $\mathrm{ord}_u h_{i,j} \geq d(-(j-(i-s)+1)p^{i-a-2} - p^{i-a-3} - \cdots - p^{s-a-1})$, therefore we are reduced to the inequality which is an easy exercise:

$$D(i, r-j) + p^{n^2}(-(j-(i-s)+1)p^{i-a-2} - p^{i-a-3} - \cdots - p^{s-a-1}) \geq D(s, r)$$

(ii) In the case when $1 \leq s \leq a$, we prove by a descending induction on s and an ascending induction on r. Suppose we have proved for a larger s and a smaller r. Define

$$v^* := \sum_{k=0}^{r-1} \lambda_{r-1,k}^{\sigma^{s-r+1}} h^{(n-1)}(u^{p^n})^{-\phi^{-1}-\phi^{-2}-\cdots-\phi^{-a-1+s}-\phi^{s-2}-\cdots-1}(\zeta_k \cdot v)$$

Note that $-a-1+s+n \geq 0$ so every factor is well defined. By the definition of $\underline{\lambda_{r-1}}$, the coefficient of e_i vanishes for $s-r+1 \leq i \leq s-1$.

The coefficient of e_s is equal to $p^{-(a+1-s+r)} h_n(u^{p^n})^{\phi^{-1}+\cdots+\phi^{-a-1+s}}$. Since $h_n(u)$ is an Eisenstein polynomial of degree $p^{n^2} - p^{n(n-1)}$, we can write

$$p^{-(a+1-s+r)} h_n(u^{p^n})^{\phi^{-1}+\cdots+\phi^{-a-1+s}} = p^{-r} e_s + \sum_{j=0}^{a-s+r} p^{-(a+1-s+r)+j} h_{s,j}$$

where $\mathrm{ord}_u h_{s,j} \geq (p^{n^2+n} - p^{n^2}) p^{-a-1+s}$ if $j \leq a+1-s$, and $\mathrm{ord}_u h_{s,j} > 0$ if $a+2-s \leq j \leq a-s+r$. Note that $(p^{n^2+n} - p^{n^2}) p^{-a-1+s} \geq D(s, r)$. Apply Lemma 5.3.5 to study the coefficients of other e_i's, we can write v^* as:

$$p^{-r} e_s + \sum_{\substack{i \leq s-r \\ \text{or} \\ i \geq a+r+2}} v_i^* e_i + \sum_{s \leq i \leq a+r+1} \sum_{j=0}^{a-s+r} h_{i,j} p^{-(a+1-s+r)+j} e_i$$

knowing:

(a) when $i \leq s-r$ or $i \geq a+r+2$, $\mathrm{ord}_u v_i^* \geq D(s, r)$.

(b1′) when $i = s$ and $j \leq a + 1 - s$, $\mathrm{ord}_u h_{s,j} \geq D(s, r)$.

(b2′) when $i = s$ and $a + 2 - s \leq j \leq a - s + r$, $\mathrm{ord}_u h_{s,j} > 0$.

(c1′) when $s + 1 \leq i \leq a$ and $j \leq a - s$, $\mathrm{ord}_u h_{i,j} \geq D(s, r)$.

(c2′) when $s + 1 \leq i \leq a$ and $a - s + 1 \leq j \leq a - s + r$, $\mathrm{ord}_u h_{i,j} \geq p^{n^2}(-(j - a + s)p^{i-a-2} - p^{i-a-3} - \cdots - p^{s-a-1})$.

(d1′) when $a + 1 \leq i \leq a + r + 1$ and $j \leq i - s - 1$, $\mathrm{ord}_u h_{i,j} \geq D(s, r)$.

(d2′) when $a + 1 \leq i \leq a + r + 1$ and $i - s \leq j \leq a - s + r$, $\mathrm{ord}_u h_{i,j} \geq p^{n^2}(-(j - i + s + 1)p^{i-a-2} - p^{i-a-3} - \cdots - p^{s-a-1})$.

Define

$$w_s^{(r)} := v^* - \sum_{(i,j)\text{as in}(b'2),(c'2),(d'2)} h_{i,j} w_i^{((a+1-s+r)-j)}$$

One can check for the pairs of (i, j) as in $(b'2)$, $(c'2)$, and $(d'2)$, $A_i^{((a+1-s+r)-j)} \subset A_s^{(r)}$ and $w_i^{((a+1-s)+r)-j)}$ has been constructed. Hence $w_s^{(r)}$ is indeed defined in $\mathfrak{N}^0_{A_s^{(r)}}$. By a easy exercise similar to that in the case when $a + 1 \leq s \leq n$, one can check $\mathrm{ord}_u(w_s^{(r)} - p^{-r}e_s) \geq D(s, r)$. □

Now for any reduced $\xi(\Phi)$-admissible vector $\underline{d} = (d_s)_s \in \mathbb{N}^n$, we define a subgroup $A(\underline{d}) \subset p^{-n}\mathcal{O}_F/\mathcal{O}_F$ such that $\#A(\underline{d}) = p^{\sum_{s=1}^{n} d_s}$, and $A_s^{(r)} \subset A(\underline{d})$ for all $s = 1, 2, \cdots, n$ and $r = 1, 2, \cdots, d_s$. We first make several combinatorical definitions before we actullay define $A(\underline{d})$:

- Define a set $H(\underline{d}) := \{(s, r) | 1 \leq s \leq n, 1 \leq r \leq d_s\} \subset \{1, 2, \cdots, n\} \times \mathbb{N}^*$.

- For $k = 1, 2, \cdots, a$, define $\Gamma_k := \{(n, k), (n-1, k), \cdots, (a+1, k), (a, k-1), (a-$

$1, k-2), \cdots\}$.

- Define $h_k := \#(H(\underline{d}) \cap \Gamma_k)$, $L := \sum_{j=1}^{a} h_j - 1$, and $m_i := k$ if $\sum_{j=k+1}^{a} h_j \leq i \leq \sum_{j=k}^{a} h_j - 1$.

By the definition of the Γ_k's, one can check the condition that $\underline{d}$ is $\xi(\Phi)$-admissible and reduced implies $H(\underline{d}) \subset \bigcup_{k=1}^{a} \bigcup_{t=0}^{e-1} \Gamma_k$.

Definition 6.4.4. With the above notations, define $h(\underline{d}) :=$ the largest integer k such that $H(\underline{d}) \cap \Gamma_k \neq \emptyset$, and $A(\underline{d}) := \prod_{t=0}^{e-1} \prod_{l=0}^{L} \langle p^{-m_l} \zeta_l \rangle \subset p^{-h(\underline{d})} \mathcal{O}_F / \mathcal{O}_F$.

Proposition 6.4.5. *We have* $\#A(\underline{d}) = p^{\sum_{s=1}^{n} d_s}$, *and* $A_s^{(r)} \subset A(\underline{d})$ *for all* $s = 1, 2, \cdots, n$ *and* $r = 1, 2, \cdots, d_s$.

Proof. To compute $\#A(\underline{d})$, note that $\dim_{\mathbb{F}_p} A(\underline{d})[p^k]/A(\underline{d})[p^{k-1}]$ is equal to $\#\{i | m_i = k\} = h_k$. Hence we have $\text{length}_{\mathbb{Z}_p} A(\underline{d}) = \sum_{k=1}^{a} h_k = \sum_{k=1}^{a} \#(H \cap \Gamma_k) = \#H = \sum_{s=1}^{n} d_s$, and $\#A(\underline{d}) = p^{\sum_{s=1}^{n} d_s}$.

Suppose $1 \leq s \leq n$ and $1 \leq r \leq d_s$. If $s \geq a+1$, then $A_s^{(r)} = \prod_{k=0}^{s+r-a-2} \langle p^{-r} \zeta_k \rangle$. Note that $d_s \geq r$ implies $h_r \geq s+r-a-1$, hence $\sum_{j=r}^{a} h_j - 1 \geq s+r-a-2$. As a result, $m_l \geq r$ for any $0 \leq l \leq s+r-a-2$. This proves $A_s^{(r)} \subset A(\underline{d})$. Similarly if $s \leq a$, then $A_s^r = \prod_{k=0}^{r-1} \langle p^{-(a+1-s+r)} \zeta_k \rangle$. Note that $d_s \geq r$ implies $h_{a+1-s+r} \geq r$, hence $\sum_{j=a+1-s+r}^{a} h_j - 1 \geq r-1$. As a result, $m_l \geq a+1-s+r$ for any $0 \leq l \leq r-1$. This proves $A_s^{(r)} \subset A(\underline{d})$. □

By a combination of Proposition (6.4.3) and (6.4.5), we deduce that $\mathfrak{N}_{A(\underline{d})} \bmod u = N(\underline{d})$, where $\mathfrak{N}_{A(\underline{d})} \bmod u$ is short for $\mathfrak{N}_{A(\underline{d})} / (\mathfrak{N}_{A(\underline{d})} \cap u \cdot p^{-n} \mathfrak{M} / \mathfrak{M})$.

This proves for every reduced $\xi(\Phi)$-admissible vector $\underline{d} \in \mathbb{N}^n$, $G(\underline{d})$ lifts to a finite locally free subgroup scheme $\mathcal{G}_{A(\underline{d})}$ of $\mathcal{X}$. For a general $\xi(\Phi)$-admissible vector $\underline{d}' \in \mathbb{N}^n$, there exists a reduced $\xi(\Phi)$-admissible vector $\underline{d}$ and a non-negative integer i, such that $\underline{d}' = \underline{d} + (i, i, \cdots, i)$. If we compose the isogenies $\mathcal{X} \xrightarrow{i} \mathcal{X} \xrightarrow{\pi} \mathcal{X}/\mathcal{G}_{A(\underline{d})}$, the reduction of $\mathrm{Ker}(\pi \circ p^i)$ is equal to $G(\underline{d}')$. This finishes the proof of Theorem (6.1.2).

Remark 6.4.6. From the definition we can see $A(\underline{d})$ is in fact $p^{h(\underline{d})}$-torsion, where the integer $h(\underline{d})$ is defined in (6.4.4). Therefore in Theorem (6.1.2), for each $\mathcal{O}_F$-stable subgroup G of $\mathcal{X}_k$, we can have control on the extension $R/W(k)$ such that G admits a lifting to a finite locally free subgroup scheme of $\mathcal{X}_R$. Similarly, in Corollary (6.1.3), we can also have control on the endomorphism ring of the CM lifting and the ramification of the base ring of the CM lifting.

Chapter 7

Strong CM lifting to a p-adic CM type induced from a local field with small ramification

7.1 Non-potentially-liftable subgroups

Let F be a p-adic local field. Let n be the inertia degree of F, Φ be a p-adic CM type for F, F' be the reflex field. Let $\mathcal{X}$ be the (unique) $\mathcal{O}_F$-linear CM p-divisible group over $\mathcal{O}_{F'.B(k)}$ with p-adic CM type Φ. In chapter 6 we considered the examples where Φ is induced from a p-adic CM type Φ' for F^{ur}, such that Φ' has the form $\{i_0, i_0 \circ \sigma, \cdots, i_0 \circ \sigma^a\}$ for some $i_0 \in \mathrm{Hom}(F^{ur}, \overline{\mathbb{Q}}_p)$ and $1 \leq a \leq n-1$. In these examples, the reflex field $F' = F^{\mathrm{ur}}$. It was proved in (6.1.2) that every

$\mathcal{O}_F$-stable subgroup G of $\mathcal{X}_k$ is potentially liftable. As a corollary, every $\mathcal{O}_F$-linear CM p-divisible group Y over k of dimension ae admits an F-linear CM lifting to characteristic 0 with p-adic CM type Φ.

For other p-adic CM types Φ, this potential liftability result on $\mathcal{O}_F$-stable subgroups of $\mathcal{X}_k$ may fail to hold. We have seen such examples in chapter 2 and 4. We showed that for a p-adic CM type (F, Φ), if we denote the residue field of the reflex field by $\kappa_{F'}$, then a potentially liftable $\mathcal{O}_F$-stable subgroup of $\mathcal{X}_k$ descends to an $\mathcal{O}_F$-stable subgroup of $\mathcal{X}_{\kappa_{F'}}$. As a corollary, if $\kappa_{F'}$ is "small", i.e., $\kappa_{F'}$ does not contain κ_F, then there exist non-potentially-liftable $\mathcal{O}_F$-stable subgroups of $\mathcal{X}_k$.

In this subsection we give more examples of p-adic CM types (F, Φ), such that $\kappa_{F'}$ is *not* small, but there still exist non-potentially-liftable $\mathcal{O}_F$-stable subgroups of $\mathcal{X}_k$.

Example 7.1.1. Let $F = B(\mathbb{F}_{p^5})$. Identify $\mathrm{Hom}(F, B(k))$ with $\{1, 2, 3, 4, 5\}$ as $\mathrm{Gal}(F/\mathbb{Q}_p) \cong \mathbb{Z}/5$-torsors, and take $\Phi := \{2, 4\}$. Let π_1 be a $(p^5 - 1)$-th root of $-p$ in $\overline{\mathbb{Q}}_p$, and take $E := B(k)(\pi_1)$. Let $\mathcal{X}$ be the $\mathcal{O}_F$-linear CM p-divisible group over $\mathcal{O}_E$ with p-adic CM type Φ. By (5), the attached Kisin module $\mathfrak{M} \cong \sum_{i=1}^{5} W(k)[[u]]e_i$, on which the action of $\mathcal{O}_F$ on the i-th component is given by the i-th embedding, and $\phi_{\mathfrak{M}} e_i = e_{i+1}$ for $i = 1, 3$, $\phi_{\mathfrak{M}} e_i = (p + u^{p^5-1})e_{i+1}$ for $i = 2, 4, 5$. By [1] (B.4), the Dieudonné module of the closed fiber is $\mathfrak{M}/u\mathfrak{M} \cong \sum_{i=1}^{5} W(k)e_i$. If we denote $W(k) \cdot e_i$ by M_i, then $FM_i = M_{i+1}$ for $i = 1, 3$, $FM_i = pM_{i+1}$ for $i = 2, 4, 5$, $VM_i = pM_{i-1}$ for $i = 2, 4$, $VM_i = M_{i-1}$ for $i = 1, 3, 5$. By (5.2) we know all the p-torsion points

on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are rational over E, and the finite Kisin modules attached to finite locally free subgroup schemes of order p have the form of $W(k)((u))\{\eta \cdot v\} \cap p^{-1}\mathfrak{M}/\mathfrak{M}$, where $\eta \in p^{-1}\mathcal{O}_F/\mathcal{O}_F$ and

$$v := u^{p^4+p^2}e_1 + u^{p^3+1}e_2 + u^{p^4+p}e_3 + u^{p^2+1}e_4 + u^{p^3+p}e_5$$

By [1] (B.4), it is clear that the Dieudonné module of the closed fiber of every finite locally free subgroup schemes of order p is equal to $p^{-1}M_4/M_4$. On the other hand, one can check $p^{-1}M_2/M_2$ is also $\mathcal{O}_F$-stable and stable under F, V. However, the observation above implies that the corresponding $\mathcal{O}_F$-stable subgroup of $\mathcal{X}_k$ is non-potentially-liftable.

Example 7.1.2. Let $F = B(\mathbb{F}_{p^3})[\pi]/(\pi^e + p)$, where $e \geq 2$ and we assume $e|p^3 - 1$, so $F/\mathbb{Q}_p$ is Galois. Identify $\mathrm{Hom}(F^{\mathrm{ur}}, B(k))$ with $\{1, 2, 3\}$ as $\mathrm{Gal}(F^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathbb{Z}/3$-torsors. Let $\mathrm{Res} : \mathrm{Hom}(F, \overline{\mathbb{Q}}_p) \to \mathrm{Hom}(F^{ur}, B(k))$ be the restriction map, let φ be an embedding of F in $\mathrm{Res}^{-1}(3)$, and define $\Phi := \mathrm{Res}^{-1}(\{2, 3\})\backslash\{\varphi\}$. Let $h(x) := -\pi x + x^{p^3}$, let $h^{(r)}(x)$ be the r-th iteration of $h(x)$, and $h_r(x) := \frac{h^{(r)}(x)}{h^{(r-1)}(x)}$ for all positive integers r. Let π_1 be a root of $h_e(x)$ in $\overline{\mathbb{Q}}_p$, and let $E := B(k)(\pi_1)$. The minimal polynomial of π_1 over $B(k)$ is $E(u) = \prod_{\gamma \in \mathrm{Gal}(F \cdot B(k)/B(k))} (\gamma_* h_e(x))$, its constant term is equal to p. Let $E_0(u) := \prod_{\gamma \in \mathrm{Gal}(F \cdot B(k)/B(k))} (\gamma_* h^{(e-1)}(x))$. Let $\mathcal{X}$ be the $\mathcal{O}_F$-linear CM p-divisible group over $\mathcal{O}_E$ with p-adic CM type Φ. By (5), the attached Kisin module $\mathfrak{M} \cong \sum_{i=1}^{3} W(k)[\pi][[u]]/(\pi^e - p)e_i$, where $\phi_{\mathfrak{M}} e_1 = e_2$, $\phi_{\mathfrak{M}} e_2 = h_e(u)e_3$, $\phi_{\mathfrak{M}} e_3 = E(u)e_1$. By [1] (B.4), the Dieudonné module of the closed

fiber is $\mathfrak{M}/u\mathfrak{M} \cong \sum_{i=1}^{3} W(k)[\pi]/(\pi^e + p)e_i$. If we denote $W(k) \cdot e_i$ by M_i, then

$$FM_1 = M_2, FM_2 = \pi M_3, FM_3 = pM_1, VM_1 = M_3, VM_2 = pM_1, VM_3 = \pi^{e-1}M_2$$

Let ϕ be the endomorphism on $W(k)[\pi][[u]]/(\pi^e + p)$ that induces σ on $W(k)$, fixes π, and sends u to u^p. Let $v := E_0(u)^{\phi^2}h^{(e-1)}(u)^{\phi}e_1 + E_0(u)h^{(e-1)}(u)^{\phi^2}e_2 + E_0(u)^{\phi}h^{(e-1)}(u)e_3$. By (5.2) we know all the p-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are rational over E, and the finite Kisin modules attached to finite locally free subgroup schemes of order p have the form of $W(k)((u))\{\eta \cdot v\} \cap p^{-1}\mathfrak{M}/\mathfrak{M}$, where $\eta \in p^{-1}\mathcal{O}_F/\mathcal{O}_F$.

Note that $E_0(u)$(resp. $h^{(e-1)}(u)$) is a monic polynomial of degree $ep^{3(e-1)}$ (resp. $p^{3(e-1)}$) in $W(k)[u]$ (resp. $W(k)[\pi][[u]]/(\pi^e + p)$). So $v \equiv u^{ep^{3e-1}}h^{(e-1)}(u)^{\phi}e_1 + u^{ep^{3e-3}}h^{(e-1)}(u)^{\phi^2}e_2 + u^{ep^{3e-2}}h^{(e-1)}(u)e_3 \mod p$. By the definition of $h^{(e-1)}(u)$, one can check that there exist $g_i(u) \in \mathcal{O}_{F^{\mathrm{ur}}}[u]$, such that $h^{(e-1)}(u) \equiv \sum_{i=1}^{e-1} \pi^i g_i(u) \mod p$, $g_i(u) \in \mathcal{O}_{F^{\mathrm{ur}}}((u))^{\times}$, and $\mathrm{ord}_u g_i(u) = p^{3e-3-3i}$. When $\eta = \pi^{-j}$ with $1 \leq j \leq e$, we have $\pi^{-j} \cdot v \equiv \pi^{-j}(u^{ep^{3e-1}} \sum_{i=1}^{j-1} \pi^i g_i(u)^{\phi}e_1 + u^{ep^{3e-3}} \sum_{i=1}^{j-1} \pi^i g_i(u)^{\phi^2}e_2 + u^{ep^{3e-2}} \sum_{i=1}^{j-1} \pi^i g_i(u)e_3)$ mod $\mathfrak{M}$.

(a) If $e > p + 1$, then one can check $u^{-ep^{3e-3}-p^{3(e-j)+2}}(\pi^{-j} \cdot v) \equiv c\pi^{-1}e_2 \mod u$, where $c \in W(k)^{\times}$. In particular, the Dieudonné module of the closed fiber of the corresponding finite locally free subgroup scheme is equal to $\pi^{-1}M_2/M_2$, which corresponds to an $\mathcal{O}_F$-stable subgroup of $\mathcal{X}$. We denote this subgroup of order p by G_2. Because for every $\eta \in p^{-1}\mathcal{O}_F/\mathcal{O}_F$, there exists some $1 \leq j \leq e$ such that η differs from π^{-j} by a unit in $\mathcal{O}_F$, this proves all finite locally free subgroup schemes of order p reduce to G_2 over k. On the other hand, one can check $\pi^{-1}M_3/M_3$ is

also stable under F, V and the $\mathcal{O}_F$-action. Let G_3 be the corresponding subgroup of $\mathcal{X}_k$. The observation above implies that G_3 is non-potentially-liftable.

(b) If $e < p+1$, then

$$u^{-ep^{3e-2}-p^{3e-3}}(\pi^{-1}v) \equiv c\pi^{-1}e_3 \mod u$$

and

$$u^{-ep^{3e-3}-p^2}(p^{-1}v) \equiv c'\pi^{-1}e_2 \mod u$$

where $c, c' \in W(k)^\times$. Thus G_2 and G_3 are both potentially liftable.

The p-adic CM type in Example (7.1.2) can be viewed as a generalization of the p-adic CM type we considered in chapter 6. However, the example shows that a large ramification index of F increases the subtlety in the CM lifting problem. Nevertheless, in the next subsection we will show that as long as the ramification index of F is small (less than $p-1$), we can still prove a result that is similar to (6.1.2).

7.2 Positive results on question (sCML)

Let F be a p-adic local field, π be a uniformizer in $\mathcal{O}_F$, κ_F be its residue field. Let n be the inertia degree of F, e be the ramification index of F. Suppose F_0 is a subextension in F/F^{ur} such that $e_0 := [F_0 : F^{ur}] < p-1$. Define $d_0 := e/e_0$. Denote $W(k)[x]/(x^{e_0}-p)$ by R_0. The fraction field Frac R_0 is the unique tamely ramified extension of $B(k)$ with degree e_0.

In this subsection we prove the following theorem:

Theorem 7.2.1. *Let a be an integer such that $0 \leq a \leq n-1$, and t be an integer such that $0 \leq t \leq e_0 - 1$. Take $i_0 \in Hom(F^{ur}, \overline{\mathbb{Q}}_p)$, and define $\Phi'' := \{i_0, i_0 \circ \sigma, \cdots, i_0 \circ \sigma^{a-1}\} \subset Hom(F^{ur}, \overline{\mathbb{Q}}_p)$. Let Φ^* be a set of t embeddings of F_0 into $\overline{\mathbb{Q}}_p$ that induce $i_0 \circ \sigma^a$ on F^{ur}. Let $\Phi' \subset Hom(F_0, \overline{\mathbb{Q}}_p)$ be the union of Φ^* and the pullback of Φ''. Let $\Phi \subset Hom(F, \overline{\mathbb{Q}}_p)$ be pullback of Φ'. Let $\mathcal{X}$ be the $\mathcal{O}_F$-linear CM p-divisible group over R_0 with p-adic CM type Φ. Then for every $\mathcal{O}_F$-stable subgroup G of $\mathcal{X}_k$, there exists a finite extension R over R_0, such that G lifts to a finite locally free subgroup scheme of $\mathcal{X}_R$.*

Remark 7.2.2. It suffices to prove Theorem (7.2.1) in the case when $t \geq 1$ and $F = F_0$. In fact, if $t = 0$ then we are reduced to (6.1.2). We may assume $F = F_0$ because $\mathcal{X}$ is $\mathcal{O}_F$-linearly isomorphic to a Serre tensor construction from an $\mathcal{O}_{F_0}$-linear CM p-divisible group over R_0 with p-adic CM type Φ'. For details of the argument, see the beginning of (6.4).

Theorem (7.2.1) has the following consequences:

Corollary 7.2.3. *Notations as in (7.2.1). Then every $\mathcal{O}_F$-linear CM p-divisible group over k with dimension $ae+td_0$ admits an F-linear CM lifting to characteristic 0 with p-adic CM type Φ.*

Proof. Every $\mathcal{O}_F$-linear CM p-divisible group Y over k with dimension $ae + td_0$ is L-linearly isogeneous to $\mathcal{X}_k$, hence there exists an $\mathcal{O}_F$-stable subgroup G of $\mathcal{X}_k$ such

that Y is $\mathcal{O}_F$-linearly isomorphic to $\mathcal{X}_k/G$. By Theorem (7.2.1), there exists a finite extension R over $W(k)$ and a finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{X}_R$, such that $\mathcal{G}_k = G$. Then $\mathcal{X}_R/\mathcal{G}$ is an F-linear CM lifting of Y with p-adic CM type Φ. $\square$

Remark 7.2.4. In the context of question (LTI) for p-divisible groups (c.f. 3.1), Corollary (7.2.3) implies $\mathrm{LTI}(F,\Phi) = \{$the set of Lie types of dimension $ae + td_0\}$.

Corollary 7.2.5. *We have the following positive results on (sCML):*

(a) Let K_0 be a p-adic local field with absolute ramification index $e(K_0) < p-1$, let $K \cong K_0 \times K_0$. Then the answer to question (sCML) relative to (K, K_0) for p-divisible groups is affirmative.

(b) Let L be a CM field, and L_0 be its maximal totally real subfield. If for every place v of L_0 above p, v is either inert in L, or split in L with absolute ramification index $e(v) < p-1$, then for the CM field L the answer to question (sCML) for abelian varieties is affirmative.

Proof. (b) follows from (a) and (6.1.5), so it suffices to prove (a). Let $n(K_0)$ be the inertia degree of K_0. We mark the two K_0-components of K by $K_{0,1}$ and $K_{0,2}$. Let ι be the K_0-involution on K such that ι flips the two components. The set of embeddings $\mathrm{Hom}(K, \overline{\mathbb{Q}}_p)$ is naturally isomorphic to $\mathrm{Hom}(K_{0,1}, \overline{\mathbb{Q}}_p) \coprod \mathrm{Hom}(K_{0,2}, \overline{\mathbb{Q}}_p)$, and the involution ι interchanges between $\mathrm{Hom}(K_{0,1}, \overline{\mathbb{Q}}_p)$ and $\mathrm{Hom}(K_{0,2}, \overline{\mathbb{Q}}_p)$. The set of embeddings $\mathrm{Hom}(K_{0,1}^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$ is isomorphic to $\{1, 2, \cdots, n(K_0)\}$ as $\mathrm{Gal}(K_0^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathbb{Z}/n$-torsors. Take a p-adic CM type for $K_{0,1}^{\mathrm{ur}}$ to be $\Phi' := \{1, 2, \cdots, a-1\}$. Take Φ^* to be a set of t embeddings of $K_{0,1}$ into $\overline{\mathbb{Q}}_p$ such that they induce the a-th embedding

on $K_{0,1}^{\mathrm{ur}}$. Let Φ be the p-adic CM type for K such that Φ is equal to the union of Φ^* and the pullback of Φ'.

Let Y be an $\mathcal{O}_K$-linear CM p-divisible group over k and suppose $\dim Y = [K_0 : \mathbb{Q}_p] = n(K_0)e(K_0)$, as in the assumption question (sCML) relative to (K, K_0) for p-divisible groups. The splitting $\mathcal{O}_K \cong \mathcal{O}_{K_{0,1}} \times \mathcal{O}_{K_{0,2}}$ induces $Y \cong Y_1 \times Y_2$, where Y_i is an $\mathcal{O}_{K_{0,i}}$-linear CM p-divisible group over k. The question (sCML) is trivial if Y_1 or Y_2 is etale. From now on we assume $\dim Y_1, \dim Y_2 > 0$. Write $\dim Y_1$ as $ae(K_0) + t$, where $0 \leq a \leq n(K_0) - 1$ and $0 \leq t \leq e(K_0) - 1$. The dimension of the Serre dual $Y_2^\vee$ is also equal to $ae(K_0)+t$. Therefore by Corollary (7.2.3), Y_1 and $Y_2^\vee$ both admit K_0-linear CM liftings with p-adic CM type Φ. We denote the liftings by $\mathcal{Y}_1$ and $\mathcal{Y}_2$, respectively. Then $\mathcal{Y}_1 \times \mathcal{Y}_2^\vee$ is a K-linear CM lifting of $Y_1 \times Y_2$. The p-adic CM type $\tilde{\Phi}$ of $\mathcal{Y}_1 \times \mathcal{Y}_2^\vee$ is equal to $\tilde{\Phi} := \Phi \coprod (\Phi \circ \iota)^c$, which is compatible with ι in the sense that $\tilde{\Phi} \coprod \tilde{\Phi} \circ \iota = \mathrm{Hom}(K, \overline{\mathbb{Q}}_p)$. This proves (a). $\square$

Now we prove Theorem (7.2.1) under the assumption that $t \geq 1$ and $F = F_0$. There exists a finite extension R_1 over R_0, such that the p^n-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are rational over Frac R_1. Let us recall from chapter 5 the construction of R_1 and the Kisin module of $\mathcal{X}_{R_1}$. Let N be the smallest integer such that $n|N$ and $e_0|\frac{p^N-1}{p^n-1}$. The field $B(\mathbb{F}_{p^N}) \cdot F_0 \cong B(\mathbb{F}_{p^N})[\pi_0]/(\pi_0^{e_0} + p)$ is Galois over $\mathbb{Q}_p$, and it contains the reflex field of (F, Φ). Let $h(x) = -\pi_0 x + x^{p^N}$, and define $h^{(r)}(x) := h \circ h \circ \cdots \circ h$ to be the r-th iteration of h, $h_r(x) := \frac{h^{(r)}(x)}{h^{(r-1)}(x)}$ for all positive integers r as in the theory of Lubin-Tate formal group laws. Let π_n be a root of $h_{ne_0}(x)$, let $\sqrt[p^n]{\pi_n}$ be

a p^n-th root of π_n. Define $R_1 := W(k)[\sqrt[p^n]{\pi_n}]$, and $K_1 := \mathrm{Frac}\ R_1$. By (5.2.4) all the p^n-torsion geometric points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are rational over K_1. We make the remark that in fact the p^n-torsion points are already rational over $B(k)(\pi_n)$, here we take a further p^n-th root of π_n for the convenience in the later computations.

The Eisenstein minimal polynomial of $\sqrt[p^n]{\pi_n}$ over $B(k)$ is

$$E(u) := \prod_{\gamma \in \mathrm{Gal}(F_0 \cdot B(k)/B(k))} (\gamma_* h_{ne_0})(u^{p^n})$$

The constant term of $E(u)$ is equal to p. Denote the natural restriction map from $\mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$ to $\mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$ by Res. According to our definition of the p-adic CM type Φ for F, there exists an identification between $\mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$ and $\{1, 2, \cdots, n\}$ as $\mathrm{Gal}(F^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathbb{Z}/n$-torsors, such that $\Phi = \mathrm{Res}^{-1}(\{2, 3, \cdots, a+1\}) \coprod \Phi^*$, where Φ^* is a subset of $\mathrm{Res}^{-1}(a+2)$. Choose an embedding $i^* \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$ such that i_{a+2} induces $a+2$ on F^{ur}. Define $S^* := \{\alpha \in \mathrm{Gal}(K_1/B(k)) | \alpha^{-1} \circ i^* \in \Phi^*\}$. Define $f(u) := \prod_{\gamma \in S^*} (\gamma_* h_{ne_0})(u^{p^n})$, $\overline{f(u)} := E(u)/f(u)$. By (5.2.4), the Kisin module $\mathfrak{M}$ attached to $\mathcal{X}_{R_1}$ is isomorphic to $\bigoplus_{j=1}^{n} W(k)[\pi_0][[u]]/(\pi_0^{e_0} + p)e_j$, on which $\phi_{\mathfrak{M}}(e_i) = e_{i+1}$ if $1 \leq i \leq a$, $\phi_{\mathfrak{M}}(e_{a+1}) = \overline{f(u)} e_{a+2}$, and $\phi_{\mathfrak{M}}(e_i) = E(u) e_{i+1}$ if $a+2 \leq i \leq n$.

The endomorphism ϕ on $W(k)[[u]]$ extends on $W(k)[\pi_0][[u]]/(\pi_0^{e_0} + p)$, such that $\phi|_{W(k)} = \sigma$, $\phi(\pi_0) = \pi_0$, and $\phi(u) = u^p$. Define

$$f_0(u) := \prod_{\gamma \in S} (\gamma_* h^{(ne_0 - 1)})(u^{p^n})^{\phi^{N-n} + \phi^{N-2n} + \cdots + \phi^n + 1}$$

$$E_0(u) := \prod_{\gamma \in \mathrm{Gal}(F_0 \cdot B(k)/B(k))} (\gamma_* h^{(ne_0 - 1)})(u^{p^n})^{\phi^{N-n} + \phi^{N-2n} + \cdots + \phi^n + 1}$$

Then the p^n-torsion points on $\mathcal{X}_{R_1}$ are in one-to-one correspondence with $\{\eta \cdot v | \eta \in p^{-n}\mathcal{O}_F/\mathcal{O}_F\}$, where $v = \sum_{i=1}^{a+1} E_0(u)^{\phi^{n-1}+\phi^{n-2}+\cdots+\phi^{n-a-1+i}+\phi^{i-2}+\phi^{i-3}+\cdots+1} f_0(u)^{\phi^{n-a-2+i}} e_i + \sum_{i=a+1}^{n} E_0(u)^{\phi^{i-2}+\phi^{i-3}+\cdots+\phi^{i-a-1}} f_0(u)^{\phi^{i-a-2}} e_i$. For a subgroup A of $p^{-n}\mathcal{O}_F/\mathcal{O}_F$, define $\mathfrak{N}_A^0 := W(k)((u))\{\eta \cdot v | \eta \in A\}$, $\mathfrak{N}_A := \mathfrak{N}_A^0 \cap p^{-n}\mathfrak{M}/\mathfrak{M}$. Let $\mathcal{G}_A$ be the finite locally free subgroup scheme associated to $\mathfrak{N}_A$. When A runs over the finite subgroups of $p^{-n}\mathcal{O}_F/\mathcal{O}_F$, $\mathcal{G}_A$ enumerates all finite locally free p^n-torsion subgroup schemes of $\mathcal{X}_{R_1}$. Denote $\mathfrak{N}_A/(\mathfrak{N}_A \cap up^{-n}\mathfrak{M}/\mathfrak{M}) \cong (\mathfrak{N}_A + up^{-n}\mathfrak{M}/\mathfrak{M})/(up^{-n}\mathfrak{M}/\mathfrak{M})$ by $\mathfrak{N}_A \mod u$, then $\mathfrak{N}_A \mod u$ is the Dieudonné module of the closed fiber of $\mathcal{G}_A$.

7.3 Technical lemmas

We state a few properties on $E_0(u)$ and $f_0(u)$ in terms of their Newton polygons. For the definition and basic properties of Newton polygons, see (5.3). We take a valuation ν on $B(k)[\pi_0]/(\pi_0^{e_0}+p)$ such that $\nu(\pi_0) = 1$. Denote the Newton polygon of a polynomial $g(u)$ by $\mathrm{NP}(g(u))$. In general suppose K is a field, for each formal power series $g(x) \in K((x))$, there exists a unique integer t such that $g(x) = x^t g_0(x)$ and $g_0(x) \in K[[x]]^\times$. We define this integer t to be the *order* of $g(x)$, denoted by $\mathrm{ord}_u g(x)$, or simply $\mathrm{ord}_u g$ for short. The following proposition is a straightforward application of Lemma (5.3.3).

Proposition 7.3.1. *Let* $d := p^{Nne_0}(1 + p^{-n} + \cdots + p^{-(N-n)})$.

(a) *The vertices of NP*$(E(u))$ *are* $(de_0(p^n-1), 0)$, $(0, e_0)$, *and the slope of NP*$(E(u))$ *is equal to* $-\frac{1}{d(p^n-1)}$ *with multiplicity* $e_0 d(p^n-1)$.

(b) *The vertices of NP*$(E_0(u))$ *are*

$$(de_0, 0), (de_0p^{-n}, e_0), \cdots, (de_0p^{-N(ne_0-1)}, e_0(Ne_0 - \frac{N}{n}))$$

the slopes of NP$(E_0(u))$ *are*

$$-\frac{1}{d(1-p^{-n})} > -\frac{1}{d(p^{-n}-p^{-2n})} > \cdots > -\frac{1}{d(p^{-N(ne_0-1)+n}-p^{-N(ne_0-1)})}$$

with multiplicities $e_0d(1-p^{-n}), e_0d(p^{-n}-p^{-2n}), \cdots, e_0d(p^{-N(ne_0-1)+n}-p^{-N(ne_0-1)})$, *respectively.*

(c) *There exists a polynomial* $\widehat{E_0}(u) \in W(k)[\pi_0][u, u^{-1}]/(\pi_0^{e_0} - p)$ *such that* $E_0(u)\widehat{E_0}(u) \equiv 1 \mod p^n$. *The vertices of NP*$(\widehat{E}_0(u))$ *are* $(-de_0, 0)$, $(de_0(-n+(n-1)p^{-n}), (n-1)e_0)$, *and the slope of NP*$(\widehat{E}_0(u))$ *is equal to* $-\frac{1}{d(1-p^{-n})}$ *with multiplicity* $e_0d(n-1)(1-p^{-n})$.

(d) *The vertices of NP*$(f_0(u))$ *are*

$$(dt, 0), (dtp^{-n}, t), (dtp^{-2n}, 2t), \cdots, (dtp^{-N(ne_0-1)}, t(Ne_0 - \frac{N}{n}))$$

the slopes of NP$(f_0(u))$ *are*

$$-\frac{1}{d(1-p^{-n})} > -\frac{1}{d(p^{-n}-p^{-2n})} > \cdots > -\frac{1}{d(p^{-N(ne_0-1)+n}-p^{-N(ne_0-1)})}$$

with multiplicities $td(1-p^{-n}), td(p^{-n}-p^{-2n}), \cdots, td(p^{-N(ne_0-1)+n}-p^{-N(ne_0-1)})$, *respectively.*

Apply Lemma (5.3.3), we can deduce the following propery of $E_0(u)$ and $f_0(u)$. Note that if $i > 0$ and a polynomial $\theta(u) \in F[u]$ can be written as $\theta_0(u^d)$ such that

$p^i|d$, then $\theta(u)$ is contained in the image of $\phi^i : F[u] \to F[u]$, therefore $\theta(u)^{\phi^{-i}}$ is well defined.

Lemma 7.3.2. *Suppose we have integers $x_1 > x_2 > \cdots > x_r > y_1 > y_2 > \cdots > y_s$, such that $y_s + n \geq 0$ and $y_1 + n \geq x_r$. Let α be an integer such that $y_1 + n \geq \alpha$. Let $l \leq r-1$ be the largest integer such that $x_l > y_1 + n$; we treat $l = 0$ if such an x_l does not exist. Then there exists $g_k(u) \in \mathcal{O}_{F^{ur}}[u]$ for $k = 0, 1, \cdots, ne_0 - 1$, such that we can write*

$$E_0(u)^{\phi^{x_1}+\cdots+\phi^{x_r}-\phi^{x_1-N}-\cdots-\phi^{x_l-N}-\phi^{y_1}-\cdots-\phi^{y_s}} f_0(u)^{\phi^\alpha} \equiv \sum_{k=0}^{ne_0-1} \pi_0^k g_k \mod p^n$$

with the following estimates on $ord_u g_k$:

(a) If $\alpha \leq y_1$, then

$$ord_u g_k \geq \begin{cases} d((re_0-k)p^{x_r} - e_0(p^{y_1}+\cdots+p^{y_s}) + tp^\alpha), & \text{for } k \leq re_0 - 1 \\ d(-(k-re_0+e_0)p^{y_1} - e_0(p^{y_2}+\cdots+p^{y_s}) + tp^\alpha), & \text{for } k \geq re_0 \end{cases}$$

(b) If $y_1 < \alpha < x_r$, then

$$ord_u g_k \geq \begin{cases} d((re_0-k)p^{x_r} - e_0(p^{y_1}+\cdots+p^{y_s}) + tp^\alpha), & \text{for } k \leq re_0 - 1 \\ d((re_0+t-k)p^\alpha - e_0(p^{y_1}+\cdots+p^{y_s})) & \\ \qquad\qquad \text{for } re_0 \leq k \leq re_0 + t - 1 & \\ d(-(k-re_0-t+e_0)p^{y_1} - e_0(p^{y_2}+\cdots+p^{y_s})), & \text{for } k \geq re_0 + t \end{cases}$$

(c) If $\alpha \geq x_r$, then

$$ord_u g_k \geq \begin{cases} d((re_0+t-k)p^{x_r} - e_0(p^{y_1}+\cdots+p^{y_s})), & \text{for } k \leq re_0 + t - 1 \\ d(-(k-re_0-t+e_0)p^{y_1} - e_0(p^{y_2}+\cdots+p^{y_s})), & \text{for } k \geq re_0 + t \end{cases}$$

7.4 The proof of Theorem (7.2.1)

The Dieudonné module of $\mathcal{X}_k$ is isomorphic to $\mathfrak{M}/u\mathfrak{M} \cong \bigoplus_{i=1}^{n} M_i$, where M_i is a free $W(k)[\pi_0]/(\pi_0^{e_0} - p)$-module of rank 1. The Frobenius and Verschiebung maps act by

$$FM_i = M_{i+1} \text{ for } 1 \leq i \leq a,\ FM_{a+1} = \pi_0^{e_0 - t} M_{a+2},\ FM_i = pM_{i+1} \text{ for } a+2 \leq i \leq n$$

$$VM_{i+1} = pM_i \text{ for } 1 \leq i \leq a,\ VM_{a+2} = \pi_0^{t} M_{a+1},\ VM_{i+1} = M_i \text{ for } a+2 \leq i \leq n$$

If G is an $\mathcal{O}_F$-stable subgroup of $\mathcal{X}_k$, then the Dieudonné module N attached to G is equal to $\bigoplus_{i=1}^{n} \pi_0^{-d_i} M_i/M_i$, where the d_i's are non-negative integers satisfying

$$0 \leq d_{i+1} - d_i \leq e_0, \text{ for } 1 \leq i \leq a$$

$$t - e_0 \leq d_{a+2} - d_{a+1} \leq t$$

$$-e_0 \leq d_{i+1} - d_i \leq 0 \text{ for } a+2 \leq i \leq n$$

Such a vector $\underline{d} = (d_i)_i \in \mathbb{N}^n$ is called $\xi(\Phi)$-*admissible* in the sense of (6.3). If moreover, $\min d_i = 0$, then we say $\underline{d}$ is $\xi(\Phi)$-*admissible and reduced*. For a $\xi(\Phi)$-admissible $\underline{d}$, define $N(\underline{d})$ to be the Dieudonné module $\bigoplus_{i=1}^{n} \pi_0^{-d_i} M_i/M_i$, and let $G(\underline{d})$ be the associated $\mathcal{O}_F$-stable subgroup of $\mathcal{X}_k$. The mapping $\underline{d} \mapsto G(\underline{d})$ is a one-to-one correspondence between $\xi(\Phi)$-admissible vectors and $\mathcal{O}_F$-stable subgroups of $\mathcal{X}_k$. Define $X(\underline{d})$ to be the quotient $\mathcal{X}_k/G(\underline{d})$, it is also an $\mathcal{O}_F$-linear CM p-divisible group, and we can write down its Lie type directly from $\underline{d}$; see (6.3.2). We will first prove for every $\xi(\Phi)$-admissible and reduced vector $\underline{d} \in \mathbb{N}^n$, there exists a subgroup $A \subset p^{-n}\mathcal{O}_F/\mathcal{O}_F$ such that $\mathfrak{N}_A \mod u = N(\underline{d})$.

Define $q_i := \begin{cases} \min\{(i-1)e_0, (n-a)e_0 - t\} & \text{if } i \leq a+1 \\ \min\{ae_0 + t, (n-a)e_0 - t\} & \text{if } i = a+2 \\ \min\{(n+1-i)e_0, ae_0 + t\} & \text{if } i \geq a+3 \end{cases}$ for each $i = 1, 2, \cdots, n$. One can easily check that for a positive integer r, there exists reduced $\xi(\Phi)$-admissible $\underline{d} \in \mathbb{N}^n$ such that the i-th component d_i is equal to r if and only if $1 \leq r \leq q_i$.

Take a set of $\mathbb{Q}_p$-basis $\{\zeta_i | i = 1, 2, \cdots, n\}$ of $F^{ur} = B(\mathbb{F}_{p^n})$, such that for any $0 \leq l \leq n-1$, the submatrix $[\zeta_i^{\sigma^j}]_{0 \leq i,j \leq l}$ is non-degenerating; c.f. (6.4). Take $\underline{\lambda_l} = (\lambda_{l,0}, \lambda_{l,1}, \cdots, \lambda_{l,l})$ in $(W(k))^{l+1}$ such that $(\lambda_{l,0}, \lambda_{l,1}, \cdots, \lambda_{l,l}) \cdot [\zeta_i^{\sigma^j}]_{0 \leq i,j \leq l} = (0, 0, \cdots, 0, 1)$.

Definition 7.4.1. Suppose (s, r) is a pair of integers such that $1 \leq s \leq n, 1 \leq r \leq q_s$.

Write $r = i_r e_0 - j_r$, where $0 \le j_r \le e_0 - 1$. Define $A_s^{(r)} :=$

$$\begin{cases} \prod_{i=0}^{i_r+s-a-3} \prod_{j=j_r}^{e_0-1} \langle p^{-i_r} \zeta_i \pi_0^j \rangle \times \prod_{i=0}^{i_r+s-a-3} \prod_{j=0}^{e_0-t-1} \langle p^{-(i_r-1)} \zeta_i \pi_0^j \rangle \times \\ \prod_{i=0}^{i_r+s-a-4} \prod_{j=e_0-t}^{j_r-1} \langle p^{-(i_r-1)} \zeta_i \pi_0^j \rangle \\ \qquad \text{if } \ a+2 \le s \le n, e_0 - t \le j_r \le e_0 - 1 \\ \prod_{i=0}^{i_r+s-a-2} \prod_{j=j_r}^{e_0-t-1} \langle p^{-i_r} \zeta_i \pi_0^j \rangle \times \prod_{i=0}^{i_r+s-a-3} \prod_{j=e_0-t}^{e_0-1} \langle p^{-i_r} \zeta_i \pi_0^j \rangle \times \prod_{i=0}^{i_r+s-a-3} \prod_{j=0}^{j_r-1} \langle p^{-(i_r-1)} \zeta_i \pi_0^j \rangle \\ \qquad \text{if } \ a+2 \le s \le n, 0 \le j_r \le e_0 - t - 1 \\ \prod_{i=0}^{i_r-1} \prod_{j=j_r-t}^{e_0-t-1} \langle p^{-(a+1-s+i_r)} \zeta_i \pi_0^j \rangle \times \prod_{i=0}^{i_r-2} \prod_{j=e_0-t}^{e_0-1} \langle p^{-(a+1-s+i_r)} \zeta_i \pi_0^j \rangle \times \\ \prod_{i=0}^{i_r-2} \prod_{j=0}^{j_r-t-1} \langle p^{-(a+1-s+i_r)} \zeta_i \pi_0^j \rangle \\ \qquad \text{if } \ 1 \le s \le a+1, t \le j_r \le e_0 - 1 \\ \prod_{i=0}^{i_r-1} \prod_{j=e_0+j_r-t}^{e_0-1} \langle p^{-(a+2-s+i_r)} \zeta_i \pi_0^j \rangle \times \prod_{i=0}^{i_r-1} \prod_{j=0}^{e_0-t-1} \langle p^{-(a+1-s+i_r)} \zeta_i \pi_0^j \rangle \times \\ \prod_{i=0}^{i_r-2} \prod_{j=e_0-t}^{e_0+j_r-t-1} \langle p^{-(a+1-s+i_r)} \zeta_i \pi_0^j \rangle \\ \qquad \text{if } \ 1 \le s \le a+1, 0 \le j_r \le t-1 \end{cases}$$

as subgroups of $p^{-n}\mathcal{O}_F/\mathcal{O}_F$.

Define integers

$$D(s,r) := \begin{cases} d(p^{s-1} - e_0(p^{s-2} + p^{s-3} + \cdots + p^{s-a-1}) - (i_r e_0 - j_r)p^{s-a-2}) \\ \qquad\qquad \text{if } \ a+2 \le s \le n \\ d(p^{s-1} - e_0(p^{s-2} + p^{s-3} + \cdots + p^{s-a-1}) - (i_r e_0 - j_r + t)p^{s-a-2}) \\ \qquad\qquad \text{if } \ 1 \le s \le a+1 \end{cases}$$

By the assumption on (s,r), when $a+2 \le s \le n$ we have $i_r e_0 - j_r \le ae_0 + t$, and when $1 \le s \le a+1$ we have $i_r e_0 - j_r \le ae_0$. Note that $e_0 < p-1$, hence in either

case we have $D(s,r) \geq d(p^{s-1} - e_0(p^{s-2} + p^{s-3} + \cdots + p^{s-a-1}) - (ae_0 + t)p^{s-a-2}) \geq d(p^{s-1} - (p-2)(p^{s-2} + p^{s-3} + \cdots + p^{s-a-1}) - (a+1)e_0 p^{s-a-2}) > 0$.

For an element $x \in p^{-n}\mathfrak{M}^0/\mathfrak{M}^0$, we define $\mathrm{ord}_u x$ as the smallest integer d such that $u^{-d}x \in p^{-n}\mathfrak{M}/\mathfrak{M}$ and $u^{-d}x \neq 0 \mod u$.

Proposition 7.4.2. *For each pair of (s,r) that satisfies the condition in (7.4.1). Write $r = i_r e_0 - j_r$, where $0 \leq j_r \leq e_0 - 1$. Then there exists $w_s^{(r)} \in \mathfrak{N}_{A_s^{(r)}}$ such that $w_s^{(r)} \equiv p^{-i_r}\pi_0^{j_r} e_s \mod ord_u \geq D(s,r)$.*

Proof. When $a+2 \leq s \leq n$ we prove by an increasing induction on r. When $1 \leq s \leq a+1$ we prove by a decreasing induction on s and an increasing induction on r. By the definition of $A_s^{(r)}$, the argument will differ depending on the range of j_r, too. We will prove the case when $a+2 \leq s \leq n$ and $e_0 - t \leq j_r \leq e_0 - 1$. The details for the other cases will be left as exercises.

Suppose we have proved the statement for smaller r's. Define

$$v^* := \sum_{k=0}^{i_r+s-a-3} \lambda_{i_r+s-a-3,k}^{\sigma^{a+3-i_r}} E_0(u)^{-\phi^{s-2}-\cdots-\phi^{s-a-1}} u^{-p^{s-a-2}td}(p^{-i_r}\zeta_k \pi_0^{j_r} \cdot v)$$

Then by the choice of $\underline{\lambda_{i_r+s-a-3}}$ one can check in v^* the coefficient of e_i vanishes for $a+3-i_r \leq i \leq s-1$. Now we examine the coefficients for e_i with $i \leq a+2-i_r$ or $i \geq s$.

When $1 \leq i \leq a+1-i_r$, the coefficient of e_i is the product of a scalar in $W(k)$ with $p^{-i_r}\pi_0^{j_r} \cdot u^{-p^{s-a-2}td}$, $f_0(u)^{\phi^{n-a-2+i}}$, and

$$E_0(u)^{\phi^{n-1}+\cdots+\phi^{\max\{s-1,n-a-1+i\}}-\phi^{\min\{s-2,n-a-2+i\}}-\cdots-\phi^{\max\{s-a-1,i-1\}}+\phi^{\min\{s-a-2,i-2\}}+\cdots+1}$$

The number of $E_0(u)^{\phi^j}$-factors with $j > 0$ is equal to $n-1-\max\{s-1, n-a-1+i\}+1 = \min\{n-s+1, a+1-i\}$, and $n-s+1 \geq i_r$ because $r \leq q_s$, $a+1-i \geq i_r$ because of the assumption on the range of i. Therefore apply Lemma 7.3.2, modulo $\mathfrak{M}$ we can write it as $p^{-i_r}\pi_0^{j_r}(g_1 + \pi_0 g_1 + \pi_0^2 g_2 + \cdots + \pi_0^{i_r e_0 - j_r - 1} g_{i_r e_0 - j_r - 1})$, with

$$\begin{aligned} \mathrm{ord}_u g_k &\geq d(p^{\max\{s-1, n-a-1+i\}} - e_0(p^{\min\{s-2, n-a-2+i\}} + \cdots + p^{s-a-1}) \\ &\quad + p^{n-a-2+i}t - p^{s-a-2}t) \\ &\geq D(s,r) \end{aligned}$$

When $i = a+2-i_r$, the coefficient of e_i is the product of a scalar in $W(k)$ with $p^{-i_r}\pi_0^{j_r}$ and

$$u^{-p^{s-a-2}td} E_0(u)^{\phi^{n-1}+\cdots+\phi^{n+1-i_r}-\phi^{s-2}-\cdots-\phi^{\max\{s-a-1, a+1-i_r\}}+\phi^{\min\{s-a-2, a-i_r\}}+\cdots+1} f(u)^{\phi^{n-i_r}}$$

This time $n - i_r \geq s-1 > s-2$, and $i_r e_0 - j_r - 1 \leq (i_r - 1)e_0 + t - 1$ (*Note that here we use the condition that* $j_r \geq e_0 - t$). Hence by Lemma 7.3.2 (b), modulo 1 we can write it as $p^{-i_r}\pi_0^{j_r}(g_1 + \pi_0 g_1 + \pi_0^2 g_2 + \cdots + \pi_0^{i_r e_0 - j_r - 1} g_{i_r e_0 - j_r - 1})$, with $\mathrm{ord}_u g_k \geq d((t-(e_0-j_r)+1)p^{n-i_r} - e_0(p^{s-2} + \cdots + p^{s-a-1}) - tp^{s-a-2}) \geq d(p^{s-1} - e_0(p^{s-2} + \cdots + p^{s-a-1}) - (i_r e_0 - j_r)p^{s-a-2}) = D(s,r)$

When $i \geq s + i_r + 1$, the coefficient of e_i is the product of a scalar in $W(k)$ with

$$p^{-i_r}\pi_0^{j_r} u^{-p^{s-a-2}td} E_0(u)^{\phi^{i-2}+\cdots+\phi^{\max\{i-a-1, s-1\}}-\phi^{\min\{i-a-2, s-2\}}-\cdots-\phi^{s-a-1}} f_0(u)^{\phi^{i-a-2}}$$

, with estimates on the order of the g_k's. The number of $E_0(u)^{\phi^j}(j > 0)$-factors is $i-2-\max\{s-1, i-a-1\}+1 = \min\{i-s, a\}$. If $i_r \leq a$, then $\min\{i-s, a\} \geq i_r$. Hence by Lemma 7.3.2 (a) (b), modulo 1 we can write this coefficient as $p^{-i_r}\pi_0^{j_r}(g_1 +$

$\pi_0 g_1 + \pi_0^2 g_2 + \cdots + \pi_0^{i_r e_0 - j_r - 1} g_{i_r e_0 - j_r - 1})$, with

$$\begin{aligned} \mathrm{ord}_u g_k &\geq d(p^{\max\{s-1, n-a-1+i\}} - e_0(p^{\min\{s-2, n-a-2+i\}} + \cdots + \\ &\quad p^{s-a-1}) + p^{i-a-2}t - p^{s-a-2}t) \\ &\geq D(s,r) \end{aligned}$$

If $i_r = a+1$, then $i \geq s + i_r + 1$ implies $i - a - 2 \geq s$; at the same time, $i_r e_0 - j_r - 1 \leq (i_r - 1)e_0 + t - 1$ (*Note that here we use the condition that* $j_r \leq e_0 - t$). Hence by Lemma 7.3.2(b), modulo 1 we can write this coefficient as $p^{-i_r}\pi_0^{j_r}(g_1 + \pi_0 g_1 + \pi_0^2 g_2 + \cdots + \pi_0^{i_r e_0 - j_r - 1} g_{i_r e_0 - j_r - 1})$, with

$$\begin{aligned} \mathrm{ord}_u g_k &\geq d((t - (e_0 - j_r) + 1)p^{i-a-2} - e_0(p^{s-2} + \cdots + p^{s-a-1}) - tp^{s-a-2}] \\ &\geq d[p^s - e_0(p^{s-2} + \cdots + p^{s-a-1}) - tp^{s-a-2}) \\ &\geq D(s,r) \end{aligned}$$

When $s+1 \leq i \leq s + i_r$, the coefficient of e_i is the product of a scalar in $W(k)$ with

$$p^{-i_r}\pi_0^{j_r} u^{-p^{s-a-2}td} E_0(u)^{\phi^{i-2} + \cdots + \phi^{\max\{i-a-1, s-1\}} - \phi^{\min\{i-a-2, s-2\}} - \cdots - \phi^{s-a-1}} f_0(u)^{\phi^{i-a-2}}$$

From the assumption on s and i we know $i \leq s + i_r$. If $i_r \leq a$ or if $i_r = a+1$ and $i \leq s+a$, then $i - a - 2 \leq s - 2$, hence by Lemma 7.3.2 (a), modulo 1 we can write it as $p^{-i_r}\pi_0^{j_r}(g_1 + \pi_0 g_1 + \pi_0^2 g_2 + \cdots + \pi_0^{i_r e_0 - j_r - 1} g_{i_r e_0 - j_r - 1})$ with the following estimates on the order of the g_k's: $\mathrm{ord}_u g_k \geq d(p^{s-1} - e_0(p^{i-a-2} + \cdots + p^{s-a-1}) + tp^{i-a-2} - tp^{s-a-2}) \geq D(s,r)$ when $k \leq (i-s)e_0 - 1$, and $\mathrm{ord}_u g_k \geq d(-(k - (i-s)e_0 + e_0 - t)p^{i-a-2} - e_0(p^{i-a-3} + \cdots + p^{s-a-1}) - tp^{s-a-2})$ when $k \geq (i-s)e_0$. If $i_r = a+1$ and $i = s + i_r$, because $i - a - 2 = s - 1$, and $i_r e_0 - j_r - 1 \leq ae + t - 1$ (*Note that here we use*

the condition that $j_r \leq e_0 - t$), hence apply Lemma 7.3.2 (c) we can write it as $p^{-i_r}\pi_0^{j_r}(g_1 + \pi_0 g_1 + \pi_0^2 g_2 + \cdots + \pi_0^{i_r e_0 - j_r - 1} g_{i_r e_0 - j_r - 1})$ with $\mathrm{ord}_u g_k \geq D(s,r)$.

When $i = s$, the coefficient of e_s is equal to $p^{-i_r}\pi^{j_r} u^{-p^{s-a-2}td} f_0(u)^{\phi^{s-a-2}}$. Note that $f_0(u)$ is a monic Eisenstein polynomial of degree $p^{s-a-2}td$. By Proposition 7.3.1(d) and Lemma (5.3.3), we can write it as $p^{-i_r}\pi_0^{j_r}(g_0 + \pi_0 g_1 + \pi_0^2 g_2 + \cdots + \pi_0^{i_r e_0 - j_r - 1} g_{i_r e_0 - j_r - 1})$ with $g_0 = 1$, and $\mathrm{ord}_u g_k \geq -kp^{s-a-2}d$.

Now let us summarize the estimates above and write down a representation of v^*. The formula will differ slightly according to whether $i_r \leq a$ or $i_r = a + 1$.

(i) First suppose $i_r \leq a$, then we can write

$$\begin{aligned} v^* \;=\; & p^{-i_r}\pi_0^{j_r} e_s + \sum_{i \leq a+2-i_r, \text{ or } i \geq s+i_r+1} v^*(i) e_i + \\ & \sum_{s+1 \leq i \leq s+i_r} \sum_{j=0}^{i_r e_0 - j_r - 1} h_{i,j} p^{-i_r} \pi_0^{j_r + j} e_i + \sum_{j=1}^{i_r e_0 - j_r - 1} h_{s,j} p^{-i_r} \pi_0^{j_r + j} e_s \end{aligned}$$

knowing:

(a) when $i \leq a + 2 - r$ or $i \geq s + i_r + 1$, $\mathrm{ord}_u v^*(i) \geq D(s,r)$.

(b1) when $s + 1 \leq i \leq s + i_r$ and $j \leq (i - s)e_0 - 1$, $\mathrm{ord}_u h_{i,j} \geq D(s,r)$.

(b2) when $s + 1 \leq i \leq s + i_r$ and $j \geq (i - s)e_0$, $\mathrm{ord}_u h_{i,j} \geq d(-(j - (i - s)e_0 + e_0 - t)p^{i-a-2} - e_0(p^{i-a-3} + \cdots + p^{s-a-1}) - tp^{s-a-2})$.

(c) when $i = s$ and $1 \leq j \leq i_r e_0 - j_1 - 1$, $\mathrm{ord}_u h_{i,j} \geq -jp^{s-a-2}d$.

For each j satisfying $0 \leq j \leq i_r e_0 - j_r$, there exists a unique pair of (i'_r, j'_r) with $0 \leq j'_r \leq e_0 - 1$ such that $i'_r e_0 - j'_r = i_r e_0 - j_r - j = r - j$. For each $1 \leq i \leq n$, let $\epsilon_{i,j}$ be the unit in $W(k)$ such that $\epsilon_{i,j}^{-1} p^{-i_r}\pi^{j_r + j} \cdot e_i = p^{-i'_r}\pi^{j'_r} \cdot e_i$. Now we define

$$w_s^{(r)} := v^* - \sum_{(i,j) \text{as in (b2) and (c)}} h_{i,j}\epsilon_{i,j} w_i^{(r - jd_0)}$$

By induction hypothesis we have already constructed $w_i^{(r-jd_0)}$ in $\mathfrak{N}_{A_i^{(r-j)}}$. One can check that under the conditions on the range of i, j, we indeed have $A_i^{(r-j)} \subset A_s^{(r)}$. Next we verify $\mathrm{ord}_u(w_s^{(r)} - p^{-i_r}\pi_0^{j_r}e_s) \geq D(s, i_r)$. Write $w_s^{(r)} - p^{-i_r}\pi_0^{j_r}e_s$ as

$$\sum_{\substack{i\leq a+2-i_r \\ \text{or} \\ i\geq s+i_r+1}} v^*(i)e_i + \sum_{\substack{s+1\leq i\leq s+i_r \\ j\leq (i-s)e-1}} h_{i,j}p^{-i_r}\pi^{j_r+j}e_i - \sum_{\substack{s+1\leq i\leq s+i_r \\ j\geq (i-s)e}} h_{i,j}\epsilon_{i,j}(w_i^{(r-jd_0)} -$$

$$\epsilon_{i,j}^{-1}p^{-i_r}\pi^{j_r+j}e_i) - \sum_{1\leq j\leq i_re_0-j_r-1} h_{s,j}(w_s^{(r-jd_0)} - \epsilon_{s,j}^{-1}p^{-i_r}\pi^{j_r+j}e_s)$$

We have shown the first two terms in the formula have orders higher than or equal to $D(s, r)$. For the third term, by the induction hypothesis and the choice of $\epsilon_{i,j}$ we know $\mathrm{ord}_u(w_i^{(r-j)} - \epsilon_{i,j}^{-1}p^{-i_r}\pi^{j_r+j}e_i) \geq D(i, r-j)$, and we have shown $\mathrm{ord}_u h_{i,j} \geq d(-(j-(i-s)e_0+e_0-t)p^{i-a-2} - e_0(p^{i-a-3}+\cdots+p^{s-a-1}) - tp^{s-a-2})$, therefore we are reduced to the inequality which is an easy exercise:

$$\begin{aligned} & p^{i-1} - e_0(p^{i-2}+\cdots+p^{i-a-1}) - (i_re_0 - j_r - j)p^{i-a-2} \\ & -(j-(i-s)e_0+e_0-t)p^{i-a-2} - e_0(p^{i-a-3}+\cdots+p^{s-a-1}) - tp^{s-a-2} \\ \geq\ & p^{s-1} - e_0(p^{s-2}+\cdots+p^{s-a-1}) - rp^{s-a-2} \end{aligned}$$

For the fourth term, since $\mathrm{ord}_u(w_s^{(r-j)} - \epsilon_{s,j}^{-1}p^{-i_r}\pi^{j_r+j}e_i) \geq D(s, r-jd_0)$, and $\mathrm{ord}_u h_{s,j} \geq -jp^{s-a-2}d$, hence its order is greater than or equal to $D(s, r-j) - jp^{s-a-2}d = D(s, r)$.

(ii) If $i_r = a+1$, then according to the estimates on the cofficient of each e_i, we can write

$$\begin{aligned} v^* \ =\ & p^{-i_r}\pi_0^{j_r}e_s + \sum_{i\leq a+2-i_r,\ \text{or}\ i\geq s+i_r} v^*(i)e_i + \\ & \sum_{s+1\leq i\leq s+i_r-1} \sum_{j=0}^{i_re_0-j_r-1} h_{i,j}p^{-i_r}\pi_0^{j_r+j}e_i + \sum_{j=1}^{i_re_0-j_r-1} h_{s,j}p^{-i_r}\pi_0^{j_r+j}e_s \end{aligned}$$

knowing:

(a′) when $i \leq a+2-r$ or $i \geq s+i_r$, $\mathrm{ord}_u v^*(i) \geq D(s,r)$.

(b1′) when $s+1 \leq i \leq s+i_r-1$ and $j \leq (i-s)e_0-1$, $\mathrm{ord}_u h_{i,j} \geq D(s,r)$.

(b2′) when $s+1 \leq i \leq s+i_r-1$ and $j \geq (i-s)e_0$, $\mathrm{ord}_u h_{i,j} \geq d(-(j-(i-s)e_0+e_0-t)p^{i-a-2}-e_0(p^{i-a-3}+\cdots+p^{s-a-1})-tp^{s-a-2})$.

(c′) when $i=s$ and $1 \leq j \leq i_r e_0 - j_1 - 1$, $\mathrm{ord}_u h_{i,j} \geq -jp^{s-a-2}d$.

Define $w_s^{(r)} := v^* - \sum_{(i,j)\text{as in (b2′) and (c′)}} h_{i,j}\epsilon_{i,j} w_i^{(r-jd_0)}$, by the same argument as in the case when $i_r \leq a$ we can prove $\mathrm{ord}_u(w_s^{(r)} - p^{-i_r}\pi_0^{j_r} e_s) \geq D(s,i_r)$, too.

This finishes the inductive proof of the proposition. □

Now for any reduced $\xi(\Phi)$-admissible vector $\underline{d} = (d_s)_s \in \mathbb{N}^n$, we define a subgroup $A(\underline{d}) \subset p^{-n}\mathcal{O}_F/\mathcal{O}_F$ such that $\#A(\underline{d}) = p^{\sum_{s=1}^{n} d_s}$, and $A_s^{(r)} \subset A(\underline{d})$ for all $s = 1, 2, \cdots, n$ and $r = 1, 2, \cdots, d_s$. We first make a few combinatorical definitions:

- Define a subset $H(\underline{d}) \subset \{1, 2, \cdots, n\} \times \mathbb{N}^*$ as $H(\underline{d}) := \{(s,r) | 1 \leq s \leq n, 1 \leq r \leq d_s\}$.

- For $k = 1, 2, \cdots, a+1$, $l = 0, 1, \cdots, e_0 - 1$, define $\Gamma_{k,l} := \{(n, ke_0 - l), (n-1, ke_0 - l), \cdots, (a+2, ke_0 - l), (a+1, ke_0 - l - t), (a, (k-1)e_0 - l - t), (a-1, (k-2)e_0 - l - t), \cdots\}$.

- Define $h_{k,l} := \#(H(\underline{d}) \cap \Gamma_{k,l})$, $d_l' := \sum_{j=1}^{a+1} h_{k,l} - 1$, and $m_{i,l} := k$ if $\sum_{j=k+1}^{a+1} h_{j,l} \leq i \leq \sum_{j=k}^{a+1} h_{j,l} - 1$.

By the definition of the $\Gamma_{k,l}$'s, one can check that if $\underline{d}$ is $\xi(\Phi)$-admissible and reduced, then $H(\underline{d}) \subset \bigcup_{k=1}^{a+1} \bigcup_{l=0}^{e_0-1} \Gamma_{k,l}$, and one can also prove the following chain of inequality: $h_{k,e_0-1} \geq h_{k,e_0-2} \geq \cdots \geq h_{k,e_0-t} \geq h_{k,e_0-t-1} - 1 \geq h_{k,e_0-t-2} - 1 \geq \cdots \geq h_{k,0} - 1 \geq h_{k+1,e_0-1} - 1 \geq h_{k+1,e_0-2} - 1 \geq \cdots$.

Definition 7.4.3. With the above notations, define $h(\underline{d}) :=$ the largest integer k such that $H(\underline{d}) \cap \Gamma_{k,l} \neq \emptyset$ for some $0 \leq l \leq e_0 - 1$. Define $A(\underline{d}) := \prod_{l=0}^{e_0-1} \prod_{j=0}^{d'_l} \langle p^{-m_{j,l}} \pi_0^l \zeta_j \rangle \subset p^{-h(\underline{d})} \mathcal{O}_F / \mathcal{O}_F$.

Proposition 7.4.4. *We have* $\#A(\underline{d}) = p^{\sum_{s=1}^{n} d_s}$ *and* $A_s^{(r)} \subset A(\underline{d})$ *for all* $s = 1, 2, \cdots, n$ *and* $r = 1, 2, \cdots, d_s$.

Proof. The first statement is a direct corollary of the fact that $H(\underline{d}) \subset \bigcup_{k=1}^{a+1} \bigcup_{l=0}^{e_0-1} \Gamma_{k,l}$. For the second statement, we can write $r = i_r e_0 - j_r$ with $0 \leq j_r \leq e_0 - 1$. The definition of $A_s^{(r)}$ differs according to the range of s and j_r. Similarly as in Proposition 7.4.2, we give a proof when $a+2 \leq s \leq n$ and $e_0 - t \leq j_r \leq e_0 - 1$, and the details for the other cases will be left as exercises.

The fact that $(s, i_r e_0 - j_r) \in H$ and $s \geq a+2$, $j_r \geq e_0 - t$ implies $h_{i_r,j_r} \geq s + i_r - a - 2$. Moreover, for any $j \geq j_r$, $h_{i_r,j} \geq h_{i_r,j_r} \geq s + i_r - a - 2$; hence $\sum_{i=i_r}^{a+1} h_{i,j} - 1 \geq s + i_r - a - 3$. For any $j \leq e_0 - t - 1$, $h_{i_r-1,j} \geq h_{i_r-1,0} \geq h_{i_r,e_0-1} \geq h_{i_r,j_r}$; hence $\sum_{i=i_r-1}^{a+1} h_{i,j} - 1 \geq s + i_r - a - 3$. For any $e_0 - t \leq j \leq j_r - 1$, $h_{i_r-1,j} \geq h_{i_r-1,0} - 1 \geq h_{i_r,e_0-1} - 1 \geq h_{i_r,j_r} - 1$; hence $\sum_{i=i_r-1}^{a+1} h_{i,j} - 1 \geq s + i_r - a - 4$. This proves $A_s^{(r)}$ is contained in $A(\underline{d})$. $\square$

By a combination of Proposition (7.4.2) and (7.4.4), we deduce that $\mathfrak{N}_{A(\underline{d})} \bmod u = N(\underline{d})$. This proves for every reduced $\xi(\Phi)$-admissible vector $\underline{d} \in \mathbb{N}^n$, $G(\underline{d})$ lifts to a finite locally free subgroup scheme $\mathcal{G}_{A(\underline{d})}$ of $\mathcal{X}_{R_1}$. For a general $\xi(\Phi)$-admissible vector $\underline{d}' \in \mathbb{N}^n$, there exists a reduced $\xi(\Phi)$-admissible vector $\underline{d}$ and a non-negative integer i, such that $\underline{d}' = \underline{d} + (i, i, \cdots, i)$. If we compose the isogenies $\mathcal{X}_{R_1} \xrightarrow{i} \mathcal{X}_{R_1} \xrightarrow{\pi} \mathcal{X}_{R_1}/\mathcal{G}_{A(\underline{d})}$, where $\pi : \mathcal{X}_{R_1} \to \mathcal{X}_{R_1}/\mathcal{G}_{A(\underline{d})}$ is the quotient isogeny, then the reduction of $\mathrm{Ker}(\pi \circ p^i)$ is equal to $G(\underline{d}')$. This finishes the proof of Theorem (7.2.1).

Remark 7.4.5. From the definition of $A(\underline{d})$ we can see it is in fact $p^{h(\underline{d})}$-torsion, where the integer $h(\underline{d})$ is defined in (7.4.3). Therefore in Theorem (7.2.1), for each $\mathcal{O}_F$-stable subgroup G of $\mathcal{X}_k$, we can have control on the extension $R/W(k)$ such that G admits a lifting to a finite locally free subgroup scheme of $\mathcal{X}_R$. Similarly, in Corollary (7.2.3), we can also have control on the endomorphism ring of the CM lifting and the ramification of the base ring of the CM lifting.

Chapter 8

A first complete list of potentially liftable subgroups

Let F be a p-adic local field, Φ be a primitive p-adic CM type for F, F' be the reflex field. Let $\mathcal{X}$ be the (unique) $\mathcal{O}_F$-linear CM p-divisible group over $R_0 := \mathcal{O}_{F' \cdot B(k)}$ with p-adic CM type Φ. A subgroup G of $X := \mathcal{X}_k$ is said to be *potentially liftable*, if there exists a finite extension R over R_0 and a finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{X}_R$ such that $\mathcal{G}_k = G$. A complete list of potentially liftable subgroups of $\mathcal{X}_k$ would allow us to identify which F-linear CM p-divisible groups admit an F-linear CM lifting with p-adic CM type Φ. In (6.1.2), for a class of p-adic CM types Φ, we proved that every $\mathcal{O}_F$-stable subgroup of $\mathcal{X}_k$ is potentially liftable. We will prove the same property for a broader class of p-adic CM types in (7.2), and give examples of other p-adic CM types such that not every $\mathcal{O}_F$-stable subgroup of $\mathcal{X}_k$ is potentially

liftable in (7.1).

In general to give a complete list of potentially liftable subgroups of $\mathcal{X}_k$, we need to let R run over all the finite extensions of R_0, and compute the reductions of all finite locally free subgroup schemes of $\mathcal{X}_R$. When $\dim \mathcal{X} = 1$ or $\operatorname{codim} \mathcal{X} = 1$, as we will explain in (8.1.5 (b)), the computation is trivial simply because the closed fiber $\mathcal{X}_k$ "does not have many subgroups". In this chapter, we will compute a first non-trivial example.

8.1 The main theorem

we first set up the example and make some definitions to state the main theorem and its corollaries. Let $p > 2$, $F = B(\mathbb{F}_{p^2})[\pi_0]/(\pi_0^2 - \epsilon p)$, where $\epsilon \in W(\mathbb{F}_{p^2})^\times$ is a Teichmuller lift and is not a square. The degree 4 extension $F/\mathbb{Q}_p$ is Galois, and $\mathrm{Gal}(F/\mathbb{Q}_p)$ is a cyclic group of order 4 generated by the automorphism $\tau : F \to F$, such that $\tau|_{B(\mathbb{F}_{p^2})} = \sigma$, and $\tau(\pi_0) = \epsilon^{\frac{p-1}{2}}\pi_0$. Throughout this section, we denote $\epsilon^{\frac{p-1}{2}}$ by λ for simplicity.

A primitive p-adic CM type for F has the form of $\{i_0, i_0 \circ \tau\}$, where i_0 is an embedding of F into $\overline{\mathbb{Q}}_p$. We identify F with its image in $\overline{\mathbb{Q}}_p$ by i_0 when there is no danger of confusion. Take an identification between $\mathrm{Hom}(F^{\mathrm{ur}}, \overline{\mathbb{Q}}_p)$ and $\{1, 2\}$ as $\mathrm{Gal}(F^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathbb{Z}/2$-torsors such that $i_0|_{F^{ur}} = 1$.

The reflex field F' of (F, Φ) is equal to F. Let $\mathcal{X}$ be the $\mathcal{O}_F$-linear CM p-divisible group over $R_0 = W(k)[\pi_0]/(\pi_0^2 - \epsilon p)$. The closed fiber $X := \mathcal{X}_k$ is an $\mathcal{O}_F$-linear CM

p-divisible group over k. The Grothendieck group $R_k(\mathcal{O}_F)$ of the category of finitely generated $\mathcal{O}_F \otimes_{\mathbb{Z}} k$-modules is isomorphic to $R_k(\mathcal{O}_F \otimes_{\mathcal{O}_{F^{\mathrm{ur}},1}} k) \times R_k(\mathcal{O}_F \otimes_{\mathcal{O}_{F^{\mathrm{ur}},2}} k) \cong \mathbb{Z} \times \mathbb{Z}$. The Lie type of X is defined to be $[\mathrm{Lie}(X)] = (1,1)$ in $R_k(\mathcal{O}_F)$. Define a Dieudonné module M as follows: (a) $M = W(k)[\pi]/(\pi^2 - \epsilon p)e_1 \oplus W(k)[\pi]/(\pi^2 - \epsilon^\sigma p)e_2$; (b) there is an $\mathcal{O}_F$-action on M defined by: $\alpha \cdot e_1 = \alpha e_1$, $\alpha \cdot e_2 = \alpha^\sigma e_2$ for $\alpha \in W(\mathbb{F}_{p^2})$, and $\pi_0 \cdot e_i = \pi e_i$; (c) the $\mathcal{O}_F$-linear Frobenius and Verschiebung maps on M are defined by:

$$Fe_1 = -\epsilon^{-1}\lambda^{-1}\pi e_2, Fe_2 = -\epsilon^{-1}\pi e_1, Ve_1 = -\pi e_2, Ve_2 = -\lambda^{-\sigma}\pi e_1$$

The p-divisible group attached to M is $\mathcal{O}_F$-linear with Lie type $(1,1)$, hence is $\mathcal{O}_F$-linearly isomorphic to X. Therefore M is $\mathcal{O}_F$-linearly isomorphic to the Dieudonné module attached to X. We say an $\mathcal{O}_F$-basis e_1, e_2 of M is "good", if the conditions (a), (b), (c) above are satisfied. If e_1', e_2' is another good $\mathcal{O}_F$-basis of M, then there exists $\zeta \in \mathcal{O}_F^\times$ such that $e_1' = \zeta e_1$, $e_2' = \zeta^\sigma e_2$.

One can check $\dim_k M/(FM + VM) = 2$, so the a-number of X is equal to 2. The set of α_p embedded in X is in bijective correspondence with $\mathbb{P}^1(k)$, i.e., the set of lines in $\pi_0^{-1}M/M \cong ke_1 + ke_2$. Define the following equivalent relation $\sim$ on $\mathbb{P}^1(k)$: $[a_1, b_1] \sim [a_2, b_2]$ if and only if there exists $c \in \mathbb{F}_{p^2}^\times$ such that $[a_1 c, b_1 c^p] = [a_2, b_2]$ in $\mathbb{P}^1(k)$. Denote the equivalent classes on $\mathbb{P}^1(k)$ by $\mathfrak{L}$. The set $\mathfrak{L}$ can be naturally identified with $\{0, \infty\} \coprod \{k^\times/(\mathbb{F}_{p^2}^\times)^{p-1}\}$ by considering a/b for $[a, b] \in \mathbb{P}^1(k)$. For each subgroup G of X with order p, as an α_p embedded in X, we can associate to G an element $\delta_0(G)$ in $\mathfrak{L}$. By our definition, $\delta_0(G)$ does not depend on the choice

of the good $\mathcal{O}_F$-basis e_1, e_2 in M, so it is a well-defined invariant for subgroups G of X with order p. Similarly, suppose G is a subgroup of X such that $X[\pi_0^n] \subset G$ for some integer n, and $[G : X[\pi_0^n]] = p$, then the Dieudonné module N attached to G is between $\pi_0^{-n}M/M$ and $\pi_0^{-(n+1)}M/M$. Thus we can also associate to G a well-defined invariant $\delta_n(G) \in \mathfrak{L}$ by looking at the direction of the k-line $N/(\pi_0^{-n}M/M)$ in $\pi_0^{-(n+1)}M/\pi_0^{-n}M$.

Now we are ready to state the main results of this section:

Theorem 8.1.1. *Notations are as above.*

(1) Suppose R is a finite extension of R_0 and $\mathcal{G}$ is a finite locally free subgroup scheme of $\mathcal{X}_R$ with order p^t, where t is an integer. Then we have the following descriptions on the closed fiber $G := \mathcal{G}_k$ as a subgroup of X:

(a) If $t = 2n$ is even, then $G = X[\pi_0^n]$.

(b) If $t = 2n + 1$ is odd, then $X[\pi_0^n]$ is contained in G with index p, and the invariant $\delta_n(G)$ is equal to either $[1]$ or $[\overline{\lambda}]$ in $\mathfrak{L}$.

(2) Conversely, for each subgroup H of X such that $X[p^n] \subset H$ with index p and $\delta_n(H) = [1]$ or $[\overline{\lambda}]$, there exists a finite extension R of R_0 and a finite locally free subgroup scheme $\mathcal{H}$ of $\mathcal{X}_R$ such that $\mathcal{H}_k = H$.

In particular, the closed fiber G is $\mathcal{O}_F$-stable if and only if the order of $\mathcal{G}$ is an even power of p.

Theorem (8.1.1) has the following consequences:

Corollary 8.1.2. *Let X be the $\mathcal{O}_F$-linear CM p-divisible group over k with Lie type $(1,1)$. If Y is an F-linear CM p-divisible group over k, then Y admits an F-linear CM lifting with p-adic CM type compatible with τ^2 if and only if:*

either (a) Y is F-linearly isomorphic to X;

or (b) Y is F-linearly isomorphic to X/G, where G is a subgroup of X with order p, and $\delta_0(G) = [1]$ or $[\overline{\lambda}]$.

In particular, if Y is $\mathcal{O}_F$-linear, then Y admits an F-linear CM lifting with p-adic CM type compatible with τ^2 if and only if $[Lie(Y)] = (1,1)$ in $R_k(\mathcal{O}_F)$.

Proof. Saying a p-adic CM type Φ for F is compatible with ι is equivalent to saying Φ has the form $\{i_0, i_0 \circ \tau\}$ for some $i_0 \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$. Sufficiency follows immediately from Theorem (8.1.1 (2)). For necessity, suppose R a complete discrete valuation ring of characteristic 0 and residue field k, $\mathcal{Y}$ is an F-linear CM p-divisible group over R lifting Y with p-adic CM type Φ compatible with τ^2. Then Φ must be primitive. Let F' be the reflex field, $R_0 := \mathcal{O}_{F' \cdot B(k)}$, and $\mathcal{X}$ be the $\mathcal{O}_F$-linear CM p-divisible group over R_0 with p-adic CM type Φ. Then $\mathcal{Y}$ is F-linearly isogeneous to $\mathcal{X}$, and the necessity of the statement also follows from Theorem (8.1.1 (1)). For the last statement, we need to show that if Y is $\mathcal{O}_F$-linear and the Lie type of Y is equal to $(2,0)$ or $(0,2)$, then Y does not admit an F-linear CM lifting with p-adic CM type compatible with τ^2. It is easy to check that under such conditions, there exists an F-linear isogeny $X \to Y$ such that the Dieudonné module attached to Y is equal to $\pi_0^{-1}M_1 \oplus M_2$ or $M_1 \oplus \pi_0^{-1}M_2$. Therefore Y is isomorphic to X/G, where

G is a subgroup of X with order p and $\delta_0(G) = 0$ or ∞. This G is not potentially liftable by (b). □

Remark 8.1.3. As a corollary, the answer to question (sCML) relative to (F, F^{ur}) for p-divisible groups is negative. Note that the reflex field F' of Φ is equal to F, so the residue field $\kappa_{F'}$ is *not* "small" in the sense of (4.1.1). Thus we obtain a new counterexample to question (sCML) that does not fall in the framework in chapter 4.

Corollary 8.1.4. *Suppose $p > 2$, L is a CM field and L_0 is its maximal totally real subfield. If there exists a place v of L_0 above p such that the inertia degree of v is 2 and v ramifies in L, then the answer to question (sCML) for abelian varieties is negative.* □

Proof. The completion $L_{0,v}$ is a degree 2 unramified extension over $\mathbb{Q}_p$, and L_v is a degree 2 ramified extension over $L_{0,v}$. It is an easy exercise in number theory to show that when $p > 2$, $L_v \cong B(\mathbb{F}_{p^2})[\pi_0]/(\pi_0^2 - p)$ or $B(\mathbb{F}_{p^2})[\pi_0]/(\pi_0^2 - \epsilon p)$, where ϵ is a Teichmuller lift in $W(\mathbb{F}_{p^2})^\times$ and is not a square. Then the statement follows from (8.1.3) and (4.1.1). □

The most interesting phenomenon revealed by Theorem (8.1.1) is that, no matter how arbitrary the subgroup scheme $\mathcal{G}$ in characteristic is, its reduction G seems to "try very hard" to be $\mathcal{O}_F$-stable. It is natural to ask the following question:

Let F be a p-adic local field, Φ be a primitive p-adic CM type for F. Let

F' be the reflex field of Φ. Let $\mathcal{X}$ be the $\mathcal{O}_F$-linear CM p-divisible group with p-adic CM type Φ over $R_0 := \mathcal{O}_{F'\cdot B(k)}$. Is there a general condition on the p-adic CM type Φ, such that there exists an integer $d(\Phi)$ which only depends on Φ, satisfying that for any finite extension R/R_0 and any finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{X}_R$, the closed fiber $G := \mathcal{G}_k$ contains an $\mathcal{O}_F$-stable subgroup with index uniformly bounded by $p^{d(\Phi)}$?

Remark 8.1.5. (a) If we drop the assumption that Φ is primitive, we can easily produce a class of finite locally free subgroup schemes $\mathcal{G}$ with arbitrarily large order, such that G does not contain any nontrivial $\mathcal{O}_F$-stable subgroups. In fact, suppose Φ is induced from a p-adic CM type Φ_1 for $F_1 \subsetneqq F$. Let $\mathcal{X}_1$ be the $\mathcal{O}_{F_1}$-linear CM p-divisible group with p-adic CM type Φ_1 over R_0. Then $\mathcal{X}$ is $\mathcal{O}_F$-linearly isomorphic to the Serre tensor construction $\mathcal{X}_1 \otimes_{\mathcal{O}_{F_1}} \mathcal{O}_F$. For any finite locally free subgroup scheme $\mathcal{G}_1$ of $\mathcal{X}_1$, when we embed it into $\mathcal{X}$ via the natural homomorphism $\mathcal{X}_1 \to \mathcal{X}$, the closed fiber of $\mathcal{G}_1$ does not contain any $\mathcal{O}_F$-stable subgroups of $\mathcal{X}$.

(b) When $\#\Phi = 1$ or $[F : \mathbb{Q}_p] - 1$, we can take $d(\Phi) = 0$. In fact, if $G \subset X$ is a subgroup, take a filtration $0 = G_0 \subset G_1 \subset G_2 \subset \cdots \subset G_s = G$, such that the index of G_i in G_{i+1} is equal to p for $i = 0, 1, \cdots, s-1$. The a-number of each X/G_i is equal to 1 since either the dimension or the codimension is equal to 1. Hence G_{i+1}/G_i is the unique subgroup of X/G_i with order p and G_{i+1}/G_i must be $\mathcal{O}_F$-stable. This proves every subgroup G of X is $\mathcal{O}_F$-stable.

(c) In the example we compute in this section, $\#\Phi = 2$ and $[F : \mathbb{Q}_p] = 4$. This

is a first nontrivial example concerning this question. As a corollary of Theorem (8.1.1), we can say $d(\Phi) = 1$ in our example.

In the rest of the section we prove Theorem (8.1.1). The proof is organized as follows. For each positive integer m, there exists a finite extension $E_m/\mathrm{Frac}\ R_0$ such that the p^m-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}}_p}$ are rational over E_m. In (8.2), we recall the constructions from chapter 5 on the Kisin module $\mathfrak{M}_m$ attached to $\mathcal{X}_{\mathcal{O}_{E_m}}$. As m runs over all the positive integers, we compute the closed fibers of the p^m-torsion finite locally free subgroup schemes $\mathcal{G}$ of $\mathcal{X}_{\mathcal{O}_{E_m}}$. The finite Kisin module $\mathfrak{N}$ attached to $\mathcal{G}$ is a $W(k)[[u]]$-module, and the Dieudonné module of the closed fiber $\mathcal{G}_k$ is $\mathfrak{N}/(\mathfrak{N} \cap (up^{-m}\mathfrak{M}_m/\mathfrak{M}_m)) \cong (\mathfrak{N} + up^{-m}\mathfrak{M}_m/\mathfrak{M}_m)/(up^{-m}\mathfrak{M}_m/\mathfrak{M}_m)$, which we will denote by $\mathfrak{N} \mod u$ in the future. At the end of subsection (8.2), we reduce the statements in Theorem (8.1.1) about the closed fiber $\mathcal{G}_k$ to the existence of certain special elements in $\mathfrak{N}$; see (8.2)(a), (b), and (c). On the other hand, the generators of the localization $\mathfrak{N}^0 := W(k)((u)) \otimes_{W(k)[[u]]} \mathfrak{N}$ have been computed in (5.2). In (8.3) we write these generators into explicit forms. In order to compute $\mathfrak{N} \mod u$, we need to find a $W(k)[[u]]$-basis of $\mathfrak{N}$ before the localization. This can be viewed as an analogy of finding a lattice in a vector space. We show several examples in (8.4), and then summarize a general linear algebra approach in (8.5). This approach successfully computes the closed fiber $\mathcal{G}_k$ in the case when the geometric generic fiber of $\mathcal{G}$ is generated by at most two elements; see (8.6). The remaining essential case is when the geometric generic fiber of $\mathcal{G}$ is generated by three elements. In

that case, it is difficult to apply directly the linear algebra approach in (8.5); see the example (8.6.3) at the end of (8.6). In (8.7), we explain how the Serre dual of $\mathcal{X}_{\mathcal{O}_{E_m}}$ comes to rescue for the problem. Finally in (8.8) we compute the closed fiber $\mathcal{G}_k$ via a detour by Serre dual in the case when the geometric generic fiber of $\mathcal{G}$ is generated by three elements, and complete the proof of Theorem (8.1.1).

If $\mathfrak{M}$ is a Kisin module (or a finite Kisin module), and x is an element in $\mathfrak{M}^0 := W(k)((u)) \otimes_{W(k)[[u]]} \mathfrak{M}$, then we define $\mathrm{ord}_u x$ to be the smallest integer d such that $u^{-d}x \in \mathfrak{M}$. If $\mathrm{ord}_u(x_1 - x_2) \geq D$, we also write $x_1 \equiv x_2 \mod \mathrm{ord}_u \geq D$.

8.2 The Kisin modules attached to $\mathcal{X}$ and its base changes

Now we prepare to prove Theorem (8.1.1). We first recall the constructions from chapter 5 on the Kisin module attached to $\mathcal{X}$, and its base changes to finite extensions of R_0.

Take $h(x) = -\pi_0 x + x^{p^2}$. For all positive integer r, define $h^{(r)}(x) := h \circ h \circ \cdots \circ h$ to be the r-th iteration of h, $h_r(x) := \frac{h^{(r)}(x)}{h^{(r-1)}(x)}$. For all positive integers m, Let π_m be a root of $h_{2m}(x)$ in $\overline{\mathbb{Q}}_p$, and define $E_m := F(\pi_m)$. Let $E_m(u)$ be the minimal Eisenstein polynomial of π_m over $B(k)$; so $E_m(u) = h_{2m}(u)\overline{h_{2m}}(u)$, where $\overline{h_{2m}}(u)$ is the conjugate of $h_{2m}(u)$ under $\pi_0 \mapsto -\pi_0$. One can check the constant term of $E_m(u)$ is equal to $-\epsilon p$. Let $\mathfrak{M}_m$ be the Kisin module constructed as in chapter 5

with (E_m, π_m), and let $\mathcal{X}_m$ be the associated p-divisible group over $\mathcal{O}_{E_m}$. By (5.2.4), $\mathcal{X}_m$ is the $\mathcal{O}_F$-linear CM p-divisible group over $\mathcal{O}_{E_m}$ with p-adic CM type Φ, and all the p^m-torsion points on its geometric generic fiber are rational over E_m. By (3.1.1) and (5.1.8), $\mathcal{X}_m$ is isomorphic to $\mathcal{X}_{\mathcal{O}_{E_m}}$, and the isomorphism induces identity over the closed fiber. Thus to prove Theorem (8.1.1), it suffices to compute the closed fibers of p^m-torsion finite locally free subgroup schemes of $\mathcal{X}_m$ when m runs over all positive integers.

By (5.1), the Kisin module $\mathfrak{M}_m = W(k)[[u]] \otimes_{\mathbb{Z}_p} \mathcal{O}_F e$ with the natural $\mathcal{O}_F$-action, and the $(\phi, \mathcal{O}_F)$-linear endomorphism $\phi_{\mathfrak{M}_m}$ (which we will abbreviate as ϕ_m in the future) is defined as $\phi_m e = P_{\Phi,\pi_m,B(k)\otimes_{\mathbb{Q}_p}F}(u)$, the characteristic polynomial of the natural action of π_m on the $W(k) \otimes_{\mathbb{Q}_p} F$-module $(E_m)_{i_0} \oplus (E_m)_{i_0\circ\tau}$, where the index indicates the F-structure. For the convenience of computation, we identify $W(k)[[u]] \otimes_{\mathbb{Z}_p} \mathcal{O}_F e$ with $W(k) \otimes_{1,\mathcal{O}_{F^{\mathrm{ur}}}} \mathcal{O}_F[[u]]e_1 \oplus W(k) \otimes_{2,\mathcal{O}_{F^{\mathrm{ur}}}} \mathcal{O}_F[[u]]e_2 \cong W(k)[\pi][[u]]/(\pi^2 - \epsilon p)e_1 \oplus W(k)[\pi][[u]]/(\pi^2 - \epsilon^\sigma p)e_2$. Under such an identification, one can check that $a \cdot e_1 = ae_1$, $a \cdot e_2 = a^\sigma e_2$ for $a \in \mathcal{O}_{F^{\mathrm{ur}}}$, and $\pi_0 \cdot e_i = \pi e_i$. The $(\phi, \mathcal{O}_F)$-linear endomorphism ϕ_m is defined by $\phi_m(e_1) = \tau_2(\overline{h_{2m}}(u))e_2, \phi_m(e_2) = \tau_1(\overline{h_{2m}}(u))e_1$, where τ_1 (resp. τ_2) is the $W(k)[[u]]$-isomorphism from $F \cdot B(k)[[u]] = B(k)[\pi_0]/(\pi_0^2 - \epsilon p)[[u]]$ to $W(k)[\pi]/(\pi^2 - \epsilon p)[[u]]$ (resp. $W(k)[\pi]/(\pi^2 - \epsilon^\sigma p)[[u]]$) that sends π_0 to π (resp. $\lambda^{-1}\pi$).

Let X_m be the closed fiber of $\mathcal{X}_m$, let $M(X_m)$ be the attached Dieudonné module; by [1] (B.4) $M(X_m) \cong \mathfrak{M}_m/u\mathfrak{M}_m$. If we still use e_i to stand for the image of e_i in

$M(X_m)$, one can check that e_1, e_2 is a "good" $\mathcal{O}_F$-basis of $M(X_m)$ (see the beginning of the section for the definition of a "good" $\mathcal{O}_F$-basis of $M(X_m)$). Now suppose $\mathcal{G}$ is a p^m-torsion finite locally free subgroup scheme of $\mathcal{X}_m$, $\#\mathcal{G} = p^t$. Let $\mathfrak{N}$ be the attached finite Kisin submodule. To prove Theorem (8.1.1(1)), it suffices to show:

(8.2.a) When $t = 2n$ is even, there exists $w_s^{(n)} \in \mathfrak{N}$ for $s = 1, 2$, such that $w_s^{(n)} \equiv x_s \pi^{-n} e_s \mod u$, where $x_s \in W(k)^\times$.

(8.2.b) When $t = 2n+1$ is odd, there exists $w \in \mathfrak{N}$ such that $w \equiv x_1 \pi^{-(n+1)} e_1 + x_2 \pi^{-(n+1)} e_2 \mod u$, where $x_1, x_2 \in W(k)^\times$, and $\overline{x}_1/\overline{x}_2 \in (\mathbb{F}_{p^2}^\times)^{p-1}$ or $\overline{\lambda}(\mathbb{F}_{p^2}^\times)^{p-1}$. Here $\overline{x_i}$ means the image of x_i in $k^\times$ modulo p.

Conversely, to prove Theorem (8.1.1(2)) it suffices to show:

(8.2.c) for every $x_1, x_2 \in W(k)^\times$ such that $\overline{x}_1/\overline{x}_2 \in (\mathbb{F}_{p^2}^\times)^{p-1}$ or $\overline{\lambda}(\mathbb{F}_{p^2}^\times)^{p-1}$, there exists a positive integer m and a p^m-torsion finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{X}_m$ such that $\#\mathcal{G} = p^{2n+1}$ and we can find an element w in $\mathfrak{N}$ satisfying $w \equiv x_1 \pi^{-(n+1)} e_1 + x_2 \pi^{-(n+1)} e_2 \mod u$.

8.3 The finite Kisin modules attached to finite locally free subgroup schemes

To achieve the goals in 8.2, we need a precise description on the finite Kisin modules attached to p^m-torsion finite locally free subgroup schemes of $\mathcal{X}_m$.

The endomorphism ϕ on $W(k)[[u]]$ extends to $\phi : W(k)[\pi][[u]]/(\pi^2 - \epsilon p) \to$

$W(k)[\pi][[u]]/(\pi^2-\epsilon^\sigma p)$, such that $\phi|_{W(k)}=\sigma$, $\phi(\pi)=\pi$, and $\phi(u)=u^p$. Similarly we can define $\phi: W(k)[\pi][[u]]/(\pi^2-\epsilon^\sigma p)\to W(k)[\pi][[u]]/(\pi^2-\epsilon p)$ in the same way.

According to (5.2.4), if we define

$$v:=\tau_2(h^{(2m-1)}(u))^\phi\tau_1(h^{(2m-1)}(u))e_1+\tau_1(h^{(2m-1)}(u))^\phi\tau_2(h^{(2m-1)}(u))e_2$$

then all the solutions $x\in p^{-m}\mathfrak{M}_m/\mathfrak{M}_m$ to $\phi_m x=\frac{1}{-\epsilon}E_m(u)x$ have the form of $\eta\cdot v$ with $\eta\in p^{-m}\mathcal{O}_F/\mathcal{O}_F$. For any subgroup A of $p^{-m}\mathcal{O}_F/\mathcal{O}_F$, let $\mathfrak{N}_A^0:=W(k)((u))\{\eta\cdot v|\eta\in p^{-m}\mathcal{O}_F/\mathcal{O}_F\}$, and $\mathfrak{N}_A:=\mathfrak{N}_A^0\cap p^{-m}\mathfrak{M}_m/\mathfrak{M}_m$. Let $\mathcal{G}_A$ be the associated finite locally free subgroup scheme. When A runs over subgroups of $p^{-m}\mathcal{O}_F/\mathcal{O}_F$, $\mathcal{G}_A$ enumerates all p^m-torsion finite locally free subgroup schemes of $\mathcal{X}_m$. Denote $\mathfrak{N}_A/(\mathfrak{N}_A\cap up^{-m}\mathfrak{M}/\mathfrak{M})\cong(\mathfrak{N}_A+up^{-m}\mathfrak{M}_m/\mathfrak{M}_m)/(up^{-m}\mathfrak{M}_m/\mathfrak{M}_m)$ by $\mathfrak{N}_A \mod u$, then $\mathfrak{N}_A \mod u$ is the Dieudonné module of the closed fiber of $\mathcal{G}_A$.

Now we derive a more precise formula for $\eta\cdot v$. By the definition of $h^{(2m-1)}(u)$, we can write $h^{(2m-1)}(u)\equiv\sum_{i=0}^{2m-1}\pi_0^iA_i(u) \mod p^m$, such that $A_i(u)\in W(\mathbb{F}_{p^2})((u))^\times$ and $\mathrm{ord}_uA_i=p^{2(2m-1-i)}$. Therefore

$$\begin{aligned}
v &:= \tau_2(h^{(2m-1)}(u))^\phi\tau_1(h^{(2m-1)}(u))e_1+\tau_1(h^{(2m-1)}(u))^\phi\tau_2(h^{(2m-1)}(u))\\
&= (\sum_{n=0}^{2m-1}A_n(u)(\lambda^{-1}\pi)^n)^\phi(\sum_{n=0}^{2m-1}A_n(u)\pi^n)e_1+\\
&\quad (\sum_{n=0}^{2m-1}A_n(u)(\lambda^{-1}\pi)^n)(\sum_{n=0}^{2m-1}A_n(u)\pi^n)^\phi e_2\\
&= \sum_{n=0}^{2m-1}\pi^n(\sum_{k=0}^{n}A_k(u)^\phi A_{n-k}(u)\lambda^{-k\sigma})e_1+\sum_{n=0}^{2m-1}\pi^n(\sum_{k=0}^{n}A_k(u)^\phi A_{n-k}(u)\lambda^{-(n-k)})e_2
\end{aligned}$$

Recall that $\lambda=\epsilon^{\frac{p-1}{2}}$ and ϵ is a Teichmuller lift, so $\lambda^{1+\sigma}=\epsilon^{\frac{p^2-1}{2}}$. Because $\epsilon\notin W(\mathbb{F}_{p^2})^\times\backslash(W(\mathbb{F}_{p^2})^\times)^2$, we deduce $\epsilon^{\frac{p^2-1}{2}}=-1$. Hence we have $\lambda^{-\sigma}=-\lambda$ and we

can then rewrite the above formula for v as:

$$\sum_{n=0}^{2m-1}\pi^n(\sum_{k=0}^{n}A_k(u)^\phi A_{n-k}(u)(-\lambda)^k)e_1+\sum_{n=0}^{2m-1}(\lambda^{-1}\pi)^n(\sum_{k=0}^{n}A_k(u)^\phi A_{n-k}(u)\lambda^k)e_2$$

Definition 8.3.1. Define

$$\pi_1:=\pi \qquad \pi_2:=\tau\pi=\lambda^{-1}\pi$$

$$b_n:=\sum\lambda^{2i}A_{2i}(u)^\phi A_{n-2i}(u), \quad c_n:=\sum\lambda^{2i+1}A_{2i+1}(u)^\phi A_{n-2i-1}(u)$$

$$y_j:=b_j-c_j, \qquad z_j:=b_j+c_j$$

Under the notations above, $v=\sum\limits_{n=0}^{2m-1}\pi_1^n y_n e_1+\sum\limits_{n=0}^{2m-1}\pi_2^n z_n e_2$.

Now we derive a more precise formula of $\eta\cdot v$ for $\eta\in p^{-m}\mathcal{O}_F/\mathcal{O}_F$. Let ν be the valuation on F such that $\nu(\pi)=1$.

Definition 8.3.2. Suppose $\eta\in p^{-m}\mathcal{O}_F/\mathcal{O}_F$ and k is the smallest integer such that $\eta\in p^{-k}\mathcal{O}_F/\mathcal{O}_F$. Let $\alpha\in W(\mathbb{F}_{p^2})^\times$ and $\beta\in W(\mathbb{F}_{p^2})$ be the unique elements such that $\eta=p^{-k}(\alpha+\pi_0\beta)$ (resp. $\eta=p^{-k}\pi_0(\alpha+\pi_0\beta)$) when $\nu(\eta)=-2k$ (resp. $\nu(\eta)=-2k+1$). Define

$$\begin{aligned} v[\eta,r,1] &:= \epsilon^k(\alpha y_{-\nu(\eta)-r}+\beta y_{-\nu(\eta)-r-1}) \\ v[\eta,r,2] &:= \epsilon^k(\lambda^{2k+\nu(\eta)}\alpha^\sigma z_{-\nu(\eta)-r}+\beta^\sigma\lambda^{2k+\nu(\eta)+1}z_{-\nu(\eta)-r-1}) \end{aligned}$$

Under such notations, one can check $\eta\cdot v=\sum\limits_{s=1}^{2}\sum\limits_{r=1}^{2m}\pi_s^{-r}v[\eta,r,s]e_s$; when $r>-\nu(\eta)$ we treat $v[\eta,r,s]$ as zero. This formula will be refered to as *the presentation of* $\eta\cdot v$ in the future.

Before we dive into the computations, let us look into the definitions of the y_i, z_i's and $v[\eta,r,s]$'s, and derive some properties of them.

Proposition 8.3.3. *Define $d := 1 + p$. The following statements about b_i, c_i, y_i, z_i are true:*

(1) *b_i, c_i are both units in $W(k)((u))$, and*

$$\min\{ord_u b_i, ord_u c_i\} = p^{4m-2-i}d, \max\{ord_u b_i, ord_u c_i\} = p^{4m-1-i}(1 - p^{-1} + p^{-2})d$$

(2) *If $\min\{ord_u b_i, ord_u c_i\} = ord_u b_i$ (resp. $ord_u c_i$), then $\min\{ord_u b_{i+2}, ord_u c_{i+2}\} = ord_u c_{i+2}$ (resp. $ord_u b_{i+2}$).*

(3) *y_i, z_i are both units in $W(k)((u))$, and $ord_u y_i = ord_u z_i = p^{4m-2-i}d$.*

(4) *$u^{-p^{4m-2-i}d} y_i \equiv (-1)^{[\frac{i+1}{2}]} u^{-p^{4m-2-i}d} z_i \mod u$.*

(5) *$v[\eta, r, s]$ is a unit in $W(k)((u))$, and $ord_u v[\eta, r, s] = p^{4m-2+\nu(\eta)+r}d$; in particular, it is independent of s and increasing in r.*

(6) *For any $2 \leq i \leq 2m$, $y_i z_{i-2} - z_i y_{i-2}$ is a unit in $W(k)((u))$, and $ord_u(y_i z_{i-2} - z_i y_{i-2}) = ord_u y_i + ord_u z_{i-2} = ord_u z_i + ord_u y_{i-2} = d(p^{4m-i} + p^{4m-2-i})$.*

(7) *Let i, j be different integers between 0 and $2m-1$, and suppose $\gamma \in W(\mathbb{F}_{p^2})^\times$. Then $\gamma y_i y_j \pm \gamma^\sigma \lambda z_i z_j$, $\gamma z_i z_j \pm \gamma^\sigma \lambda y_i y_j$, and $\gamma y_i z_j \pm \gamma^\sigma \lambda z_i y_j$ are all units in $W(k)((u))$, and their orders are all equal to $d(p^{4m-2-i} + p^{4m-2-j})$.*

Proof. (1) and (2) are clear by a direct examination of each summand in the definition of b_i, c_i and using the elementary lemma (8.3.4) below. (3) is because of (1), and (4) follows from (2). (5) is clear by the definition of $v[\eta, r, s]$.

To see (6), note that $y_i z_{i-2} - z_i y_{i-2} = (b_i - c_i)(b_{i-2} + c_{i-2}) - (b_i + c_i)(b_{i-2} - c_{i-2}) = 2b_i c_{i-2} - 2b_{i-2} c_i$, then the statement follows from (1) and (2).

To see (7), when we expand them based on b_i, c_i, b_j, c_j, the coefficient of b_ib_j, b_ic_j, c_ib_j, and c_ic_j is $\gamma \pm \gamma^\sigma \lambda$. If $p|\gamma \pm \gamma^\sigma \lambda$, it implies that $\lambda^{\sigma+1} \equiv \gamma^{\sigma^2-1} = 1 \mod p$, contradiction to the fact that $\lambda^{\sigma+1} = \epsilon^{\frac{p^2-1}{2}} = -1$. Moreover, by (1) there is a unique term among b_ib_j, b_ic_j, c_ib_j, and c_ic_j that has the lowest order, and this order is equal to $d(p^{4m-2-i} + p^{4m-2-j})$. This proves the statement. □

Lemma 8.3.4. *Let $x = y + z$, $x, y, z \in W(k)((u))$. If y is a unit in $W(k)((u))$ and $ord_u z > ord_u y$, then x is also a unit in $W(k)((u))$ and $ord_u x = ord_u y$.* □

8.4 Examples of reductions of finite locally free subgroup schemes

We take this subsection to compute a few examples of $\mathfrak{N}_A$ and $\mathfrak{N}_A \mod u$.

Example 8.4.1. Let $m \geq 1$, $\eta \in p^{-1}\mathcal{O}_F/\mathcal{O}_F$, and $A = \langle \eta \rangle \cong \mathbb{Z}/p$. Then $\mathfrak{N}_A = W(k)((u))\{\eta \cdot v\} \cap p^{-1}\mathfrak{M}/\mathfrak{M}$. In the presentation $\eta \cdot v = \sum_{i=1}^{2}\sum_{j=1}^{2} \pi_i^{-j} v[\eta, j, i]e_i$, we know $v[\eta, j, 1]$ and $v[\eta, j, 2]$ are both units in $W(k)((u))$, and their orders are both equal to $p^{4m-2+\nu(\eta)+j}d$. Let $w := u^{-p^{4m-2+\nu(\eta)+j}d}(\eta \cdot v)$, then $w \equiv \sum_{i=1}^{2} x_i \pi_i^{-1} e_i \mod u$ for $x_1, x_2 \in W(k)^\times$, and the goal of (8.2.b) is achieved.

Example 8.4.2. Let $m \geq 2$, $\eta \in (p^{-2}\mathcal{O}_F/\mathcal{O}_F)\backslash(p^{-1}\mathcal{O}_F\mathcal{O}_F)$, $A = \langle \eta \rangle \cong \mathbb{Z}/p^2$. Let $v_1 := \eta \cdot v = \sum_{i=1}^{2}\sum_{j=1}^{4} \pi_i^{-j} v[\eta, j, i]e_i$, and $v_2 := (p\eta) \cdot v = \sum_{i=1}^{2}\sum_{j=1}^{2} \pi_i^{-j} v[p\eta, j, i]e_i$. We want to produce $w_1^{(1)}$ and $w_2^{(1)}$ by a linear combination of v_1, v_2 with coefficients in $W(k)((u))$, such that $w_i^{(1)} \equiv \pi_i^{-1} e_i \mod u$. A natural candidate for $w_1^{(1)}$ is

given by $(v[p\eta,1,2]v[\eta,1,1]-v[\eta,1,2]v[p\eta,1,1])^{-1}(v[p\eta,1,2]v_1-v[\eta,1,2]v_2)$. By the construction of $w_1^{(1)}$, we have

$$\begin{aligned} w_1^{(1)}-\pi_1^{-1}e_1 &= (v[p\eta,1,2]v[\eta,1,1]-v[\eta,1,2]v[p\eta,1,1])^{-1}\cdot \\ &\quad \sum_{s=1}^{2}\sum_{r=2}^{4}(v[p\eta,1,2]v[\eta,r,s]-v[\eta,1,2]v[p\eta,r,s])e_s \end{aligned}$$

It suffices to:

(8.4.2.a) Show $v[\eta,1,1]v[p\eta,1,2]-v[\eta,1,2]v[p\eta,1,1]$ is a unit in $W(k)((u))$ and estimate its order (in u);

(8.4.2.b) For $s=1,2$ and $r>1$, show $\mathrm{ord}_u(v[p\eta,1,2]v[\eta,r,s]-v[\eta,1,2]v[p\eta,r,s])$ is greater than $\mathrm{ord}_u(v[p\eta,1,2]v[\eta,1,1]-v[\eta,1,2]v[p\eta,1,1])$.

Write $\eta=p^{-2}(\alpha+\pi_0\beta)$ or $p^{-2}\pi_0(\alpha+\pi_0\beta)$ according to $\nu(\eta)=-4$ or -3, where $\alpha\in W(\mathbb{F}_{p^2})^\times$, $\beta\in W(\mathbb{F}_{p^2})$. By the definition of $v[\eta,r,s]$ and $v[p\eta,r,s]$,

$$\begin{aligned} & v[p\eta,1,2]v[\eta,1,1]-v[\eta,1,2]v[p\eta,1,1] \\ = \;& \epsilon^3(\alpha y_{-\nu(\eta)-1}+\beta y_{-\nu(\eta)-2})(\alpha^\sigma\lambda^{2+\nu(p\eta)}z_{-\nu(p\eta)-1}+\beta^\sigma\lambda^{3+\nu(p\eta)}z_{-\nu(p\eta)-2})- \\ & \epsilon^3(\alpha^\sigma\lambda^{2+\nu(\eta)}z_{-\nu(\eta)-1}+\beta^\sigma\lambda^{3+\nu(\eta)}z_{-\nu(\eta)-2})(\alpha y_{-\nu(p\eta)-1}+\beta y_{-\nu(p\eta)-2}) \\ = \;& \epsilon^3\alpha\alpha^\sigma\lambda^{2+\nu(\eta)}(y_{-\nu(\eta)-1}z_{-\nu(\eta)-3}-z_{-\nu(\eta)-1}y_{-\nu(\eta)-3})+\text{Higher order terms} \end{aligned}$$

By Proposition (8.3.3)(6) and Lemma 8.3.4, it is a unit with order equal to

$$d(p^{4m+1+\nu(\eta)}+p^{4m-1+\nu(\eta)})$$

Now for $s=1,2$ and $r\geq 2$,

$$\mathrm{ord}_u v[\eta,r,s]\geq dp^{4m-2+\nu(\eta)+r}\geq dp^{4m+\nu(\eta)}$$

and

$$\mathrm{ord}_u v[p\eta,r,s]\geq dp^{4m-2+\nu(p\eta)+r}\geq dp^{4m+2+\nu(\eta)}$$

Hence $\mathrm{ord}_u(v[p\eta,1,2]v[\eta,r,s]-v[\eta,1,2]v[p\eta,r,s])\geq d(p^{4m+1+\nu(\eta)}+p^{4m+\nu(\eta)})$.

Based on the estimates above, we deduce that $\mathrm{ord}_u(w_1^{(1)}-\pi_1^{-1}e_1)\geq d(p^{4m+\nu(\eta)}-p^{4m-1+\nu(\eta)})$. In particular we have found $w_1^{(1)}$ such that it reduces to $\pi_1^{-1}e_1$ modulo u. The desired $w_2^{(1)}$ can be constructed similarly. Thus the goal of (8.2.a) is achieved.

Example 8.4.3. Let $m\geq 3$, $\eta\in(p^{-3}\mathcal{O}_F\mathcal{O}_F)\backslash(p^{-2}\mathcal{O}_F\mathcal{O}_F)$, and $A=\langle\eta\rangle\cong\mathbb{Z}/p^3$. Take $A_1:=\langle p\eta\rangle\cong\mathbb{Z}/p^2$. By Example (8.4.2), we have constructed $w_s^{(1)}$ in $\mathfrak{N}_{A_1}\subset\mathfrak{N}_A$ such that $\mathrm{ord}_u(w_s^{(1)}-\pi_s^{-1}e_s)\geq d(p^{4m+\mu(p\eta)}-p^{4m-1+\mu(p\eta)})$. Define $w:=u^{-dp^{4m+\nu(\eta)}}(\eta\cdot v-\sum_{s=1}^{2}v[\eta,1,s]w_s^{(1)})$, then we have

$$w=\sum_{s=1}^{2}\sum_{r=2}^{6}u^{-dp^{4m+\nu(\eta)}}v[\eta,r,s]\pi_s^{-r}e_s-u^{-dp^{4m+\nu(\eta)}}\sum_{s=1}^{2}v[\eta,1,s](w_s^{(1)}-\pi_s^{-1}e_s)$$

The order of the second term is $\geq d(p^{4m+\nu(p\eta)}-p^{4m-1+\nu(p\eta)})-dp^{4m+\nu(\eta)}>0$. Note that $\mathrm{ord}_u v[\eta,r,s]$ is increasing in r and does not depend on s, so $u^{-dp^{4m+\nu(\eta)}}v[\eta,2,s]$ are units in $W(k)[[u]]$ and $\mathrm{ord}_u u^{-dp^{4m+\nu(\eta)}}v[\eta,r,s]>0$ when $r>2$. Thus we deduce $w\equiv\sum_{s=1}^{2}x_s\pi_s^{-2}e_s \mod u$, where $x_s\in W(k)^\times$. This achieves the goal of (8.2.b).

Example 8.4.4. Let $m\geq 1$, $\eta_1,\eta_2\in p^{-1}\mathcal{O}_F/\mathcal{O}_F$, and $A=\langle\eta_1\rangle\times\langle\eta_2\rangle\cong\mathbb{Z}/p\times\mathbb{Z}/p$. Let $\alpha_i\in W(\mathbb{F}_{p^2})^\times$ and $\beta_i\in W(\mathbb{F}_{p^2})$ be the unique elements such that $w_i=p^{-1}(\alpha_i+\pi_0\beta_i)$ or $p^{-1}\pi_0(\alpha_i+\pi_0\beta_i)$ depending on $\nu(\eta_i)=-2$ or -1. We may further assume that if $\nu(\eta_1)=\nu(\eta_2)$, then $\alpha_1 \mod p, \alpha_2 \mod p$ are $\mathbb{F}_p$-linearly independent. In fact, if otherwise, there exists $\gamma\in\mathbb{Z}_p$ such that $\alpha_2\equiv\gamma\alpha_1 \mod p$, then we can replace η_2 with $\eta_2-\gamma\eta_1$, to reduce to the situation when $\nu(\eta_1)\neq\nu(\eta_2)$. Without of loss of generality we assume $\nu(\eta_1)\leq\nu(\eta_2)$.

Define $w_1^{(1)} := (v[\eta_1,1,1]v[\eta_2,1,2] - v[\eta_2,1,1]v[\eta_1,1,2])^{-1}(v[\eta_2,1,2](\eta_1 \cdot v) - v[\eta_1,1,2](\eta_2 \cdot v))$. Then $w_1^{(1)} - \pi_1^{-1}e_1$ is equal to

$$(v[\eta_1,1,1]v[\eta_2,1,2]-v[\eta_2,1,1]v[\eta_1,1,2])^{-1}\sum_{s=1}^{2}(v[\eta_2,1,2]v[\eta_1,2,s]-v[\eta_1,1,2]v[\eta_2,2,s])$$

We claim $v[\eta_1,1,1]v[\eta_2,1,2] - v[\eta_2,1,1]v[\eta_1,1,2]$ is a unit in $W(k)((u))$, with order equal to $d(p^{4m-1+\nu(\eta_1)} + p^{4m-1+\nu(\eta_2)})$. To verify this, we divide the situation into the case when $\nu(\eta_1) < \nu(\eta_2)$ and the case when $\nu(\eta_1) = \nu(\eta_2)$.

When $\nu(\eta_1) < \nu(\eta_2)$, then $\nu(\eta_1) = -2$, $\nu(\eta_2) = -1$. So $v[\eta_1,1,1]v[\eta_2,1,2] - v[\eta_2,1,1]v[\eta_1,1,2] = \epsilon^2(\alpha_1 y_1 + \beta_1 y_0)\alpha_2^\sigma \lambda z_0 - \epsilon^2(\alpha_1^\sigma y_1 + \beta_1^\sigma \lambda y_0)\alpha_2 y_0 = \epsilon^2(\alpha_1\alpha_2^\sigma \lambda y_1 z_0 - \alpha_1^\sigma \alpha_2 y_0 z_1) + \text{Higher order terms}$. By Proposition 8.3.3 (7), we see the claim is true.

When $\nu(\eta_1) = \nu(\eta_2)$,

$$\begin{aligned}
& v[\eta_1,1,1]v[\eta_2,1,2] - v[\eta_2,1,1]v[\eta_1,1,2] \\
= \;& \epsilon^2(\alpha_1 y_{-\nu(\eta_1)-1} + \beta_1 y_{-\nu(\eta_1)-2})\alpha_2^\sigma z_{-\nu(\eta_2)-1} - \\
& \epsilon^2(\alpha_1^\sigma y_{-\nu(\eta_1)-1} + \beta_1^\sigma \lambda y_{-\nu(\eta_1)-2})\alpha_2 y_{-\nu(\eta_1)-1} \\
= \;& \epsilon^2(\alpha_1\alpha_2^\sigma - \alpha_1^\sigma\alpha_2) y_{-\nu(\eta_1)-1} z_{-\nu(\eta_1)-1} + \text{Higher order terms}
\end{aligned}$$

Since we have assumed $\alpha_1 \mod p, \alpha_2 \mod p$ are $\mathbb{F}_p$-linearly independent, $(\alpha_1\alpha_2^\sigma - \alpha_1^\sigma\alpha_2)$ is a unit in $W(\mathbb{F}_{p^2})$, and the claim follows.

So for $s = 1, 2$, we have

$$\begin{aligned}
& \mathrm{ord}_u(v[\eta_2,1,2]v[\eta_1,2,s] - v[\eta_1,1,2]v[\eta_2,2,s]) \\
& -\mathrm{ord}_u(v[\eta_1,1,1]v[\eta_2,1,2] - v[\eta_2,1,1]v[\eta_1,1,2]) \\
\geq \;& d(p^{4m+\nu(\eta_1)} + p^{4m-1+\nu(\eta_2)}) - d(p^{4m-1+\nu(\eta_1)} + p^{4m-1+\nu(\eta_2)}) \\
= \;& d(p^{4m+\nu(\eta_1)} - p^{4m-1+\nu(\eta_1)})
\end{aligned}$$

In particular, this implies $w_1^{(1)}$ reduces to $\pi_1^{-1}e_1$ modulo u. Similarly we can find $w_2^{(1)}$ that reduces to $\pi_2^{-1}e_1$ modulo u, and the goal of (8.2.a) is achieved.

8.5 Linear algebra lemmas

Now we summarize a linear algebra approach from the examples we computed above. For a square matrix C, we denote the entry on the i-th row, j-th column by $C[i,j]$, and its cofactor by $C_{i,j}$.

Lemma 8.5.1. *Suppose $A \subset p^{-m}\mathcal{O}_F/\mathcal{O}_F$, $v_1, v_2, \cdots, v_{2n}$ are elements in $\mathfrak{N}_A^0$, and for each $1 \leq i \leq 2n$ we have a presentation $v_i = \sum_{s=1}^{2}\sum_{r=1}^{2m} v_{i,r,s}\pi_s^{-r}e_s$, where $v_{i,r,s} \in W(k)((u))$. Define an $2n \times 2n$ matrix*

$$C := \begin{pmatrix} v_{1,n,1} & v_{2,n,1} & \cdots & v_{2n,n,1} \\ v_{1,n,2} & v_{2,n,2} & \cdots & v_{2n,n,2} \\ v_{1,n-1,1} & v_{2,n-1,1} & \cdots & v_{2n,n-1,1} \\ v_{1,n-1,1} & v_{2,n-1,2} & \cdots & v_{2n,n-1,2} \\ \vdots & & & \vdots \\ v_{1,1,1} & v_{2,1,1} & \cdots & v_{2n,1,1} \\ v_{1,1,2} & v_{2,1,2} & \cdots & v_{2n,1,2} \end{pmatrix}$$

Suppose $\det C \in W(k)((u))^\times$, and there exists a positive integer D such that

$$ord_u(\sum_{l=1}^{2n} v_{l,i,j}C_{s,l}) - ord_u \det C \geq D$$

for $i, s = 1, 2$, *and* $j \geq n+1$. *Define* $w_s^{(n)} := \sum_{l=1}^{2n} (\det C)^{-1} C_{s,l} v_l$ *for* $s = 1, 2$. *Then* $w_s^{(n)} \in \mathfrak{N}_A$ *and* $w_s^{(n)} \equiv \pi_s^{-n} e_s \mod ord_u \geq D$.

Proof. By the definition of C, one can check

$$w_s^{(n)} = \pi_s^{-n} e_s + \sum_{i=1}^{2} \sum_{j \geq n+1} \sum_{l=1}^{2n} (\det C)^{-1} C_{s,l} v_{l,i,j} \pi_i^{-j} e_i$$

then it follows from the assumption on the order of $(\det C)^{-1} \sum_{l=1}^{2n} C_{s,l} v_{l,i,j}$. □

To apply Lemma (8.5.1), the key step is to show $\det C$ is a unit in $W(k)((u))$, and estimate $\mathrm{ord}_u \det C$. With this aim, now we make some definitions for matrices of special types that will show up in our computations, and establish a few technical lemmas.

Let R be a commutative ring with 1, and $\mathrm{ord}_u : R^\times \to \mathbb{Z}$ be a discrete valuation on R; here we are not assuming that R is the valuation ring with respect to ord_u. Let k be a positive integer, and C be a $k \times k$ matrix with entries in R. We denote the set of permutations on $\{1, 2, \cdots, k\}$ by $\mathcal{P}_k$.

Definition 8.5.2. We say C is *dominated by the diagonals*, if for any permutation $\sigma \in \mathcal{P}_k$, $\sum_{j=1}^{k} \mathrm{ord}_u(C[\sigma(j), j]) \geq \sum_{j=1}^{k} \mathrm{ord}_u(C[j, j])$; if the inequality is strict, then we say C is *strictly dominated by the diagonals*. We say C is *faithfully dominated by the diagonals*, if C is dominated by the diagonals, and $\mathrm{ord}_u \det C = \sum_{j=1}^{k} \mathrm{ord}_u(C[j, j])$. We say C is *in pairwise order*, if for any pair of (i_1, j_1), (i_2, j_2) with $i_1 < i_2$, $j_1 < j_2$, $\mathrm{ord}_u C[i_1, j_1] + \mathrm{ord}_u C[i_2, j_2] \leq \mathrm{ord}_u C[i_1, j_2] + \mathrm{ord}_u C[i_2, j_1]$; if the inequality is strict, then we say C is *strictly in pairwise order*.

In general, let $J_1 \coprod J_2 \coprod \cdots \coprod J_t$ be a partition of $\{1, 2, \cdots, k\}$, we say C is *dominated by the diagonal blocks* $(J_1|J_2|\cdots|J_t)$, if for any permutation $\sigma \in \mathcal{P}_k$, there exists a permutation τ such that $\tau(J_i) = J_i$ for $i = 1, 2, \cdots, t$, and $\sum_{j=1}^{k} \mathrm{ord}_u(C[\sigma(j), j])$ is $\geq \sum_{j=1}^{k} \mathrm{ord}_u(C[\tau(j), j])$; if the inequality is strict, then we say C is *strictly dominated by the diagonal blocks* $(J_1|J_2|\cdots|J_t)$. We say C is *in pairwise order relative to partition* $(J_1|J_2|\cdots|J_t)$, if for any pair of (i_1, j_1), (i_2, j_2) such that $i_1, j_1 \in J_{r_1}$, $i_2, j_2 \in J_{r_2}$ with $r_1 < r_2$, we have $\mathrm{ord}_u C[i_1, j_1] + \mathrm{ord}_u C[i_2, j_2] \leq \mathrm{ord}_u C[i_1, j_2] + \mathrm{ord}_u C[i_2, j_1]$; if the inequality is strict, then we say C is *strictly in pairwise order relative to partition* $(J_1|J_2|\cdots|J_t)$.

The following lemma is straightforward by the formula

$$\det C = \sum_{\sigma \in \mathcal{P}_k} (-1)^{\mathrm{sgn}(\sigma)} \prod_{j=1}^{k} C[\sigma(j), j]$$

Lemma 8.5.3. *Notations as in Definition (8.5.2). Then:*

(a) If C is (strictly) in pairwise order, then C is (strictly) dominated by the diagonals.

(b) If C is strictly dominated by the diagonals, then C is faithfully dominated by the diagonals.

(c) If C is (strictly) in pairwise order relative to partition $(J_1|J_2|\cdots|J_t)$, then C is (strictly) dominated by the diagonal blocks $(J_1|J_2|\cdots|J_t)$.

(d) If C is strictly dominated by the diagonal blocks $(J_1|J_2|\cdots|J_t)$, and each block that consists of the rows and columns in J_i is faithfully dominated by the diagonals, then C is faithfully dominated by the diagonals.

8.6 The proof of Theorem (8.1.1) in the special case

Let A be a finite abelian p-group. Let $r(A)$ be the largest positive integer r such that $(\mathbb{Z}/p)^r$ can be embedded in A; this $r(A)$ is called the *p-rank* of the A. The p-rank of A is also the smallest integer k such that A can be generated by k elements. Suppose A is a subgroup of $p^{-m}\mathcal{O}_F/\mathcal{O}_F$, then we have $r(A) \leq r(p^{-m}\mathcal{O}_F/\mathcal{O}_F) = 4$. Let $\mathcal{G} := \mathcal{G}_A$ be the associated p^m-torsion finite locally free subgroup scheme of $\mathcal{X}_m$. If $r(A) = 4$, then $p^{-1}\mathcal{O}_F/\mathcal{O}_F \subset A$, hence $\mathcal{X}[p] \subset \mathcal{G}$. This implies the isogeny $\mathcal{X} \to \mathcal{X}/\mathcal{G}$ factors through $\mathcal{X} \xrightarrow{p} \mathcal{X}$, and the problem is reduced to another finitely locally free subgroup scheme with a smaller order. So we may assume $r(A) \leq 3$.

In this subsection we prove Theorem 8.1.1 in the case when $\mathcal{G} = \mathcal{G}_A$ such that $r(A) \leq 2$. Suppose $A = \langle\eta_1\rangle \times \langle\eta_2\rangle$, $\eta_i \in (p^{-m_i}\mathcal{O}_F/\mathcal{O}_F)\backslash(p^{-m_i+1}\mathcal{O}_F/\mathcal{O}_F)$ for $i = 1, 2$. Suppose $\#A = p^t$, then $m_1 + m_2 = t$. Without loss of generality we assume $\nu(\eta_1) \leq \nu(\eta_2)$. Let $\alpha_i \in W(\mathbb{F}_{p^2})^\times$ and $\beta_i \in W(\mathbb{F}_{p^2})$ be the elements such that $\eta_i = p^{-m_i}(\alpha_i + \pi_0\beta_i)$ or $p^{-m_i}\pi_0(\alpha_i + \pi_0\beta_i)$, depending on whether $\nu(\eta_i) = -2m_i$ or $-2m_i + 1$. Define the following integer associated to A:

$$L(A) := 4m - 2 + \nu(\eta_1) + \lceil\frac{t+1}{2}\rceil$$

Proposition 8.6.1. *Notations and assumptions as above. Then:*

(a) *If $t = 2n$, then for $s = 1, 2$ and $r = 1, 2, \cdots, n$, there exists $w_s^{(r)} \in \mathfrak{N}_A$ such that $ord_u(w_s^{(r)} - \pi_s^{-r}e_s) \geq d(p^{L(A)+1} - p^{L(A)})$.*

(b) *If* $t = 2n+1$, *then there exists* $w \in \mathfrak{N}_A$, *such that* $w \equiv \pi_1^{-(n+1)}\alpha_1 e_1 + (-1)^c \pi_2^{-(n+1)} \alpha_1^\sigma \lambda^{2m_1+\nu(\eta_1)} e_2 \mod ord_u \geq d(p^{L(A)+1} - p^{L(A)})$, *where* $c = [\frac{-\nu(\eta_1)-n}{2}]$.

Before proving Proposition (8.6.1), we show that it implies Theorem (8.1.1)(1) in the case when $\mathcal{G} = \mathcal{G}_A$ such that $r(A) \leq 2$, and also implies Theorem (8.1.1)(2). It suffices to show the goals (8.2) (a), (b), and (c) are achieved. (8.6.1)(a) obviously implies (8.2)(a). Recall that $\pi_1 = \pi$, $\pi_2 = \lambda^{-1}\pi$, so the element w in (8.6.1)(b) can be written as $w \equiv \alpha_1 \pi^{-(n+1)} e_1 + (-1)^c \lambda^{2m_1+\nu(\eta_1)+n+1} \alpha_1^\sigma \pi^{-(n+1)} e_2$. Let $x_1 := \alpha_1$, $x_2 := (-1)^c \lambda^{2m_1+\nu(\eta_1)+n+1} \alpha_1^\sigma$. Because -1 and $\overline{\lambda}^2 = \overline{\epsilon}^{p-1}$ are both in $(\mathbb{F}_{p^2}^\times)^{p-1}$, it is then clear that $\overline{x}_1/\overline{x}_2 \in (\mathbb{F}_{p^2}^\times)^{p-1}$ or $\overline{\lambda}(\mathbb{F}_{p^2}^\times)^{p-1}$. Thus (8.2) (b) is achieved. Concerning (8.2) (c), if we let $\eta_2 = 0$, $\eta_1 = p^{-2n-1}\alpha_1$ or $p^{-2n-1}\pi_0\alpha_1$ where n runs over non-negative integers and α_1 runs over $W(\mathbb{F}_{p^2})^\times$, then Proposition (8.6.1)(b) implies that for each $[c_1, c_2] \in \mathbb{P}^1(k)$ such that $\overline{c_1}/\overline{c_2} \in (\mathbb{F}_{p^2}^\times)^{p-1}$ or $\overline{\lambda}(\mathbb{F}_{p^2}^\times)^{p-1}$, there exists a finite locally free subgroup scheme $\mathcal{G}$ satisfying $\delta_n(\mathcal{G}_k) = [\overline{c_1}/\overline{c_2}]$ in $\mathfrak{L}$. Therefore Theorem (8.1.1)(2) is proved once we prove Proposition (8.6.1).

The plan to prove Proposition 8.6.1 is as follows: we apply Lemma (8.5.1) to prove (a). For (b), we "knock out" the unwanted entries in the presentation of $\eta_1 \cdot v$ by using the constructed lifts of $\pi_s^{-r} e_s$, where $s = 1, 2$ and $r = 1, 2, \cdots, n$.

First suppose $t = 2n$. Define an order $\prec$ on $\{p^j \eta_i \cdot v | i = 1, 2, j = 0, 1, \cdots, m_i - 1\}$ such that $p^j \eta_i \cdot v \prec p^{j'} \eta_{i'} \cdot v$ when: (a) $\nu(p^j \eta_i) < \nu(p^{j'} \eta_{i'})$; or (b) $\nu(p^j \eta_i) = \nu(p^{j'} \eta_{i'})$ and $i < i'$. Let $v_l = p^{j_l} \eta_{i_l} \cdot v$ be the l-th element in the set under this order. Then

define a matrix (cf. Lemma 8.5.1)

$$C := \begin{pmatrix} v[p^{j_1}\eta_{i_1}, n, 1] & v[p^{j_2}\eta_{i_2}, n, 1] & \cdots & v[p^{j_{2n}}\eta_{i_{2n}}, n, 1] \\ v[p^{j_1}\eta_{i_1}, n, 2] & v[p^{j_2}\eta_{i_2}, n, 2] & \cdots & v[p^{j_{2n}}\eta_{i_{2n}}, n, 2] \\ v[p^{j_1}\eta_{i_1}, n-1, 1] & v[p^{j_2}\eta_{i_2}, n-1, 1] & \cdots & v[p^{j_{2n}}\eta_{i_{2n}}, n-1, 1] \\ v[p^{j_1}\eta_{i_1}, n-1, 2] & v[p^{j_2}\eta_{i_2}, n-1, 2] & \cdots & v[p^{j_{2n}}\eta_{i_{2n}}, n-1, 2] \\ \vdots & & & \vdots \\ v[p^{j_1}\eta_{i_1}, 1, 1] & v[p^{j_2}\eta_{i_2}, 1, 1] & \cdots & v[p^{j_{2n}}\eta_{i_{2n}}, 1, 1] \\ v[p^{j_1}\eta_{i_1}, 1, 2] & v[p^{j_2}\eta_{i_2}, 1, 2] & \cdots & v[p^{j_{2n}}\eta_{i_{2n}}, 1, 2] \end{pmatrix}$$

If we delete the first row of C and add the row of

$$(v[p^{j_1}\eta_{i_1}, r, s], v[p^{j_2}\eta_{i_2}, r, s], \cdots, v[p^{j_{2n}}\eta_{i_{2n}}, r, s])$$

on top of the remaining $(2n-1) \times 2n$ matrix for $s = 1, 2$ and $r \geq n+1$, we denote the new $2n \times 2n$ matrix by $C(1, r, s)$. Similarly, we can delete the second row of C and add $(v[p^{j_1}\eta_{i_1}, r, s], v[p^{j_2}\eta_{i_2}, r, s], \cdots, v[p^{j_{2n}}\eta_{i_{2n}}, r, s])$ on the top to get a new $2n \times 2n$ matrix; we denote it by $C(2, r, s)$.

Proposition 8.6.2. *Notations as above, then the $2n \times 2n$ matrices $C, C(1, r, s)$, and $C(2, r, s)$ are all faithfully dominated by the diagonals, for $s = 1, 2$, $r \geq n+1$. In particular, their determinants are all units in $W(k)((u))$.*

Proof. Define a partition of $\{1, 2, \cdots, 2n\} = J_1 \coprod J_2 \coprod \cdots \coprod J_n$ where $J_i := \{2i - 1, 2i\}$. By the definition of the matrices and the estimates on the orders of their entries by Proposition 8.3.3 (5), one can check all the matrices considered in the

Proposition are strictly dominated by the diagonal blocks $(J_1|J_2|\cdots|J_n)$. Each 2×2 diagonal block of C has the form

$$\begin{pmatrix} v[p^j\eta_1, r, 1] & v[p^{j+1}\eta_1, r, 1] \\ v[p^j\eta_1, r, 2] & v[p^{j+1}\eta_1, r, 2] \end{pmatrix}, \begin{pmatrix} v[p^j\eta_1, r, 1] & v[p^j\eta_2, r, 1] \\ v[p^j\eta_1, r, 2] & v[p^j\eta_2, r, 2] \end{pmatrix}$$

or

$$\begin{pmatrix} v[p^j\eta_2, r, 1] & v[p^j\eta_1, r, 1] \\ v[p^j\eta_2, r, 2] & v[p^j\eta_1, r, 2] \end{pmatrix}$$

By computations similar to those in Example 8.4.2 and Example 8.4.4, it is straightforward to check that these blocks are all faithfully dominated by the diagonals. Therefore by Lemma 8.5.3 (d), the matrix C is faithfully dominated by the diagonals. For $C(k, r, s)$ where $k = 1, 2$, $s = 1, 2$, and $r \geq n + 1$, all the diagonal blocks are the same as those of C except for the first 2×2 block on the upper left corner, and a direct examination of that block will prove they are faithfully dominated by the diagonals, too.

For the last statement, note that the matrices are strictly dominated by their diagonal blocks $(J_1|J_2|\cdots|J_n)$, and the determinants of all the blocks are units in $W(k)((u))$, by Lemma 8.3.4 we deduce that the determinants of the $2n\times 2n$ matrices $C, C(1, r, s), C(2, r, s)$ are all units in $W(k)((u))$. □

Now we are ready to prove Proposition 8.6.1.

Proof of Proposition 8.6.1:

(a) In this case $m_1 + m_2 = 2n$. Prove by induction on n. Suppose we have proved for all the subgroups $A \subset p^{-m}\mathcal{O}_F/\mathcal{O}_F$ with order equal to $p^{2n'}$ and $n' < n$.

Let $A_1 := \langle p\eta_1 \rangle \times \langle p\eta_2 \rangle$ if $m_2 > 0$, and $\langle p^2\eta_1 \rangle$ if $m_2 = 0$. Then $\#A_1 = p^{2(n-1)}$ and $L(A_1) > L(A)$. By the induction hypothesis we have already produced $w_s^{(r)}$ for $s = 1, 2$ and $r = 1, 2, \cdots, n-1$. Now it suffices to produce $w_s^{(n)}$. With $v_l = p^{j_l}\eta_{i_l} \cdot v$ for $l = 1, 2, \cdots, 2n$ and matrix C defined before Proposition (8.6.2), we have shown $\det C \in W(k)((u))^\times$, so to apply Lemma (8.5.1) it remains to prove $\mathrm{ord}_u(\sum_{l=1}^{2n} v[p^{j_l}\eta_{i_l}, r, s]C_{k,l}) > \mathrm{ord}_u \det C$ for $k, s = 1, 2$ and $r \geq n+1$. But $\sum_{l=1}^{2n} v[p^{j_l}\eta_{i_l}, r, s]C_{k,l}$ is equal to $\det C(k, r, s)$, and by Proposition (8.6.2) $\mathrm{ord}_u \det C$ and $\mathrm{ord}_u \det C(k, r, s)$ are equal to the sum of the orders of their diagonal entries, respectively. By their definition one can check $\mathrm{ord}_u \det C(k, r, s) - \mathrm{ord}_u \det C \geq d(p^{4m-2+\nu(\eta_s)+r} - p^{4m-2+\nu(\eta_1)+n}) \geq d(p^{4m-1+\nu(\eta_1)+n} - p^{4m-2+\nu(\eta_1)+n}) = d(p^{L(A)+1} - p^{L(A)})$. By Lemma (8.6.2), we deduce the existence of $w_s^{(n)}$ in $\mathfrak{N}_A$ such that $\mathrm{ord}_u(w_s^{(n)} - \pi_s^{-n}e_s) \geq d(p^{L(A)+1} - p^{L(A)})$.

(b) In this case $m_1 + m_2 = 2n+1$. By our assumption $\nu(\eta_1) \leq \nu(\eta_2)$, so $m_1 > m_2$. Let $A_1 := \langle p\eta_1 \rangle \times \langle \eta_2 \rangle$, then $\#A = p^{2n}$, hence by (a) we can produce $w_s^{(r)} \in \mathfrak{N}_{A_1} \subset \mathfrak{N}_A$ for $s = 1, 2$ and $r = 1, 2, \cdots, n$, such that $w_s^{(r)} \equiv \pi_s^{-r}e_s \mod \mathrm{ord}_u \geq d(p^{L(A_1)+1} - p^{L(A_1)})$. Define $w := u^{-dp^{L(A)}}(\eta_1 \cdot v - \sum_{s=1}^{2}\sum_{r=1}^{n} v[\eta_1, r, s]w_s^{(r)})$, then we have $w = \sum_{s=1}^{2}\sum_{r=n+1}^{2m_1} u^{-dp^{L(A)}}v[\eta_1, r, s]\pi_s^{-r}e_s - \sum_{s=1}^{2}\sum_{r=1}^{n} u^{-dp^{L(A)}}v[\eta_1, r, s](w_s^{(r)} - \pi_s^{-r}e_s)$. The order of the second term is $\geq d(p^{L(A_1)+1} - p^{L(A_1)} - p^{L(A)}) \geq d(p^{L(A)+1} - p^{L(A)})$ because $L(A_1) \geq L(A) + 1$. In the first term, note that $\mathrm{ord}_u v[\eta_1, r, s] \geq dp^{L(A)+1}$ when $r \geq n+2$, and $v[\eta_1, n+1, 1] \equiv \alpha_1 y_{-\nu(\eta_1)-n-1} \mod \mathrm{ord}_u \geq dp^{L(A)+1}$, $v[\eta_1, n+1, 2] \equiv \alpha_1^\sigma \lambda^{2m_1+\nu(\eta_1)} z_{-\nu(\eta_1)-n-1} \mod \mathrm{ord}_u \geq dp^{L(A)+1}$. Therefore the proposition follows

from Proposition (8.3.3)(4). $\square$

Therefore to complete the proof of Theorem 8.1.1(1), the remaining situation is when $r(A) = 3$. In that case, we will meet difficulties if we still try to apply Lemma (8.5.1) directly, since the crucial proposition (8.6.2) may no longer hold. This phenomenon is reflected by the following example.

Example 8.6.3. Let $m \geq 2$, take $\alpha \in W(\mathbb{F}_{p^2})^\times \backslash \mathbb{Z}_p^\times$. Let $\eta_1 = p^{-2}$, $\eta_2 = p^{-2}\alpha$, and $\eta_3 = p^{-2}\pi$, and take $A = \langle \eta_1 \rangle \times \langle \eta_2 \rangle \times \langle \eta_3 \rangle$. The presentations of $\eta_i \cdot v$ are: $\eta_1 \cdot v = \sum_{r=1}^{4} y_{4-r}\pi_1^{-r}e_1 + \sum_{r=1}^{4} z_{4-r}\pi_2^{-r}e_2$, $\eta_2 \cdot v = \sum_{r=1}^{4} \alpha y_{4-r}\pi_1^{-r}e_1 + \sum_{r=1}^{4} \alpha^\sigma z_{4-r}\pi_2^{-r}e_2$, and $\eta_3 \cdot v = \sum_{r=1}^{3} y_{3-r}\pi_1^{-r}e_1 + \sum_{r=1}^{3} \lambda z_{3-r}\pi_2^{-r}e_2$. If we follow the linear algebra approach in (8.5) and form the 6×6 matrix:

$$C = \begin{pmatrix} y_1 & \alpha y_1 & y_0 & & & \\ z_1 & \alpha^\sigma z_1 & \lambda z_0 & & & \\ y_2 & \alpha y_2 & y_1 & y_0 & \alpha y_0 & \\ z_2 & \alpha^\sigma z_2 & \lambda z_1 & z_0 & \alpha^\sigma z_0 & \\ y_3 & \alpha y_3 & y_2 & y_1 & \alpha y_1 & y_0 \\ z_3 & \alpha^\sigma z_3 & \lambda z_2 & z_1 & \alpha^\sigma z_1 & \lambda z_0 \end{pmatrix}$$

One can check that

$$\det C \equiv -\lambda(\alpha - \alpha^\sigma)^2 y_1 z_1 (y_1^2 z_0^2 - z_1^2 y_0^2) \mod \mathrm{ord}_u > d(2p^{4m-2} + 4p^{4m-3})$$

However, $y_1^2 z_0^2 - z_1^2 y_0^2 = (b_1 - c_1)^2 b_0^2 - (b_1 + c_1)^2 b_0^2 = -4b_1 c_1 b_0^2$ has order equal to $d(3p^{4m-2} + p^{4m-4})$, hence $\mathrm{ord}_u(y_1 z_1 (y_1^2 z_0^2 - z_1^2 y_0^2)) = d(3p^{4m-2} + 2p^{4m-3} + p^{4m-4}) >$

$d(2p^{4m-2}+4p^{4m-3})$. So $\mathrm{ord}_u \det C > d(2p^{4m-2}+4p^{4m-3}) = \sum_{j=1}^{6} \mathrm{ord}_u C[j,j]$, in particular the matrix C is *not* faithfully dominated by the diagonals.

However, a look into the Serre dual of $\mathcal{X}_m$ will come to rescue for this example. Recall that $\tau^2 \in \mathrm{Gal}(F/\mathbb{Q}_p)$ is the involution on F, and the p-adic CM type Φ satisfies $\Phi \coprod \Phi \circ \tau^2 = \mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$. Let $\rho : \mathcal{O}_F \to End(\mathcal{X}_m)$ be the $\mathcal{O}_F$-structure on $\mathcal{X}_m$, if we define the $\mathcal{O}_F$-linear structure $\rho^* : \mathcal{O}_F \to End(\mathcal{X}_m^\vee)$ on the Serre dual $\mathcal{X}_m^\vee$ by $\rho^*(x) = \rho(\iota(x))^\vee$, then $\mathcal{X}_m$ and $\mathcal{X}_m^\vee$ are both $\mathcal{O}_F$-linear with the same p-adic CM type. Since the $\mathcal{O}_F$-isomorphism class of $\mathcal{O}_F$-linear CM p-divisible groups over R is uniquely determined by the p-adic CM type (see 3.1), we know $\mathcal{X}_m$ and $\mathcal{X}_m^\vee$ are $\mathcal{O}_F$-linearly isomorphic.

For a finite locally free p^m-torsion subgroup scheme $\mathcal{G}$ of $\mathcal{X}_m$, denote the Cartier dual $(\mathcal{X}_m[p^m]/\mathcal{G})^\vee$ by $\mathcal{G}^{\perp;m}$; it is a finite locally free p^m-subgroup scheme of $\mathcal{X}_m^\vee$. In our example 8.6.3, take $m = 2$, let $\mathcal{G} = \mathcal{G}_A$ be the finite locally free p^2-torsion subgroup scheme associated to A, then one can check $\mathcal{G}^{\perp;2}$ is a cyclic group of order p^2; in particular, it is associated with a subgroup A' with p-rank 1. Hence we can apply Theorem 8.1.1 to $\mathcal{G}^{\perp;2}$ in $\mathcal{X}^\vee$, and deduce that $\mathcal{G}_k^{\perp;2}$ is not $\mathcal{O}_F$-stable. That implies $\mathcal{G}_k$ is not $\mathcal{O}_F$-stable, too. Thus, we can take a detour via the Serre dual $\mathcal{X}^\vee$ and reduce to the solved case. To prove Theorem 8.1.1 in the general case when $\mathcal{G} = \mathcal{G}_A$ where the p-rank of A is equal to 3, we need more explicit information on $\mathcal{G}^{\perp;m}$. This will constitute the next subsection.

8.7 The Serre dual

Recall from (8.2) that the Kisin module $\mathfrak{M}_m$ attached to $\mathcal{X}_m$ is $\cong W(k)[[u]][\pi]/(\pi^2-\epsilon p)e_1 \oplus W(k)[[u]][\pi]/(\pi^2-\epsilon^\sigma p)e_2$, and $\phi_{\mathfrak{M}_m}(e_1) = \tau_2(\overline{h_{2m}}(u))e_2, \phi_{\mathfrak{M}_m}(e_2) = \tau_1(\overline{h_{2m}}(u))e_1$, where τ_1 (resp. τ_2) is the $W(k)[[u]]$-isomorphism from $F\cdot B(k)[[u]] = B(k)[\pi_0]/(\pi_0^2-\epsilon p)[[u]]$ to $B(k)[\pi]/(\pi^2-\epsilon p)[[u]]$ (resp. $B(k)[\pi]/(\pi^2-\epsilon^\sigma p)[[u]]$) by sending π_0 to π (resp. $\lambda^{-1}\pi$). Let $g_1(u), g_2(u)$ be the polynomial in $W(k)[u]$ such that $h_{2m}(u) = g_1(u) + \pi_0 g_2(u)$. Then in matrix form we can write

$$\phi_{\mathfrak{M}_m}(e_1, \pi e_1, e_2, \pi e_2) = (e_1, \pi e_1, e_2, \pi e_2)\cdot \begin{pmatrix} & & g_1(u) & -\epsilon p g_2(u) \\ & & -g_2(u) & g_1(u) \\ g_1(u) & -\epsilon^\sigma p\lambda^{-1} g_2(u) & & \\ -\lambda^{-1}g_2(u) & g_1(u) & & \end{pmatrix}$$

The Kisin module attached to $\mathcal{X}^\vee$ is $\mathfrak{M}_m^\vee = Hom_{W(k)[[u]]}(\mathfrak{M}_m, W(k)[[u]])$. If we denote the dual basis of $\{e_1, \pi e_1, e_2, \pi e_2\}$ by $\{e_1^\vee, (\pi e_1)^\vee, e_2^\vee, (\pi e_2)^\vee\}$, then

$$\phi_{\mathfrak{M}_m^\vee}(e_1^\vee, (\pi e_1)^\vee, e_2^\vee, (\pi e_2)^\vee)$$

is given by

$$(e_1^\vee, (\pi e_1)^\vee, e_2^\vee, (\pi e_2)^\vee)\cdot \frac{1}{-\epsilon}\begin{pmatrix} & & g_1(u) & g_2(u) \\ & & \epsilon p g_2(u) & g_1(u) \\ g_1(u) & \lambda^{-1} g_2(u) & & \\ \epsilon^\sigma p\lambda^{-1} g_2(u) & g_1(u) & & \end{pmatrix}$$

Here recall that $-\epsilon p$ is the constant term of the Eisenstein polynomial $E_m(u)$. Take $\mu \in W(k)^\times$ such that $\mu^{\sigma-1} = -\epsilon^{-1}$. Define

$$\widehat{e_1} := \mu(\pi e_1)^\vee, \pi\widehat{e_1} := -\mu e_1^\vee, \widehat{e_2} := \mu(\pi e_2)^\vee, \pi\widehat{e_2} := -\mu e_2^\vee$$

then $\mathfrak{M}^\vee = W(k)[[u]][\pi]/(\pi^2 - \epsilon p)\widehat{e_1} \oplus W(k)[[u]][\pi]/(\pi^2 - \epsilon^\sigma p)\widehat{e_2}$, with $\phi_{\mathfrak{M}^\vee}\widehat{e_1} = \tau_2(\overline{h_{2m}}(u))\widehat{e_2}, \phi_{\mathfrak{M}^\vee}\widehat{e_2} = \tau_1(\overline{h_{2m}}(u))\widehat{e_1}$. If we twist the natural $\mathcal{O}_F$-structure on $\mathfrak{M}_m^\vee$ by ι, i.e., define $a \cdot e_1 = ae_1$, $a \cdot e_2 = a^\sigma e_2$ for $a \in W(\mathbb{F}_{p^2})$, and $\pi_0 \cdot e_i = -\pi e_i$ for $i = 1, 2$, then the mapping that sends e_i to $\widehat{e_i}$ is an $\mathcal{O}_F$-linear isomorphism of Kisin modules from $\mathfrak{M}_m$ to $\mathfrak{M}_m^\vee$. The natural $W(k)[[u]]$-bilinear pairing $\langle , \rangle : \mathfrak{M}_m \times \mathfrak{M}_m^\vee \to W(k)[[u]]$ is a perfect pairing that is compatible with the $\mathcal{O}_F$-structures, i.e., $\langle x \cdot v, w\rangle = \langle v, x \cdot w\rangle$ for $x \in \mathcal{O}_F$, $v \in \mathfrak{M}_m$, and $w \in \mathfrak{M}_m^\vee$.

The pairing $\langle , \rangle : \mathfrak{M}_m \times \mathfrak{M}_m^\vee \to W(k)[[u]]$ naturally extends to $(\mathbb{Q} \otimes_{\mathbb{Z}} \mathfrak{M}_m) \times (\mathbb{Q} \otimes_{\mathbb{Z}} \mathfrak{M}_m) \to B(k)[[u]]$. For any positive integer n, it induces a pairing $\langle , \rangle_n : p^{-n}\mathfrak{M}_m/\mathfrak{M}_m \times p^{-n}\mathfrak{M}_m^\vee/\mathfrak{M}_m^\vee \to p^{-n}W(k)[[u]]/W(k)[[u]]$, by defining $\langle v, w\rangle_n := p^n\langle v, w\rangle$. If $\mathfrak{N}$ is the finite Kisin module attached to a finite locally free p^n-torsion subgroup scheme $\mathcal{G}$ of $\mathcal{X}$, then its orthogonal complement $\mathfrak{N}^{\perp;n}$ is the finite Kisin module attached to $\mathcal{G}^{\perp;n}$ (see the end of Example (8.6.3) for the definition of $\mathcal{G}^{\perp;n}$). The following lemma allows us to extract the information of $\mathfrak{N}^{\perp;n}$ from $\mathfrak{N}$, and vice versa.

Lemma 8.7.1. *Let D be a positive integer, and l be an integer between 1 and $2n$. Assumptions and notations on $\mathfrak{N}$ and $\mathfrak{N}^{\perp;n}$ are as above.*

(a) If $\mathfrak{N} \equiv \pi^{-l}\mathfrak{M}_m/\mathfrak{M}_m \mod ord_u \geq D$, *then*

$$\mathfrak{N}^{\perp;n} \equiv \pi^{-(2n-l)}\mathfrak{M}_m^\vee/\mathfrak{M}_m^\vee \mod ord_u \geq D$$

and vice versa.

(b) If $\mathfrak{N} \equiv \pi^{-l}\mathfrak{M}_m/\mathfrak{M}_m + W(k)[[u]] \cdot \sum_{i=1}^{2} \mu_i \pi_i^{-(l+1)} e_i \mod ord_u \geq D$ *with* $\mu_i \in W(k)[[u]]^\times$, *then* $\mathfrak{N}^{\perp;n} \equiv \pi^{-(2n-1-l)}\mathfrak{M}_m^\vee/\mathfrak{M}_m^\vee + \sum_{i=1}^{2} \widehat{\mu}_i \pi_i^{-(2n-l)} \widehat{e_i} \mod ord_u \geq D$, *where* $\widehat{\mu}_i \in W(k)[[u]]^\times$ *satisfy* $\lambda\mu_1\widehat{\mu}_1 + \mu_2\widehat{\mu}_2 \equiv 0 \mod u$; *and vice versa.*

Proof. First look at (a). Let M_m be the Dieudonné module attached to $X = (\mathcal{X}_m)_k$. The Dieudonné module attached to $\mathcal{G}_k$ is $\pi^{-l}M_m/M_m$, so the Dieudonné module associated to $\mathcal{G}_k^{\perp;n}$ is the orthogonal complement of $\pi^{-l}M_m/M_m$ under the induced pairing $p^{-n}M_m/M_m \times p^{-n}M_m^\vee/M_m^\vee \to p^{-n}W(k)/W(k)$, which is easily seen to be $\pi^{-(2n-l)}M_m^\vee/M_m^\vee$. Therefore for $\pi_i^{-j}\widehat{e_i}$ with $i = 1, 2$ and $j = 1, 2, \cdots, 2n-l$, there exist their lifts in $\mathfrak{N}^{\perp;n}$ in the forms of $v_{i,j} = \pi_i^{-j}\widehat{e_i} + \sum_{s=1}^{2} \sum_{r=2n-l+1}^{2n} h_{i,j,s,r}\pi_s^{-r}\widehat{e_s}$, where $h_{i,j,s,r} \in uW(k)[[u]]$. Because they are orthogonal to $\mathfrak{N}$, for each $i' = 1, 2$ and $j' = 1, 2, \cdots, l$, the pairing $\langle \pi_{i'}^{-j'} e_{i'}, v_{i,j} \rangle_n \equiv 0 \mod \mathrm{ord}_u \geq D$. Take $j' = 1$, this implies $\mathrm{ord}_u h_{i,j,s,2n} \geq D$. Take $j' = 2, 3, \cdots, l$ inductively, we deduce that $\mathrm{ord}_u h_{i,j,s,r} \geq D$ for all i, j, s, r. This proves (a). (b) can be proved in the same way, only to notice that under our definitions of $\widehat{e_1}$ and $\widehat{e_2}$, we have $\langle \pi_1^{-(l+1)} e_1, \pi_1^{-(2n-l)}\widehat{e_1} \rangle = \lambda \langle \pi_2^{-(l+1)} e_2, \pi_2^{-(2n-l)}\widehat{e_2} \rangle \neq 0$. □

Proposition (8.7.1) has the following immediate corollary:

Corollary 8.7.2. *If $X[\pi^i]$ is contained in $\mathcal{G}_k$ with index p, then $X[\pi^{2n-1-i}]$ is contained in $\mathcal{G}_k^{\perp;n}$ with index p, and vice versa. If that is the case, let $\delta_i(\mathcal{G}_k)$ and $\delta_{2n-1-i}(\mathcal{G}_k^{\perp;n})$ be the classes of $\mathcal{G}_k$ and $\mathcal{G}_k^{\perp;n}$ in $\mathfrak{L}$, then $\delta_i(\mathcal{G}_k) = \overline{\lambda}\delta_{2n-1-i}(\mathcal{G}_k^{\perp;n})$. In particular, $\delta_i(\mathcal{G}_k) = [1]$ or $[\overline{\lambda}]$ if and only if $\delta_{2n-1-i}(\mathcal{G}_k^{\perp;n}) = [1]$ or $[\overline{\lambda}]$.* □

If we define

$$\hat{v} := \tau_2(h^{(2m-1)}(u))^{\phi}\tau_1(h^{(2m-1)}(u))\widehat{e_1} + \tau_1(h^{(2m-1)}(u))^{\phi}\tau_2(h^{(2m-1)}(u))\widehat{e_2}$$

then all the solutions $x \in p^{-m}\mathfrak{M}_m^{\vee}/\mathfrak{M}_m^{\vee}$ to $\phi_{\mathfrak{M}_m^{\vee}}(x) = \frac{1}{-\epsilon}E_m(u)x$ have the form $\eta \cdot \hat{v}$, $\eta \in p^{-m}\mathcal{O}_F/\mathcal{O}_F$. For any subgroup A of $p^{-m}\mathcal{O}_F/\mathcal{O}_F$, define $\widehat{\mathfrak{N}_A}^0 := W(k)\{\eta \cdot \hat{v} | \eta \in A\}$, and $\widehat{\mathfrak{N}_A} := \widehat{\mathfrak{N}_A}^0 \cap p^{-m}\mathfrak{M}_m^{\vee}/\mathfrak{M}_m^{\vee}$. Let $\widehat{\mathcal{G}_A}$ be the associated finite locally free subgroup scheme of $\mathcal{X}_m^{\vee}$, then they enumerate all p^m-torsion finite locally free subgroup schemes when A runs over subgroups of $p^{-m}\mathcal{O}_F/\mathcal{O}_F$. Now supppose $n \leq m$, A is a subgroup of $p^{-n}\mathcal{O}_F/\mathcal{O}_F$, and $\mathfrak{N}_A, \mathcal{G}_A$ are the corresponding p^n-torsion finite Kisin modules and finite locally free subgroup schemes of $\mathcal{X}_m$. The definition below provides a direct and concrete way to write down the subgroup $p^{-n}\mathcal{O}_F/\mathcal{O}_F$ attached to $\mathfrak{N}^{\perp;n}$ and $\mathcal{G}^{\perp;n}$.

Definition 8.7.3. Define a symmetric $\mathbb{Q}_p$-pairing on F as follows:

$$\langle a + b\pi, c + d\pi \rangle := (ad + bc) + (ad + bc)^{\sigma}, \qquad a, b, c, d \in B(\mathbb{F}_{p^2})$$

It induces a symmetric pairing $p^{-n}\mathcal{O}_F/\mathcal{O}_F \times p^{-n}\mathcal{O}_F/\mathcal{O}_F \to p^{-n}\mathbb{Z}/\mathbb{Z}$:

$$\langle a + b\pi, c + d\pi \rangle_n := p^n((ad + bc) + (ad + bc)^{\sigma})$$

For any subgroup $A \subset p^{-n}\mathcal{O}_F/\mathcal{O}_F$, let $A^{\perp;n}$ be its orthogonal complement.

Under the definitions above, when $n \leq m$ one can check $(\mathfrak{N}_A)^{\perp;n} = \widehat{\mathfrak{N}_{A^{\perp;n}}}$, and hence $\mathcal{G}_A^{\perp;n} = \widehat{\mathcal{G}_{A^{\perp;n}}}$. Moreover, the following proposition illustrates the relation between the structure of A and $A^{\perp;n}$; we leave the details to readers.

Definition 8.7.4. Suppose $A \subset p^{-n}\mathcal{O}_F/\mathcal{O}_F$ is a subgroup. for all positive integers i, denote the kernel of $A \xrightarrow{\pi^i} A$ by $A[\pi^i]$. For $i = 1, 2, \cdots, 2n$, define

$$R_i(A) := \dim_{\mathbb{F}_p} A[\pi^i]/A[\pi^{i-1}]$$

Since $\dim_{\mathbb{F}_p} \pi_0^{-i}\mathcal{O}_F/\pi_0^{-(i-1)}\mathcal{O}_F = 2$, we know $R_i(A)$ can only take value $0, 1$, or 2.

Proposition 8.7.5. *Suppose A is a subgroup of $p^{-n}\mathcal{O}_F/\mathcal{O}_F$. Then we have:*

(a) *If $A \cong \prod_{i=1}^{4} \mathbb{Z}/p^{n_i}$ with $0 \leq n_i \leq n$, then $A^{\perp;n} \cong \prod_{i=1}^{4} \mathbb{Z}/p^{n-n_i}$.*

(b) *$R_i(A^{\perp;n}) + R_{2n+1-i}(A) = 2$ for all $i = 1, 2, \cdots, 2n$.* □

Now we can prove Theorem 8.1.1 for $\mathcal{G}_A$ in the case when $A \cong \mathbb{Z}/p^i \times \mathbb{Z}/p^i \times \mathbb{Z}/p^j \subset p^{-m}\mathcal{O}_F/\mathcal{O}_F$, where $i \geq j$. In fact, by Proposition 8.7.5 we know $A^{\perp;i} \cong \mathbb{Z}/p^i \times \mathbb{Z}/p^{i-j}$ has p-rank at most 2, hence Theorem (8.1.1) for $\mathcal{G}_A$ follows from Proposition (8.6.1) and Corollary (8.7.2). Explore this idea further we will be able to prove Theorem 8.1.1 for $\mathcal{G}_A$ in the general case when the p-rank of A is equal to 3 in the next subsection.

8.8 The proof of Theorem (8.1.1) in the general case

Suppose $\mathcal{G} = \mathcal{G}_A$ is a finite locally free p^m-torsion subgroup scheme of $\mathcal{X}$, and $A = \prod_{i=1}^{3} \langle \eta_i \rangle$, where $\eta_i \in (p^{-m_i}\mathcal{O}_F/\mathcal{O}_F)\backslash(p^{-(m_i-1)}\mathcal{O}_F/\mathcal{O}_F)$ with $m_1 \geq m_2 \geq m_3 \geq 1$. Suppose $\#A = p^t$, so $t = m_1 + m_2 + m_3$. Let $\alpha_i \in W(\mathbb{F}_{p^2})^\times$ and $\beta_i \in W(\mathbb{F}_{p^2})$ be the elements such that $\eta_i = p^{-m_i}(\alpha_i + \pi_0\beta_i)$ or $p^{-m_i}\pi_0(\alpha_i + \pi_0\beta_i)$, depending on whether $\nu(\eta_i) = -2m_i$ or $-2m_i + 1$.

By the argument at the end of the previous subsection, we may assume $m_1 > m_2$. We may also assume that $\mathcal{X}[\pi] \nsubseteq \mathcal{G}$, otherwise the isogeny $\mathcal{X} \to \mathcal{X}/\mathcal{G}$ factors through $\mathcal{X} \xrightarrow{\pi} \mathcal{X}$ and we may reduce to a subgroup scheme with a smaller order. This assumption translates into $R_1(A) < 2$. Because we have assumed the p-rank of A is 3 and the p-rank is equal to $R_1(A) + R_2(A)$, we deduce that $R_1(A) = 1$ and $R_2(A) = 2$.

Definition 8.8.1. Assumptions on A are as above. Define

$$L(A) := 4m - 2 + \nu(\eta_1) + \lceil \frac{t+1}{2} \rceil$$

and

$$D(A) := \begin{cases} d(p^{L(A)} - p^{L(A)-1}) & \text{if } \nu(\eta_1) = -2m_1 + 1 \text{ and } m_1 = m_2 + m_3 \\ d(p^{L(A)+1} - p^{L(A)}) & \text{otherwise} \end{cases}$$

Proposition 8.8.2. *Assumptions on A are as in the beginning of the subsection. Then:*

(a) *If* $t = 2n$, *then there exists* $w_s^{(r)} \in \mathfrak{N}_A$ *for* $s = 1, 2$ *and* $r = 1, 2, \cdots, n$, *such that* $ord_u(w_s^{(r)} - \pi_s^{-r} e_i) \geq D(A)$.

(b) *If* $t = 2n + 1$, *then there exists* $w \in \mathfrak{N}_A$ *such that* $w \equiv \pi_1^{-(n+1)} \alpha_1 e_1 + (-1)^c \pi_2^{-(n+1)} \alpha_1^\sigma \lambda^{2m_1 + \nu(\eta_1)} e_2 \mod ord_u \geq d(p^{L(A)+1} - p^{L(A)})$, *where* $c = [\frac{-\nu(\eta_1) - n}{2}]$.

Before we prove Proposition 8.8.2, we first explain how to deduce Theorem 8.1.1(1) from it under the assumption on A as in the beginning of the subsection. It suffices to prove (8.2)(a) and (b). When $m_1 \geq m_2 + m_3$, they follow immediately from Proposition 8.8.2; see the argument after Proposition (8.6.1). In general we prove by induction on m_3. When $m_3 = 1$, since we have assumed $m_1 > m_2$, we always have $m_1 \geq m_2 + 1 = m_2 + m_3$. Suppose $m_3 \geq 2$ and we have proved the theorem for smaller m_3. We may assume $m_1 \leq m_2 + m_3 - 1$. Then $A^{\perp; m_1} \cong \mathbb{Z}/p^{m_1} \times \mathbb{Z}/p^{m_1 - m_3} \times \mathbb{Z}/p^{m_1 - m_2}$ by Proposition 8.7.5. But now $m_1 - m_2 < m_3$, hence (8.2)(a) and (b) follows from induction hypothesis and Corollary (8.7.2), and Theorem 8.1.1 is proved.

In the rest of this subsection we prove Proposition 8.8.2. Once (a) is proved, for (b) one can construct w by knocking out the unwanted entries in the presentation of $\eta_1 \cdot v$ by using the constructed lifts of $\pi_s^{-r} e_s$, where $s = 1, 2$ and $r = 1, 2, \cdots, n$. The argument is similar to that in the proof of Proposition 8.6.1 (b) and is left as an exercise.

Now we look at Proposition 8.8.2 (a). We point out that it suffices to prove the case when $m_1 = m_2 + m_3$. In fact, suppose $m_1 - 2 \geq m_2 + m_3$ and we have

proved the claim for (m_1-2,m_2,m_3). Let $A' := \langle p^2\eta_1\rangle \times \langle \eta_2\rangle \times \langle \eta_3\rangle$, then we have already produced $w_i^{(r)} \in \mathfrak{N}_{A'} \subset \mathfrak{N}_A$ for $i=1,2$ and $r=1,2,\cdots,n-1$ by induction hypothesis. Define $v_1^* := \eta_1 \cdot v - \sum_{s=1}^{2}\sum_{r=1}^{n-1} v[\eta_1,r,s]w_s^{(r)}$, $v_2^* := p\eta_1 \cdot v - \sum_{s=1}^{2}\sum_{r=1}^{n-1} v[p\eta_1,r,s]w_s^{(r)}$, then $v_1^*, v_2^* \in \mathfrak{N}_A$ and

$$v_1^* \equiv \sum_{s=1}^{2}\sum_{r=n}^{2m_1} v[\eta_1,r,s]\pi_s^{-r}e_s, v_2^* \equiv \sum_{s=1}^{2}\sum_{r=n}^{2m_1-2} v[p\eta_1,r,s]\pi_s^{-r}e_s \mod \mathrm{ord}_u \geq D(A')$$

Define

$$w_1^{(1)} := (v[p\eta_1,n,2]v[\eta_1,n,1]-v[\eta_1,n,2]v[p\eta_1,n,1])^{-1}(v[p\eta_1,n,2]v_1^*-v[\eta_1,n,2]v_2^*)$$

One can check that $v[p\eta_1,n,2]v[\eta_1,n,1]-v[\eta_1,n,2]v[p\eta_1,n,1]$ is a unit in $W(k)((u))$ and has order $d(p^{4m-2+\nu(\eta_1)+n}+p^{4m+\nu(\eta_1)+n})$. Since

$$\mathrm{ord}_u v[p\eta_1,n,2] \geq \mathrm{ord}_u v[\eta_1,n,2] \geq dp^{4m-2+\nu(\eta_1)+n}$$

and

$$-(d(p^{4m-2+\nu(\eta_1)+n}+p^{4m+\nu(\eta_1)+n}))+dp^{4m-2+\nu(\eta_1)+n}+D(A') \geq D(A)$$

we deduce that

$$\begin{aligned} w_1^{(1)} \equiv\ & (v[p\eta_1,n,2]v[\eta_1,n,1]-v[\eta_1,n,2]v[p\eta_1,n,1])^{-1}(v[p\eta_1,n,2] \\ & \sum_{s=1}^{2}\sum_{r=n}^{2m_1} v[\eta_1,r,s]\pi_s^{-r}e_s - v[\eta_1,n,2]\sum_{s=1}^{2}\sum_{r=n}^{2m_1-2} v[p\eta_1,r,s]\pi_s^{-r}e_s) \\ & \mod \mathrm{ord}_u \geq D(A) \end{aligned}$$

and it is routine to check that the right hand side is further congruent to $\pi_1^{-n}e_1$ modulo $\mathrm{ord}_u \geq D(A)$. Similarly we can construct $w_2^{(n)} \in \mathfrak{N}_A$ such that $w_2^{(n)} \equiv \pi_2^{-n}e_2$

mod $\mathrm{ord}_u \geq D(A)$, too. Thus the claim in Proposition 8.8.2 (a) for (m_1, m_2, m_3) will be proved.

Therefore now we are reduced to the case when $m_1 = m_2 + m_3$. We divide the situation into the case when $\nu(\eta_1) = -2m_1$ and $\nu(\eta_1) = -2m_1 + 1$. We first assume $\nu(\eta_1) = -2m_1$.

Prove by induction on m_3. First suppose $m_3 = 1$, so $m_1 = m_2 + 1$. Define $A_1 := \langle p\eta_1 \rangle \times \langle \eta_2 \rangle \times \langle \eta_3 \rangle$ and $A_2 := \langle \eta_1 \rangle \times \langle \eta_2 \rangle$. They are both subgroups of index p in A. We will produce two vectors v_1' and v_2' from $\mathfrak{N}_{A_1}$ and $\mathfrak{N}_{A_2}$, respectively, and then produce the desired $w_1^{(n)}$ and $w_2^{(n)}$ by a linear combination of v_1' and v_2'.

By Proposition 8.7.5 (1), $A_1^{\perp;m_2} = \langle \widehat{\eta_1} \rangle \times \langle \widehat{\eta_2} \rangle$, with

$$\widehat{\eta_1} \in (p^{-m_2}\mathcal{O}_F/\mathcal{O}_F) \backslash (p^{-(m_2-1)}\mathcal{O}_F/\mathcal{O}_F)$$

and

$$\widehat{\eta_2} \in (p^{-(m_2-1)}\mathcal{O}_F/\mathcal{O}_F) \backslash (p^{-(m_2-2)}\mathcal{O}_F/\mathcal{O}_F)$$

Moreover, by Proposition 8.7.5 (2) we know $R_{2m_2}(A_1^{\perp;m_2}) = 2 - R_1(A_1) = 1$, so $\nu(\widehat{\eta_1}) = -2m_2$. Write $\widehat{\eta_1} = p^{-m_2}(\widehat{\alpha_1} + \pi_0\widehat{\beta_1})$, where $\widehat{\alpha_1} \in W(\mathbb{F}_{p^2})^\times$, $\widehat{\beta_1} \in W(\mathbb{F}_{p^2})$.

Since the p-rank of $A_1^{\perp;m_2}$ is 2, by Proposition 8.6.1, we deduce that $\widehat{\mathfrak{N}_{A_1^{\perp;m_2}}} \equiv \pi^{-(m_2-1)}\mathfrak{M} + W(k)[[u]] \cdot (\pi_1^{-m_2}\widehat{\alpha_1}\widehat{e_1} + (-1)^{c_1}\pi_2^{-m_2}\widehat{\alpha_1}^\sigma\widehat{e_2}) \mod \mathrm{ord}_u \geq D(A_1^{\perp;m_2})$, where $c_1 = [\frac{-\nu(\widehat{\eta_1})-(m_2-1)}{2}]$. By Lemma 8.7.1 we deduce there exists

$$v_1' \equiv \sum_{i=1}^{2} x_i \pi_i^{-(m_2+1)} e_i \mod \mathrm{ord}_u \geq D(A_1^{\perp;m_2})$$

where $x_i \in W(k)[[u]]^\times$ such that $\lambda x_1\widehat{\alpha_1} + (-1)^{c_1}x_2\widehat{\alpha_1}^\sigma \equiv 0 \mod u$.

On the other hand, since the p-rank of A_2 is 2, by Proposition 8.6.1 we deduce there exists $v_2' \equiv \pi_1^{-(m_2+1)}\alpha_1 e_1 + (-1)^{c_2}\pi_2^{-(m_2+1)}\alpha_1^{\sigma} e_2 \mod \mathrm{ord}_u \geq D(A_2)$, where $c_2 = [\frac{-\nu(\eta_1)-m_2}{2}]$. Note that $L(A) = L(A_2) = 4m-3-m_2 = L(A_1^{\perp;m_2})-1$, so $D(A_2), D(A_1^{\perp;m_1}) \geq D(A)$. One can check the determinant of $\begin{pmatrix} x_1 & x_2 \\ \alpha_1 & (-1)^{c_2}\alpha_1^{\sigma} \end{pmatrix}$ is a unit in $W(k)[[u]]$, therefore by a linear combination of v_1', v_2' we can produce w_1' and w_2' in $\mathfrak{N}_A$ such that $w_i' \equiv \pi_i^{-(m_2+1)} e_i \mod \mathrm{ord}_u \geq D(A)$. This finishes the proof when $m_3 = 1$.

Now suppose $m_2 \geq 2$, $m_1 = m_2 + m_3$ and we have proved Proposition 8.8.2 for a smaller m_3. Define $A_1 := \langle p^2\eta_1\rangle \times \langle \eta_2\rangle \times \langle \eta_3\rangle$, by Proposition 8.7.5 (a) we know $A_1^{\perp;m_1-2} = \langle \widehat{\eta_1}\rangle \times \langle \widehat{\eta_2}\rangle \times \langle \widehat{\eta_3}\rangle$, and if we assume $\widehat{\eta_i} \in (p^{-m_i'}\mathcal{O}_F/\mathcal{O}_F)\backslash(p^{-(m_i'-1)}\mathcal{O}_F/\mathcal{O}_F)$, then $m_1' = m_2 + m_3 - 2$, $m_2' = m_2 - 2$, $m_3' = m_3 - 2$. By Proposition 8.7.5 (b) we know $\nu(\widehat{\eta_1}) = -2(m_2+m_3-2) = -2(n-2)$. By the induction hypothesis, we know $\widehat{\mathfrak{N}_{A_1^{\perp;(m_1-2)}}}$ reduces to $\pi^{-(n-3)}M_1^{\vee} \oplus \pi^{-(n-3)}M_2^{\vee}$ modulo u, hence as its orthogonal complement under the Weil pairing $p^{-(n-2)}\mathfrak{M}_m/\mathfrak{M}_m \times p^{-(n-2)}\mathfrak{M}^{\vee}/\mathfrak{M}_m^{\vee} \to p^{-(n-2)}W(k)[[u]]/W(k)[[u]]$, there exists $w_s^{(r)} \in \mathfrak{N}_{A_1}$ for $s = 1, 2$ and $r = 1, 2, \cdots, n-1$, such that $w_s^{(r)} = \pi_s^{-r}e_s + \sum_{i=1}^{2}\sum_{j=n}^{2n-4}\pi_i^{-j}h_{i,j,r,s}e_i$, with $h_{i,j,r,s} \in uW(k)[[u]]$.

Define $A_2 := \langle p^2\widehat{\eta_1}\rangle \times \langle \widehat{\eta_2}\rangle \times \langle \widehat{\eta_3}\rangle \subset A_1^{\perp;m_1-2}$. Then by induction hypothesis we know there exists $\widehat{w_k^{(l)}} \in \widehat{\mathfrak{N}_{A_2}}$ for $k = 1, 2$ and $l = 1, 2, \ldots, n-4$ such that $\widehat{w_k^{(l)}} \equiv \pi_k^{-l}\hat{e_k} \mod \mathrm{ord}_u \geq D(A_2)$. Since the $\widehat{w_k^{(l)}}$'s are orthogonal to the w_s^r's, by computing $\langle w_s^{(r)}, \widehat{w_k^{(l)}}\rangle_{m_1-2}$ inductively for $l = 1, 2, \cdots, n-4$, we can deduce $\mathrm{ord}_u h_{i,j,r,s} \geq D(A_2) = d(p^{4m+3-n} - p^{4m+2-n})$ for $n+1 \leq j \leq 2n-4$ and all i, r, s.

Since $\widehat{\eta_1}\cdot\hat{v} = \sum_{i=1}^{2}\sum_{j=1}^{2n-4}\pi_i^{-j}v[\widehat{\eta_1},j,i]\widehat{e_i}$ is also orthogonal to $w_s^{(r)}$, and $\mathrm{ord}_u v[\widehat{\eta_1},j,i] \geq dp^{4m+1-n}$ when $j \geq n-1$, so when $r \leq n-2$ we can deduce

$$\sum_{i=1}^{2}\langle v[\widehat{\eta_1},n-3,i]\pi_i^{-(n-3)}\widehat{e_i}, h_{i,n,r,s}\pi_i^{-n}e_i\rangle_{m_2-2} \equiv 0 \mod \mathrm{ord}_u \geq dp^{4m+1-n}$$

Similarly if we consider the pairing between $p\widehat{\eta_1}\cdot\hat{v}$ and $w_s^{(r)}$ when $r \leq n-2$, we get

$$\sum_{i=1}^{2}\langle v[p\widehat{\eta_1},n-3,i]\pi_i^{-(n-3)}\widehat{e_i}, h_{i,n,r,s}\pi_i^{-n}e_i\rangle_{m_2-2} \equiv 0$$

$$\mod \mathrm{ord}_u \geq d(p^{4m+3-n} - p^{4m+2-n})$$

Because $\langle \pi_1^{-(n-3)}\widehat{e_1}, \pi_1^{-n}e_1\rangle = \lambda\langle \pi_2^{-(n-3)}\widehat{e_2}, \pi_2^{-n}e_2\rangle$, if we denote

$$T := \begin{pmatrix} \lambda v[\widehat{\eta_1},n-3,1] & v[\widehat{\eta_1},n-3,2] \\ \lambda v[p\widehat{\eta_1},n-3,1] & v[p\widehat{\eta_1},n-3,2] \end{pmatrix}$$

then we can write the equations in matrix form as

$$T\begin{pmatrix} h_{1,n,r,1} & h_{1,n,r,2} \\ h_{2,n,r,1} & h_{2,n,r,2} \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$$

with $\mathrm{ord}_u x_{11}, \mathrm{ord}_u x_{12} \geq dp^{4m+1-n}$, and $\mathrm{ord}_u x_{21}, \mathrm{ord}_u x_{22} \geq d(p^{4m+3-n} - p^{4m+2-n})$. Then by a direct computation of T^{-1} one can deduce that $\mathrm{ord}_u h_{i,n,r,s} \geq d(p^{4m+1-n} - p^{4m-1-n})$ for all i, s, and $r \leq n-2$.

When $r = n-1$, we will have

$$\begin{pmatrix} h_{1,n,n-1,1} & h_{1,n,n-1,2} \\ h_{2,n,n-1,1} & h_{2,n,n-1,2} \end{pmatrix} \equiv T^{-1}\begin{pmatrix} \lambda v[\widehat{\eta_1},n-2,1] & v[\widehat{\eta_1},n-2,2] \\ \lambda v[p\widehat{\eta_1},n-2,1] & v[p\widehat{\eta_1},n-2,2] \end{pmatrix}$$

$$\mod \mathrm{ord}_u \geq d(p^{4m+1-n} - p^{4m-1-n})$$

Now we consider the following elements in $\mathfrak{N}_{A_1}$:

$$v_1 = \eta_1 \cdot v, v_2 = p\eta_1 \cdot v, v_{2k+1} = w_1^{(n-k)}, v_{2k+2} = w_2^{(n-k)}, \text{ for } k = 1, 2, \cdots, n-1$$

If we follow the linear algebra approach in 8.5 with the presentations

$$v_i = \sum_{s=1}^{2} \sum_{r=1}^{2n} v_{i,r,s} \pi_s^{-r} e_s$$

$$v_1 = \sum_{s=1}^{2} \sum_{j=1}^{2n} v[\eta_1, j, s] \pi_s^{-j} e_s, v_2 = \sum_{s=1}^{2} \sum_{j=1}^{2n-2} v[p\eta_1, j, s] \pi_s^{-j} e_s$$

$$w_s^{(r)} = \pi_s^{-r} e_s + \sum_{i=1}^{2} \sum_{j=n}^{2n-4} \pi_i^{-j} h_{i,j,r,s} e_i$$

we will form the $2n \times 2n$ matrix:

$$C \equiv \begin{pmatrix} v[\eta_1, n, 1] & v[p\eta_1, n, 1] & h_{1,n,n-1,1} & h_{1,n,n-1,2} & 0 & \cdots & 0 \\ v[\eta_1, n, 2] & v[p\eta_1, n, 2] & h_{2,n,n-1,1} & h_{2,n,n-1,2} & 0 & \cdots & 0 \\ v[\eta_1, n-1, 1] & v[p\eta_1, n-1, 1] & 1 & & & & \\ v[\eta_1, n-1, 2] & v[p\eta_1, n-1, 2] & & 1 & & & \\ \vdots & \vdots & & & 1 & & \\ v[\eta_1, 1, 1] & v[p\eta_1, 1, 1] & & & & \ddots & \\ v[\eta_1, 1, 2] & v[p\eta_1, 1, 2] & & & & & 1 \end{pmatrix}$$

$$\bmod \operatorname{ord}_u \geq d(p^{4m+1-n} - p^{4m-1-n})$$

By Lemma (8.5.1), it suffices to show $\det C$ is a unit in $W(k)((u))$, and

$$\operatorname{ord}_u (\det C)^{-1} C_{k,l} v_{l,r,s} \geq D(A) = d(p^{4m-1-n} - p^{4m-2-n})$$

for $k = 1, 2$, $l = 1, 2, \cdots, 2n$, $r = n+1, n+2, \cdots, 2n$, and $s = 1, 2$.

With the given form for the matrix C, $\det C$ is equal to the determinant of the following 2×2 matrix:

$$C_0 := \begin{pmatrix} v[\eta_1, n, 1] & v[p\eta_1, n, 1] \\ v[\eta_1, n, 2] & v[p\eta_1, n, 2] \end{pmatrix} - \begin{pmatrix} h_{1,n,n-1,1} & h_{1,n,n-1,2} \\ h_{2,n,n-1,1} & h_{2,n,n-1,2} \end{pmatrix} \cdot \begin{pmatrix} v[\eta_1, n-1, 1] & v[p\eta_1, n-1, 1] \\ v[\eta_1, n-1, 2] & v[p\eta_1, n-1, 2] \end{pmatrix}$$

One can check

$$\begin{aligned} \det C \equiv\ & \epsilon^{2n-1}(\hat{\alpha}_1^{1+\sigma}\lambda(y_{n-1}z_{n-3} - z_{n-1}y_{n-3}))^{-1}(\lambda\alpha_1\hat{\alpha}_1 y_{n-3}y_{n-2} + \alpha_1^{\sigma}\hat{\alpha}_1^{\sigma} z_{n-3}z_{n-2})\cdot \\ & (\lambda\alpha_1\hat{\alpha}_1 y_{n-1}y_n + \alpha_1^{\sigma}\hat{\alpha}_1^{\sigma} z_{n-1}z_n) \mod \mathrm{ord}_u > d_0(p^{-(n-2)} + p^{-n}) \end{aligned}$$

By Proposition 8.3.3, the three factors above

$$(y_{n-1}z_{n-3} - z_{n-1}y_{n-3})^{-1}, (\lambda\alpha_1\widehat{\alpha_1} y_{n-3}y_{n-2} + \alpha_1^{\sigma}\widehat{\alpha_1}^{\sigma} z_{n-3}z_{n-2})$$

and

$$(\lambda\alpha_1\widehat{\alpha_1} y_{n-1}y_n + \alpha_1^{\sigma}\widehat{\alpha_1}^{\sigma} z_{n-1}z_n)$$

are all units in $W(k)((u))$, with orders equal to $-d(p^{4m+1-n}+p^{4m-1-n})$, $d(p^{4m+1-n}+p^{4m-n})$, and $d_0(p^{4m-1-n}+p^{4m-2-n})$, respectively. So we have proved $\det C$ is a unit in $W(k)((u))$ with order equal to $d_0(p^{4m-n}+p^{4m-2-n})$.

The cofactors $C_{k,l}$ for $k = 1, 2$ and $l = 1, 2$ are equal to the four entries of the 2×2 matrix C_0. One can check by a direct computation of C_0 to see $\mathrm{ord}_u C_{1,1}, \mathrm{ord}_u C_{2,1} \geq dp^{4m-n}$, and $\mathrm{ord}_u C_{1,2}, \mathrm{ord}_u C_{2,2} \geq dp^{4m-2-n}$.

Now suppose $k = 1, 2$, $r \geq n+1$ and $s = 1, 2$, we have $\mathrm{ord}_u v_{1,r,s} \geq dp^{4m-1-n}$

and $\mathrm{ord}_u v_{2,r,s} \geq dp^{4m+1-n}$ from the definition of the presentations, then

$$\mathrm{ord}_u(\det C)^{-1}C_{k,1}v_{1,r,s} \geq d(p^{4m-1-n} - p^{4m-2-n})$$

$$\mathrm{ord}_u(\det C)^{-1}C_{k,2}v_{2,r,s} \geq d(p^{4m+1-n} - p^{4m-n})$$

On the other hand, when $l \geq 3$, $\mathrm{ord}_u v_{l,r,s} \geq d(p^{L(A_2)+1} - p^{L(A_2)}) = d(p^{4m+3-n} - p^{4m+2-n})$, hence $\mathrm{ord}_u(\det C)^{-1}C_{k,l}v_{l,r,s} \geq d_0(p^{4m+3-n} - p^{4m+2-n} - p^{4m-n} - p^{4m-2-n})$. Thus in total we have $\mathrm{ord}_u(\det C)^{-1}C_{k,l}v_{l,r,s} \geq d(p^{4m-1-n} - p^{4m-2-n})$ for all $k = 1, 2$, $l = 1, 2, \cdots, 2n$, $r = n+1, n+2, \cdots, 2n$, and $s = 1, 2$. This means $w_k^{(n)} := \sum_{l=1}^{2n}(\det C)^{-1}C_{k,l}v_l \in \mathfrak{N}_A$ satisfies $\mathrm{ord}_u(w_k^{(n)} - \pi_k^{-n}e_k) \geq d(p^{4m-1-n} - p^{4m-2-n})$ by Lemma (8.5.1). That lower bound is exactly equal to $D(A)$, thus Proposition 8.8.2 is proved in the case when $\nu(\eta_1) = -2m_1$.

Finally we are left with the case when $\nu(\eta_1) = -2m_1 + 1$. We still prove by induction on m_3. Now $m_1 + m_2 + m_3 = 2n$ is even, and $m_1 = m_2 + m_3$. Since we have assumed $R_1(A) = 1$, this means we may assume $\nu(\eta_i) = -2m_i$ for $i = 2, 3$. Pick $\eta_i^* \in p^{-m}\mathcal{O}_F/\mathcal{O}_F$ such that $\pi\eta_i^* = \eta_i$ and define $A^* := \langle\eta_1^*\rangle \times \langle\eta_2^*\rangle \times \langle\eta_3^*\rangle$; the orders of the three factors are equal to $m_1, m_2 + 1, m_3 + 1$, respectively. By Proposition 8.7.5 we know $(A^*)^{\perp;m_1} = \langle\widehat{\eta_1^*}\rangle \times \langle\widehat{\eta_2^*}\rangle \times \langle\widehat{\eta_3^*}\rangle$ with the orders of the three factors equal to $m_1, m_1 - m_3 - 1 = m_2 - 1$, and $m_1 - m_2 - 1 = m_3 - 1$. Moreover, since $R_{2m_1}((A^*)^{\perp;m_1}) = 2 - R_1(A^*) = 0$, we deduce that $\nu(\widehat{\eta_1^*}) = -2m_1 + 1$.

When $m_3 \geq 2$, the induction hypothesis guarantees the existence of $\widehat{w_s^{*(r)}} \in \widehat{\mathfrak{N}_{(A^*)^{\perp;m_1}}}$ for $s = 1, 2$ and $r = 1, 2, \cdots, n-1$. such that $\mathrm{ord}_u(\widehat{w_s^{*(r)}} - \pi_i^{-r}e_i) \geq D((A^*)^{\perp;m_1})$. Note that $m_1 \geq (m_2 - 1) + (m_3 - 1) + 2$, so $D((A^*)^{\perp;m_1}) = d_0(p^{4m-1-n} -$

$p^{4m-2-n}) = D(A)$. When $m_3 = 1$, the p-rank of $(A^*)^{\perp;m_1}$ is equal to 2 and Proposition 8.6.1 also implies the existence of such $\widehat{w_i^{*(r)}}$. Then by Lemma 8.7.1 there exists $w_s^{*(r)} \in \mathfrak{N}_{A^*}$ for $s = 1, 2$ and $r = 1, 2, \cdots, n+1$, such that $w_s^{*(r)} \equiv \pi_s^{-r} e_s$ mod $\mathrm{ord}_u \geq D(A)$. Since $\mathfrak{N}_A = \pi \cdot \mathfrak{N}_{A^*}$, the proof of Proposition 8.8.2 is completed.

8.9 A final remark

Let R runs over the finite extensions of R_0, it is unexpected from Theorem (8.1.1) that whether the reduction of a finite locally free subgroup scheme $\mathcal{G}$ in $\mathcal{X}_R$ is $\mathcal{O}_F$-stable is completely determined by its order. We finally comment that if we have known Theorem (8.1.1)(1)(b) for all odd positive integers t, then there is in fact a simple proof to deduce Theorem (8.1.1)(1)(a) for all even positive integers t.

Since the reflex field of the p-adic CM type (F, Φ) is $F = B(\mathbb{F}_{p^2})[\pi_0]/(\pi_0^2 - \epsilon p)$ itself, there exists an $\mathcal{O}_F$-linear CM p-divisible group $\mathcal{Y}$ over $\mathcal{O}_F$ with p-adic CM type Φ, such that the associated Galois representation $\rho : \mathrm{Gal}(F^{ab}/F) \to \mathcal{O}_F^\times$ carries I_F^{ab} onto the image of ρ; see [1](3.7.3). This implies any p^i-torsion geometric point on $\mathcal{Y}$ is rational over a totally ramified extension F_i over F. Let $Y := \mathcal{Y}_{\mathbb{F}_{p^2}}$. Since $\mathcal{Y}_{R_0}$ is $\mathcal{O}_F$-linearly isomorphic to $\mathcal{X}$, it suffices to prove for every finite totally ramified extension E of F and every finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{Y}_{\mathcal{O}_E}$ such that $\#\mathcal{G} = p^{2n}$, the closed fiber $G := \mathcal{G}_k$ is equal to $Y[\pi^n]$.

We prove by induction on n. Suppose we have proved for all smaller n's. Take a filtration $\mathcal{G}_2 \subset \mathcal{G}_1 \subset \mathcal{G}$ such that the rank of $\mathcal{G}/\mathcal{G}_1$ and $\mathcal{G}_1/\mathcal{G}_2$ are both equal to p.

Denote G_i as the closed fiber of $\mathcal{G}_i$. By induction hypothesis we may assume $G_2 = Y[\pi^{-(n-1)}]$. Note that Y/G_2 is $\mathcal{O}_F$-linearly isomorphic to Y. The subgroup $G_1/G_2 \subset Y/G_2$ has order p, and since $Y/G_2 \cong Y$ is local-to-local type we know $G_1/G_2 \cong \alpha_p$. We have seen the Dieudonné module attached to Y/G_2 is $\mathcal{O}_F$-linearly isomorphic to $M = W(\mathbb{F}_{p^2})[\pi]/(\pi^2 - \epsilon p)e_1 \oplus W(\mathbb{F}_{p^2})[\pi]/(\pi^2 - \epsilon^\sigma p)e_2$, where the $\mathcal{O}_F$-structure is defined by $a \cdot e_1 := ae_1, a \cdot e_2 := a^\sigma e_2$ for $a \in W(\mathbb{F}_{p^2})$, and $\pi_0 \cdot e_i := \pi e_i$. The $\mathcal{O}_F$-linear Frobenius and Verschiebung maps are defined by $Fe_1 = -\epsilon^{-1}\lambda^{-1}\pi e_2, Ve_1 = -\pi e_2$, and $Fe_2 = -\epsilon^{-1}\pi e_1, Ve_2 = -\lambda^{-\sigma}\pi e_1$. The Dieudonné module M' attached to X/G_1 is equal to $M + W(k) \cdot x$, where $x \in p^{-1}M/M$. It is easy to check $a(M) = 2$. We claim the Dieudonné module M' is $\mathcal{O}_F$-stable if and only if $a(M') = 2$. In fact, to make $Fx \in M'$ we must have $x \equiv \pi^{-1}(x_1e_1 + x_2e_2) \mod M$ with $x_1, x_2 \in \mathbb{F}_{p^2}$, then

$$Fx \equiv -(\epsilon^{-1}x_2^\sigma e_1 + \epsilon^{-1}\lambda^{-1}x_1^\sigma e_2), Vx \equiv -(\lambda^{-\sigma}x_2^{-\sigma}e_1 + x_1^{-\sigma}e_2) \mod \pi M_1 \oplus \pi M_2$$

It is clear that $a(M') = 2$ if and only if Fx and $Vx \mod p$ are linearly dependent over $\mathbb{F}_{p^2}$ modulo $\pi M_1 \oplus \pi M_2$. This is further equivalent to the degeneracy of the 2×2 matrix $\begin{pmatrix} \epsilon^{-1}x_2^\sigma & \epsilon^{-1}\lambda^{-1}x_1^\sigma \\ \lambda^{-\sigma}x_2^{-\sigma} & x_1^{-\sigma} \end{pmatrix}$. Note that $x_i \in \mathbb{F}_{p^2}$, hence $x_i^\sigma = x_i^{-\sigma}$. The determinant is therefore equal to $\epsilon^{-1}(x_1x_2)^\sigma(1 - \lambda^{-\sigma-1}) = 2\epsilon^{-1}(x_1x_2)^\sigma$, since $\lambda^{-\sigma-1} = \epsilon^{-\frac{p^2-1}{2}} = -1$. Thus $a(M') = 2$ if and only if $x_1 = 0$ or $x_2 = 0$, which is clearly equivalent to saying M' is $\mathcal{O}_F$-stable.

As a result, since the order of G_1 is an odd power of p, by our assumption we have known G_1 is not $\mathcal{O}_F$-stable. Hence $a(M') = 1$. As a result, there is a

unique Dieudonné module $M'' \supset M'$ with length$M''/M' = p$, which is necessarily the Diedonne module attached to Y/G_2. But $M'' := \pi^{-1}M \cong M$ obviously satisfies that condition, hence $G/G_2 = (Y/G_2)[\pi]$, $G = Y[\pi^n]$.

Part II

The Relabelling Action On The Equicharacteristic Universal Deformation Space of p-divisible Smooth Formal Groups over $\overline{\mathbb{F}}_p$

Chapter 9

Introduction to Part II

Let X be a connected p-divisible group over $\overline{\mathbb{F}}_p$. The universal deformation space of X is a smooth formal scheme $\mathrm{Spf}\,\mathcal{R}$ over $W(\overline{\mathbb{F}}_p)$. There is a natural action by $\mathrm{Aut}(X)$ on $\mathrm{Spf}\,\mathcal{R}$ by "changing the label on the closed fiber", which we will refer to as the *relabelling action* throughout this paper. The equacharacteristic universal deformation space of X is $\mathrm{Spf}\,\mathcal{R}/p\mathcal{R}$, and the action by $\mathrm{Aut}(X)$ induced from the relabelling action will be referred to as the *equicharacteristic relabelling action*. On the other hand, let G be the formal group associated to X, then the universal deformation space and the equicharacteristic deformation space of G are naturally isomorphic to those defined for X. The relabelling action and equicharacteristic relabelling action can be defined in the same way, and these definitions are compatible with the corresponding notions for X. The relabelling action and the equicharacteristic relabelling action by $\rho \in \mathrm{Aut}(X)$ will be denoted by R_ρ and

$\overline{R}_\rho$, respectively.

The relabelling action was first studied by Lubin and Tate in [14] in the one-dimensional case. In this second part of the thesis, we study the relabelling action, especially the equicharacteristic relabelling action, for X in general dimensions. For $\rho \in \mathrm{Aut}(X)$, an algorithm of computing $\overline{R}_\rho$ is given, and some asymptotic properties of $\overline{R}_\rho$ in $\mathrm{Aut}(\mathcal{R}/p\mathcal{R})$ as $\rho \to 1$ in $\mathrm{Aut}(X)$ are obtained.

The relabelling action is interesting mainly due to the following two applications:

Stable homotopy theory. Since Quillen's discovery in [19], the connection between formal groups and stable homotopy theory have been heavily studied by algebraic topologists. In the case when G is one-dimensional with height h, the automorphism group $\mathrm{Aut}(G)$ is also known as the *Morava group* in stable homotopy theory ([15] Lec. 19). The relabelling action induces an action by $\mathrm{Aut}(G)$ on a cohomology theory E_h^*, which is called the *Morava E-theory* ([15] Lec. 22). For a finite complex X, there exist spectral sequences whose E_2 terms are group cohomologies of the Morava group with coefficients in $E_h^*(X)$, such that E^{**} converges to an approximation of the homotopy group $\pi_* X$, and the accuracy increases as h increases (c.f. [4] and [16]).

The Hecke orbit problem. Let $\mathcal{A}_g$ be the moduli stack over $\overline{\mathbb{F}}_p$ that classifies principally polarized abelian varieties of dimension g over $\overline{\mathbb{F}}_p$. A point $x \in \mathcal{A}_g(\overline{\mathbb{F}}_p)$ corresponds to an principally polarized abelian variety (A_x, λ_x) over $\overline{\mathbb{F}}_p$. The Hecke

orbit conjecture in the Siegel case asks whether $\mathcal{G}^{(p)}(x) :=$

$$\{y \in \mathcal{A}_g(\overline{\mathbb{F}}_p) | \exists \text{ an isogeny } \phi : A_y \to A_x, m \in \mathbb{N} \text{ such that } (m,p) = 1, \phi^* \lambda_x = m\lambda_y\}$$

is Zariski dense in $\mathcal{A}_g$ if x is ordinary.

It was Chai who introduced the idea that the equicharacteristic relabelling action plays an important role in studying the Hecke orbit problem in [2]. We briefly explain the so-called *local stabilizer principle* as follows. The group $\mathrm{GSp}_{2g}(\mathbb{A}_f^{(p)})$ operates on $\mathcal{A}_g$ as algebraic correspondences. Let Z be the Zariski closure of $\mathcal{G}^{(p)}(x)$, and $y \in Z(\overline{\mathbb{F}}_p)$. The principally polarized abelian variety (A_y, λ_y) is stable under $\mathrm{Aut}(A_y, \lambda_y)$. On the other hand, the formal completion $Z^{/y}$ embedded in $\mathcal{A}_g^{/y}$ is invariant under $\mathrm{Aut}((A_y, \lambda_y)[p^\infty])$, the so-called *stabilizer subgroup*. When y has a large stabilizer subgroup, if we can have enough information on the relabelling action to identify the invariant formal subvarieties of $\mathcal{A}_g^{/y}$, then we would have better understanding on Z.

The Hecke orbit conjecture for the Siegel case was proved in [2] using the "Hilbert trick", which is special phenomenon that no longer comes for rescue on general Shimura varieties of PEL type. To approach the Hecke orbit conjecture in general, the local stabilizer principle seems the only known method at this time to get information about Z. In the case of Shimura varieties of unitary (m,n) type, the equicharacteristic relabelling action $\overline{R}_\rho$ on $\mathrm{Spf}\,\mathcal{R}/p\mathcal{R}$ naturally arises.

In the case when X has dimension 1 and height h, Gross and Hopkins used in

[7] the p-adic period map

$$\mathrm{Spf}\,(\mathcal{R} \otimes_{W(\overline{\mathbb{F}}_p)} B(\overline{\mathbb{F}}_p)) \to \mathbb{P}^{h-1}_{B(\overline{\mathbb{F}}_p)}$$

to compute the relabelling action. Here $\mathcal{R} \otimes_{W(\overline{\mathbb{F}}_p)} B(\overline{\mathbb{F}}_p)$ is a rigid analytic space over $B(\overline{\mathbb{F}}_p)$ that is isomorphic to the open unit ball of dimension $h-1$, and $\mathbb{P}^{h-1}_{B(\overline{\mathbb{F}}_p)}$ is the projective space of one-dimensional quotients of the covariant crystal attached to X. The p-adic period map is $\mathrm{Aut}(X)$-invariant, hence "linearizes" the relabelling action on the "generic fiber" of $\mathrm{Spf}\,\mathcal{R}$. However, the period map is not defined over $W(\overline{\mathbb{F}}_p)$, hence does not provide much information on the equicharacteristic relabelling action $\overline{R}_\rho$ on $\mathrm{Spf}\,\mathcal{R}/p\mathcal{R}$.

Working with the Cartier-Dieudonné theory in [3], Chai obtained information in the one-dimensional case on the leading terms of the equicharacteristic relabelling action under an appropriate filtration on $\mathcal{R}/p\mathcal{R}$. Recently, Chai discovered a new approach via formal group laws to compute the equicharacteristic relabelling action in the one-dimensional case. This approach can provide more information on the asymptotic behavior of $\overline{R}_\rho$ as $\rho \to 1$. In this second part of the thesis, we generalize his approach to arbitrary dimensions.

The main tool employed in this approach is the theory of p-typical formal group laws. A formal group law $F = F(\underline{x}, \underline{y})$ over R is said to be *p-typical*, if $\mathbf{f}_l \gamma = 0$ for every formal curve $\gamma(t)$ and $(l, p) = 1$, where $\mathbf{f}_l$ is the l-th Frobenius operator on formal curves in F; see (10.3 and 10.5) for details of the definition. Over a $\mathbb{Z}_{(p)}$-algebra, every smooth formal group can be assigned a coordinate such that the

corresponding formal group law is p-typical. If we choose a p-typical formal group law F on the given formal group $G/\overline{\mathbb{F}}_p$, the universal deformation space can be interpreted as classifying the p-typical liftings of F up to isomorphisms that reduce to identity over $\overline{\mathbb{F}}_p$; (see 13.1.6).

Let $\mathcal{F}$ be a universal p-typical lifting of F over $\mathcal{R}$. A natural approach to compute the relabelling action R_ρ on $\mathcal{R}$ is to first find another p-typical lifting $\hat{\mathcal{F}}$ over $\mathcal{R}$ equipped with an isomorphism $\alpha_\rho : \mathcal{F} \to \hat{\mathcal{F}}$ such that α_ρ reduces to ρ over $\overline{\mathbb{F}}_p$. If we can modify $\hat{\mathcal{F}}$ by an isomorphism, which reduces to identity over $\overline{\mathbb{F}}_p$, into a p-typical formal group law $\mathcal{F}'$ that is equal to the pushforward of $\mathcal{F}$ via some $W(\overline{\mathbb{F}}_p)$-endomorphism $\mathcal{R} \to \mathcal{R}$, then this endomorphism is the desired relabelling action R_ρ.

The advantage of working with p-typical formal group laws is that not only the p-typical formal group laws themselves but also the isomorphisms between them can be parametrized by an infinite sequence of parameters. More importantly, the transition formulas on the parameters to describe isomorphic p-typical formal group laws can be made into *integral* recursive formulas in the sense that every term in the formulas is defined over $W(\overline{\mathbb{F}}_p)$. This allows us to find a pattern of the equicharacteristic relabelling action $\overline{R}_\rho$ on $\operatorname{Spf}\mathcal{R}/p\mathcal{R}$. Since $\mathcal{R}/p\mathcal{R}$ is a power series ring over $\overline{\mathbb{F}}_p$, there exists a natural subgroup filtration $\mathrm{Fil}^{\cdot}(\mathrm{Aut}(\mathcal{R}/p\mathcal{R}))$ on $\mathrm{Aut}(\mathcal{R}/p\mathcal{R})$ such that $\mathrm{Fil}^i(\mathrm{Aut}(\mathcal{R}/p\mathcal{R}))$ consists of automorphisms that are congruent to identity modulo order $\geq i$. On the other hand, there exists a natural subgroup filtration

$\mathrm{Fil}^{\cdot}(\mathrm{Aut}(X))$ on $\mathrm{Aut}(X)$ such that $\mathrm{Fil}^{i}(\mathrm{Aut}(X)) = 1 + p^{i}\mathrm{End}(X)$. We prove that when $\rho \in \mathrm{Fil}^{M}(\mathrm{Aut}(X))$, $\overline{R}_{\rho} \in \mathrm{Fil}^{p^{M}}(\mathrm{Aut}(\mathcal{R}/p\mathcal{R}))$. For fixed $\rho \in \mathrm{Aut}(X)$ and order N, we describe the process of computing $\overline{R}_{\rho}$ modulo order $\geq N$.

The structure of this second part of the thesis is as follows. In chapter 10, we introduce some preliminary facts on formal groups and formal group laws, including the definition of p-typical formal group laws and the various ways to parametrize them. In chapter 11, we derive some integral recursive formulas between the different ways in parametrizing the same or isomorphic p-typical formal group laws are derived. In 12, we develop some technical lemmas on solving systems of infinitely many formal power series equations in infinitely many indeterminates over an adic ring. In 13, we first show that under a specific choice of the p-typical formal group law F associated to $G/\overline{\mathbb{F}}_{p}$, the computation of the relabelling action R_{ρ} (as well as the equicharacteristic relabelling action $\overline{R}_{\rho}$) is largely simplified. Then we obtain asymptotic properties of the equicharacteristic relabelling action $\overline{R}_{\rho}$ in $\mathrm{Aut}(\mathcal{R}/p\mathcal{R})$ as $\rho \to 1$ in $\mathrm{Aut}(X)$, and describe the algorithm of computing approximations to $\overline{R}_{\rho}$ with any desired accuracy.

Chapter 10

Formal groups and formal group laws

Throughout this second part of the thesis, p is a prime number that is greater than 2. All the rings mentioned have 1. If R is a ring, we denote the R-algebra of $m \times n$ matrices by $R^{m \times n}$. In this section, we review some facts on formal groups and formal group laws.

10.1 Basic definitions

Let R be a commutative ring with 1. Denote by $\mathfrak{Nil}_R$ the category of nilpotent R-algebras, and by $\mathfrak{ProNil}_R$ the category of filtered projective limits of nilpotent R-algebras. Denote by $\mathfrak{Sets}$ the category of sets, and $\mathfrak{Ab}$ the category of abelian groups. Note that every functor $G : \mathfrak{Nil}_R \to \mathfrak{Sets}$ uniquely extends to a functor

$\mathfrak{ProNil}_R \to \mathfrak{Sets}$ which commutes filtered projective limits. The similar property on extensions holds for functors from $\mathfrak{Nil}_R$ to $\mathfrak{Ab}$.

We say a functor G from $\mathfrak{Nil}_R$ to $\mathfrak{Ab}$ is *exact* if it sends a short exact sequence to a short exact sequence.

Definition 10.1.1. A functor $G : \mathfrak{Nil}_R \to \mathfrak{Ab}$ is said to be a (*commutative*) *formal group*, if G is exact and commutes with arbitrary direct sums.

Let $\mathfrak{Mod}_R$ be the category of R-modules. There is a natural embedding from $\mathfrak{Mod}_R$ to $\mathfrak{ProNil}_R$ by endowing the algebra structure on $M \in \mathfrak{Mod}_R$ as $M \cdot M = 0$. For a smooth formal group functor G, define its *tangent functor* $\mathfrak{t}_G : \mathfrak{Mod}_R \to \mathfrak{Mod}_R$ by restricting G to the subcategory $\mathfrak{Mod}_R$ of $\mathfrak{ProNil}_R$, and endowing $G(M)$ with the natural R-module structure induced from that on $M \in \mathfrak{Mod}_R$.

Proposition 10.1.2. ([24]) *Let G be a formal group functor. If $\mathfrak{t}_G(R)$ is a finitely generated projective R-module, then G is propresentable. If moreover $\mathfrak{t}_G(R)$ is a free R-module of rank m, then G is propresentable by $Spf R[[X_1, X_2, \cdots, X_m]]$.*

In the latter case of the statement in the property, we say G is an *m-dimensional smooth formal group* and the integer m is called the *dimension* of G. In the future, if the dimension is known, we write the coordinate ring $R[[X_1, X_2, \cdots, X_m]]$ of G as $R[[X]]$ in abbreviation. The group structure on G induces a homomorphism $\mu : R[[X]] \to R[[X]] \otimes_R R[[Y]]$. The following notion of *formal group laws* provides a concrete way to describe μ:

Definition 10.1.3. An (m-dimensional) formal group law is an m-tuple of formal power series $F(X,Y) = (F_1(X,Y), F_2(X,Y), \cdots, F_m(X,Y))$ satisfying the following conditions:

(a) (identity) $F(X,0) = X, F(0,Y) = Y$;

(b) (commutativity) $F(X,Y) = F(Y,X)$;

(c) (associativity) $F(F(X,Y),Z) = F(X,F(Y,Z))$.

Remark 10.1.4. In general, for any index set I, we can define *a formal group law with index set* I to be a set of formal power series $\{F_i(X,Y)|i \in I\}$ where each $F_i(X,Y) \in R[[X_i, Y_i|i \in I]]$, such that the three conditions above are satisfied, plus the following finiteness condition when I is infinite:

$$\text{if } F_i(X,Y) = \sum_{\mathbf{m},\mathbf{n} \in I} c_{\mathbf{m},\mathbf{n},i} X^{\mathbf{m}} Y^{\mathbf{n}}$$

then for every $\mathbf{m}, \mathbf{n}$ there are only finitely many $i \in I$ such that $c_{\mathbf{m},\mathbf{n},i} \neq 0$

This additional condition in the case when I is infinite is necessary such that the condition $F(F(X,Y),Z) = F(X,F(Y,Z))$ makes sense.

A *homomorphism* $\alpha : F \to G$ from an m-dimensional formal group law F to an n-dimensional formal group law G is an n-tuple of formal power series in m-variables: $\alpha(X) = (\alpha_1(X), \alpha_2(X), \cdots, \alpha_m(X))$ such that

$$G(\alpha(X), \alpha(Y)) = \alpha(F(X,Y))$$

A *homomorphism* $\alpha : F \to G$ is said to be an *isomorphism* if $m = n$ and there exists a homomorphism $\beta : G \to F$ such that $\alpha(\beta(X)) = X = \beta(\alpha(X))$. A

homomorphism is an isomorphism if and only if $m = n$ and the evaluation of its Jacobian at $X = 0$ is an invertible matrix in $R^{m\times m}$. We say an isomorphism is a *strict isomorphism*, if the evaluation of its Jacobian at $X = 0$ is the identity matrix. An isomorphism $\alpha(X)$ between formal group laws decompose into a composition of a strict isomorphism and the scalar multiplication $X \mapsto JX$, where J is the evaluation of the Jacobian of $\alpha(X)$ at $X = 0$.

If we fix a rigidification $G \cong \operatorname{Spf} R[[X]]$ for an m-dimensional formal group G, the homomorphism $\mu : R[[X]] \to R[[X]] \otimes_R R[[Y]]$ induced by the group structure gives rise to an m-dimensional formal group law. Different rigidifications of G produce isomorphic formal group laws. Conversely, an m-dimensional formal group law defines an m-dimensional smooth formal group over R, by assigning N^m to any nilpotent R-algebra N, with the abelian group structure on N^m defined by the formal group law. If $F(X, Y)$ is an infinite dimensional formal group law with index set I, where I is an infinite set, then the associated formal group is the functor G from $\mathfrak{Nil}_R$ to $\mathfrak{Ab}$, such that $G(N) = \bigoplus_{i\in I} N_{(i)}$[1], equipped with the abelian group structure defined by $F(X, Y)$.

Example 10.1.5. (a) The *additive formal group law* is $\widehat{\mathbf{G}}_a(X, Y) = X + Y$.

(b) The *multiplicative formal group law* is $\widehat{\mathbf{G}}_m(X, Y) = X + Y + XY$.

Proposition 10.1.6. ([8] 1.6.2, 11.1.6) *If R is a $\mathbb{Q}$-algebra, then every formal group*

[1]Here we use $\bigoplus_{i\in I} N_{(i)}$ instead of $\prod_{i\in I} N_{(i)}$ to ensure that G commutes with arbitrary direct sums.

law is strictly isomorphic to the additive formal group law.

Therefore if $\operatorname{char} R = 0$, i.e., all integers n are nonzero in R, a formal group law over R is isomorphic to the additive formal group law after a base change to $R \otimes \mathbb{Q}$. This motivates the following definition:

Definition 10.1.7. If $\operatorname{char} R = 0$, F is a formal group law over R, then the *logarithm* of F is the m-tuple of formal power series $f(X)$ over $R \otimes \mathbb{Q}$ that induces a strict isomorphism from F to $\widehat{\mathbf{G}}_a$ after base change to $R \otimes \mathbb{Q}$.

In particular, if $f(X)$ is the logarithm of $F(X, Y)$, then $F(X, Y) = f^{-1}(f(X) + f(Y))$. We often denote the logarithm of F by $\log_F$.

10.2 Functional equation lemma

Throughout this subsection we assume $\operatorname{char} R = 0$, and denote $K := R \otimes \mathbb{Q}$. In §I.2 and §II.10 of [8], Hazewinkel gave a systematic construction of m-tuple of formal power series $f(X)$ over K that are logarithms of formal group laws over R, i.e., the coefficients of $f^{-1}(f(X) + f(Y))$ are all in R.

Definition 10.2.1. A *Honda ring* is a triple $(R, \mathfrak{a}, \sigma)$, where $\mathfrak{a}$ is an ideal of R, $\sigma : K \to K$ is an endomorphism that sends R to R, satisfying (1) $p \in \mathfrak{a}$; (2) $\sigma(a) \equiv a^p \mod \mathfrak{a}$ for each $a \in R$; (3) for every positive integer r and $b \in K$, $\mathfrak{a}^r b \subset \mathfrak{a} \Rightarrow \mathfrak{a}^r \sigma(b) \subset \mathfrak{a}$.

Note that this condition is automatically satisfied if $\mathfrak{a} = (a)$ is principal, and $\frac{\sigma(a)}{a} \in R^\times$. The endomorphism naturally extends to $K^{m\times n}$ for any m, n.

Example 10.2.2. (a) Let $R = W(\mathbb{F}_{p^n})$, $K = B(\mathbb{F}_{p^n})$, $\mathfrak{a} = (p)$, and σ be the Frobenius automorphism on K. Then $(W(\mathbb{F}_{p^n}), (p), \sigma)$ is a Honda ring.

(b) Suppose $(R, \mathfrak{a}, \sigma)$ is a Honda ring, and assume $p \in \mathfrak{a}$. Let I be a countable index set, $\tilde{R} := R[X_i; i \in I]$, $\tilde{K} := \tilde{R} \otimes \mathbb{Q}$, and $\tilde{\mathfrak{a}} := \mathfrak{a}\tilde{R}$. Extend σ to $\tilde{\sigma} : \tilde{R} \to \tilde{R}$ by defining $\sigma(X_i) := X_i^p$ for $i \in I$. Then $(\tilde{R}, \tilde{\mathfrak{a}}, \tilde{\sigma})$ is also a Honda ring.

Definition 10.2.3. (a) The *Honda's twisted formal power series ring* $K_\sigma^{m\times m}[[\partial]]$ is the non-commutative formal power series ring in one indeterminate ∂ with the multiplication rule $\partial a = \sigma(a)\partial$ for all $a \in K^{m\times m}$. Similarly, $R_\sigma^{m\times m}[[\partial]]$ is the subring of $K_\sigma^{m\times m}[[\partial]]$ that consists of formal power series in ∂ with coefficients in $R^{m\times m}$.

(b) Define the action of $K_\sigma^{m\times m}[[\partial]]$ on $K[[X]]^{m\times 1}$ by $a * \phi(X) = \phi(aX)$ for $a \in K^{m\times m}$, and $(\partial * f)(X) := (\sigma_* f)(X^p)$, where X is the $m \times 1$ column vector $(X_1, X_2, \cdots, X_m)^t$, and X^p stands for $(X_1^p, X_2^p, \cdots, X_m^p)^t$.

Proposition 10.2.4. (*Functional equation lemma*) *Let* $s_1, s_2, \cdots \in K^{m\times m}$ *whose entries* $s_k(i,j)$ *satisfies* $s_k(i,j)\mathfrak{a} \subset R$. *Let* $\eta := 1 - \sum_{n=1}^{\infty} s_i\partial$, $g(X) \in \mathbb{R}[[X]]^{m\times 1}$ *with invertible Jacobian matrix, and* $f_g(X) := \eta^{-1} * g(X) \in K[[X]]^{m\times 1}$.

(*a*) $F_g(X,Y) := f_g^{-1}(f_g(X) + f_g(Y))$ *is an* m*-dimensional formal group law over* R.

(*b*) *For every* $\overline{g}(X) \in \mathbb{R}[[X]]^{m\times 1}$, *if we define* $f_{\overline{g}}(X) := p\eta^{-1} * \overline{g}(X)$, *then*

$f_g^{-1}(f_{\overline{g}}(X)) \in R[[X]]^{m\times 1}$.

(*c*) (*converse to* (*b*)) *For every* $h(X) \in R[[X]]^{m\times 1}$ *such that* $h(0) = 0$, *there exists* $\hat{h}(X) \in R[[X]]^{m\times 1}$ *such that* $h(X) = f_g^{-1}(f_{\hat{h}}(X))$, *where* $f_{\hat{h}}(X) := \eta^{-1} * \hat{h}(X)$.

(*d*) *If* $\alpha(X), \beta(X) \in K[[X]]^{m\times 1}$, *and at least one of them is in* $R[[X]]^{m\times 1}$, *then for every positive integer* r, $f_g(\alpha(X)) \equiv f_g(\beta(X)) \mod \mathfrak{a}^r$ *if and only if* $\alpha(X) \equiv \beta(X) \mod \mathfrak{a}^r$.

Remark 10.2.5. If the triple $(R, \mathfrak{a}, \sigma)$ does not satisfy the condition (3) in the definition of Honda ring (10.2.1), but $s_1, s_2, \cdots \in K^{m\times m}$ satisfies $\sigma^r(s_k(i,j))\mathfrak{a} \subset R$ for all $r, k = 1, 2, \cdots$ and $i, j = 1, 2, \cdots, m$, then the functional equation lemma (10.2.4) still holds; see [8] (2.4.15).

The formal group law F_g over R defined in (a) of the proposition will be called *of functional equation type*, due to the fact that $f_g(X)$ satisfies the following functional equation:

$$f_g(X) = g(X) + \sum_{i=1}^{\infty} s_i \sigma_*^i f_g(X)$$

Proposition 10.2.6. ([8]20.1.3) *If* R *is a* $\mathbb{Z}_{(p)}$*-algebra* $\mathfrak{a} = (p)$ *in a Honda ring* $(R, \mathfrak{a}, \sigma)$, *then every formal group law over* R *is of functional equation type.*

10.3 Universal formal group laws

If F is an m-dimensional formal group law over R, and $\phi : R \to R'$ is a ring homomorphism, then the pushforward of F via ϕ is a formal group law over R',

and we denote it by $\phi_* F$. It is a trivial matter to see the existence of a universal (m-dimensional) formal group law over some ring L, such that for every ring R and every m-dimensional formal group law F over R, there exists a unique homomorphism $\phi : L \to R$ making F the pushforward of the universal formal group law via ϕ. We sketch the argument here. Let $\tilde{L} := \mathbb{Z}[\cdots, C_{i,\mathbf{a},\mathbf{b}}, \cdots; i = 1, 2, \cdots, m, \mathbf{a}, \mathbf{b} \in \mathbb{N}^m]$ where $C_{i,\mathbf{a},\mathbf{b}}$ are indeterminates. Consider the m-tuple of formal power series $F_C(X, Y) = (F_{C,1}(X, Y), \cdots, F_{C,m}(X, Y))$ where $F_{C,i}(X, Y) = X_i + Y_i + \sum C_{i,\mathbf{a},\mathbf{b}} X^{\mathbf{a}} Y^{\mathbf{b}}$, then the identities in the definition of formal group laws yield infinitely many equations among the indeterminates C_{ij}. Let $\mathfrak{a}$ be the ideal of $\tilde{L}$ generated by these equations, then the induced formal group law from F_C over $L := \tilde{L}/\mathfrak{a}$ is a universal formal group law. However, it was Lazard who first proved in the one-dimensional case that the structure of the ring L is incredibly simple:

Theorem 10.3.1. (*Lazard*) *When $m = 1$, L is isomorphic to the polynomial ring $\mathbb{Z}[x_1, x_2, \cdots]$.*

Making use of the functional equation lemma, Hazewinkel gave explicit constructions of m-dimensional universal formal group laws $H_U(X, Y)$ over polynomial rings with countably infinitely many indeterminates. We first make some notations that will be used in the definition of H_U (see [8] §11):

- For each sequence $(q_1, \cdots, q_t)$, $t \in \mathbb{N}^*$, of powers of prime numbers, $q_i = p_i^{s_i}$, $s_i \in \mathbb{N}$, p_i a prime number, choose an integer $n(q_1, \cdots, q_t)$ such that the

following congruences are satisfied:

$$n(q_1, \cdots, q_t) \equiv 1 \mod p_1^r \qquad \text{if } p_1 = p_2 = \cdots = p_r \neq p_{r+1}, \quad 1 \leq r \leq t$$

$$n(q_1, \cdots, q_t) \equiv 1 \mod p_2^{r-1} \qquad \text{if } p_1 \neq p_2 = \cdots = p_r \neq p_{r+1}, \quad 2 \leq r \leq t$$

If $r = t$, then the coniditon $p_r \neq p_{r+1}$ is supposed to be vacuously satisfied. We further require that $n(q_1, \cdots, q_t) = 1$ if $p_1 = p_2 = \cdots = p_t$; note that this definition satisfies the congruences above.

- Denote by $\mathbf{n}$ the m-tuple of natural numbers $\mathbf{n} = (n_1, \cdots, n_m)$, $n_i \in \mathbb{N}$.
- Define $|\mathbf{n}| := n_1 + \cdots + n_m$ for $\mathbf{n} = (n_1, \cdots, n_m)$.
- Define $\mathbf{0} := (0, 0, \cdots, 0)$, $\mathbf{e}(i) = (0, \cdots, 0, 1, 0, \cdots, 0)$ with the only 1 in the i-th place.
- If $\mathbf{n}$ is an m-tuple of natural numbers and $i \in \mathbb{N}$, then $i\mathbf{n}$ is defined to be $(in_1, \cdots, in_m)$.
- Denote by $\mathbf{I}$ the set of all m-tuple of natural numbers $\mathbf{n}$, by $\mathbf{D}$ the set of all m-tuples of natural numbers $\mathbf{n}$ for which $\mathbf{n} \neq \mathbf{0}$ and $\mathbf{n} \neq p^r\mathbf{e}(i)$ for all prime numbers p and $r \geq 1$. Note that the indices $\mathbf{e}(i)$ themselves, $i = 1, 2, \cdots, m$, are in $\mathbf{D}$.
- If $\mathbf{n} = (n_1, \cdots, n_m) \in \mathbf{I}$, denote $X_1^{n_1} \cdots X_m^{n_m}$ by $X^{\mathbf{n}}$. If $a = (a_1, \cdots, a_m)^t$ is a column vector, then $aX^{\mathbf{n}}$ is short for the vector $(a_1X^{\mathbf{n}}, \cdots, a_mX^{\mathbf{n}})^t$.
- Denote by X the column vector $(X_1, X_2, \cdots, X_m)^t$, by X^{p^n} the column vector $(X_1^{p^n}, X_2^{p^n}, \cdots, X_m^{p^n})^t$.

- If A is a matrix, we denote the matrix obtained by raising each entry to its p^n-th power by $A^{(p^n)}$ to distinguish from A^{p^n}, the p^n-th power in the usual sense of matrix multiplications.

- Let $\tilde{\mathcal{R}}^\infty := \mathbb{Z}[U]$ be short for $\mathbb{Z}[U(i,\mathbf{n})|n \in \mathbf{I}, |\mathbf{n}| \geq 2, i = 1, \cdots, m]$. Define $U(i, \mathbf{e}(j)) = 0$ if $i \neq j$ and $U(i, \mathbf{e}(i)) = 1$ for $i, j = 1, 2, \cdots, m$.

- Define $\sigma : \tilde{\mathcal{R}}^\infty \to \tilde{\mathcal{R}}^\infty$ by fixing $\mathbb{Z}$ and sending $U(i,\mathbf{n})$ to $U(i,\mathbf{n})^p$. The triple $(\tilde{\mathcal{R}}^\infty, (p), \sigma)$ is a Honda ring.

- If $q = p^s$, $s \in \mathbb{N}$, p is a prime number, then denote by U_q the $m \times m$ matrix $U(i, q\mathbf{e}(j))_{i,j}$.

- If $\mathbf{d} \in \mathbf{I}\backslash\{\mathbf{0}\}$, denote by $U_\mathbf{d}$ the column vector $(U(1,\mathbf{d}), \cdots, U(m,\mathbf{d}))$.

Definition 10.3.2. For each $\mathbf{n} \in \mathbf{I}$ with $|\mathbf{n}| \geq 1$, define a column vector $a_\mathbf{n}$ with entries in $\mathbb{Q}[U] = \mathbb{Q} \otimes \mathbb{Z}[U]$ by means of the formula

$$a_\mathbf{n}(U) = \sum_{(q_1,\cdots,q_t,\mathbf{d})} \frac{n(q_1,\cdots,q_t)}{p_1} \cdots \frac{n(q_{t-1},q_t)}{p_{t-1}} \frac{n(q_t)}{p_t} U_{q_1} U_{q_2}^{(q_1)} \cdots U_{q_t}^{(q_1\cdots q_{t-1})} U_\mathbf{d}^{(q_1\cdots q_t)}$$

where the sum is over all $q_1, q_2, \cdots, q_t$ which are powers of prime numbers and $\mathbf{d} \in \mathbf{D}$ such that $\mathbf{n} = q_1 q_2 \cdots q_s \mathbf{d}$.

Define $h_U(X) := \sum_{|\mathbf{n}|\geq 1} a_\mathbf{n}(U) X^\mathbf{n}$, $H_U(X,Y) = h_U^{-1}(h_U(X) + h_U(Y))$.

Proposition 10.3.3. ([8] 11.2.4) *The m-tuple of formal power series $h_U(X,Y)$ satisfies a functional equation of the form*

$$h_U(X) = g_p(X) + \sum_{i=1}^{\infty} p^{-1} U_{p^i} h_U^{(p^i)}(X^{p^i})$$

with $g_p(X) \in \mathbb{Z}_{(p)}[U][[X]]^m$ *and* $g_p(X) \equiv X \mod \deg \geq 2$ *for every prime* p.

As a corollary of (10.2.4), $H_U(X,Y)$ is a formal group law over $\tilde{\mathcal{R}}^\infty$.

Proposition 10.3.4. ([8]11.1.5) *$H_U(X,Y)$ is a universal m-dimensional formal group law over $\tilde{\mathcal{R}}^\infty$, i.e., for every ring R and every m-dimensional formal group law $F(X,Y)$ over R, there exists a unique homomorphism $\phi : \tilde{\mathcal{R}}^\infty \to R$ such that $F = \phi_* H_U$.*

In §10, Hazewinkel also constructed another formal group law which is important in studying formal group laws over $\mathbb{Z}_{(p)}$-algebras. Let $\mathcal{R}^\infty := \mathbb{Z}[V]$ be short for $\mathbb{Z}[V_i(j,k); i = 1, 2, \cdots; j, k = 1, 2, \cdots, m]$, and let $\mathcal{K}^\infty := \mathbb{Q}[V]$. Write V_i for the $m \times m$ matrix $(V_i(j,k))$. Define $\sigma : \mathcal{R}^\infty \to \mathcal{R}^\infty$ by sending $V_i(j,k)$ to $V_i(j,k)^p$ and fixing $\mathbb{Z}$. The triple $(\mathcal{R}^\infty, (p), \sigma)$ is a Honda ring. Define $\eta_V := p - \sum_{i=1}^{\infty} V_i \partial^i \in \mathcal{K}_\sigma^\infty[[X]]^{m\times m}$, $f_V(X) := p\eta_V^{-1} * X$, and $F_V(X,Y) := f_V^{-1}(f_V(X) + f_V(Y))$. By (10.2.4), F_V is an m-dimensional formal group law over $\mathcal{R}^\infty$.

Definition 10.3.5. We call F_V the (m-dimensional) *universal p-typical formal group law*. In general, a formal group law F over R is called *p-typical*, if there exists a homomorphism $\phi : \mathcal{R}^\infty \to R$ such that $F = \phi_* F_V$; the infinite sequence of matrices $\phi(V_1), \phi(V_2), \cdots$ is called the *p-typical coordinate* of F.

It can be easily computed that:

Proposition 10.3.6. ([8]§10.4) *If we denote $f_V(X) = \sum_{n=0}^{\infty} a_n(V) X^{p^n}$, then:*

(a) $a_n(V) = \frac{1}{p} \sum_{i=1}^{n} V_i a_{n-i}(V)^{(p^i)} = \frac{1}{p} \sum_{i=1}^{n} a_{n-i}(V) V_i^{(p^{n-i})}$.

(b) $a_n(V) = \sum_{i_1+i_2+\cdots+i_r=n} p^{-t} V_{i_1} V_{i_2}^{(p^{i_1})} \cdots V_{i_r}^{(p^{i_1+\cdots+i_{r-1}})}$.

Proposition 10.3.7. *(a) The unique homomorphism $\varphi : \tilde{\mathcal{R}}^\infty \to \mathcal{R}^\infty$ such that $\varphi_* H_U = F_V$ is defined by $\varphi(U(i,\mathbf{n})) = V_s(i,j)$ if $\mathbf{n} = p^s\mathbf{e}(j)$, and $\varphi(U(i,\mathbf{n})) = 0$ otherwise.*

(b) Let $\kappa : \mathcal{R}^\infty \to \tilde{\mathcal{R}}^\infty$ be the homomorphism such that $\kappa(V_s(i,j)) := U(i, p^s\mathbf{e}(j))$. For every p-typical formal group law F over a ring R, if $\phi : \mathcal{R}^\infty \to R$ and $\tilde{\phi} : \tilde{\mathcal{R}}^\infty \to R$ are the homomorphisms such that $\phi_* F_V = \tilde{\phi}_* H_U = F$, then $\phi = \tilde{\phi} \circ \kappa$.

Proof. Part (a) can be easily seen by (10.3.2) and (10.3.6), since $\varphi(a_{\mathbf{n}}(U)) = a_s(V(\cdot, j))$ if $n = p^s\mathbf{e}(j)$, and $(0, 0, \cdots, 0)^t$ if otherwise. Part (b) follows from the fact that $\varphi \circ \kappa = \mathrm{Id}$. □

Proposition 10.3.8. *Let $\tilde{\mathcal{R}}^\infty_{(p)}$ be the localization of $\tilde{\mathcal{R}}^\infty$ at p. There exists a strict isomorphism $\varsigma : H_U \to \kappa_* F_V$ over $\tilde{\mathcal{R}}^\infty_{(p)}$. Moreover, $\varsigma(X) \equiv X \mod \tilde{\mathfrak{a}}$, where $\tilde{\mathfrak{a}}$ is the ideal of $\tilde{\mathcal{R}}^\infty_{(p)}$ generated by $U(i,\mathbf{n})$ with $\mathbf{n}$ running over all m-tuple of natural integers that are not of the form $p^s\mathbf{e}(j)$.*

Proof. The logarithm of H_U is $h_U(X) = (p\eta_U^{-1}) * g_p(X)$, where $\eta_U = p - \sum_{i=1}^{\infty} U_{p^i}\partial^i$, and $g_p(U) \in \tilde{\mathcal{R}}^\infty_{(p)}$ as in (10.3.3). The logarithm of $\kappa_* F_V$ is $\kappa_* f_V(X) = (p\eta_U)^{-1}) * X$, hence $\varsigma(X) = \kappa_* f_V^{-1}(h_U(X))$ is a strict isomorphism between H_U and $\kappa_* F_V$ over $\tilde{\mathcal{R}}^\infty_{(p)}$ by (10.3.3 (b)). For the second statement, note that $\kappa_* f_V(X)$ and $h_U(X)$ are formal power series over $\tilde{\mathcal{R}}^\infty[\frac{1}{p}]$. Their pushforwards over the quotient ring $(\tilde{\mathcal{R}}^\infty/\tilde{\mathfrak{a}})[\frac{1}{p}]$ satisfy the same functional equation, hence are equal to each other. Therefore $\varsigma(X)$ is congruent to X modulo $\tilde{\mathfrak{a}}$. □

Note that $f_V(X) = \sum_{n=0}^{\infty} a_n(V)X^{p^n}$ is obtained from $h_U(X) = \sum_{|\mathbf{n}|\geq 1} a_{\mathbf{n}}(U)X^{\mathbf{n}}$ by striking out all terms that should not occur in the logarithm of a p-typical formal group law. Because of the universality of F_V and H_U, it provides a universal way to "p-typify" a formal group law.

Definition 10.3.9. Let R be a $\mathbb{Z}_{(p)}$-algebra, F be an m-dimensional formal group law over R. Let $\tilde{\phi} : \tilde{\mathcal{R}}^{\infty}_{(p)} \to R$ be the homomorphism such that $F = \tilde{\phi}_* F_U$. Let $\kappa_{(p)} : \mathcal{R}^{\infty}_{(p)} \to \tilde{\mathcal{R}}^{\infty}_{(p)}$ be the homomorphism induced by κ after localizing at p. Define *the p-typification of* F to be $\phi_* F_V$, where $\phi = \tilde{\phi} \circ \kappa_{(p)} : \mathcal{R}^{\infty}_{(p)} \to R$.

Corollary 10.3.10. *Every formal group law over a $\mathbb{Z}_{(p)}$-algebra is strictly isomorphic to its p-typification, which in particular is a p-typical formal group law.*

In the case when $\operatorname{char} R = 0$, we can have an equivalent characterization of p-typical formal group laws via logarithm:

Proposition 10.3.11. ([8]15.2.6) *If* $\operatorname{char} R = 0$*, a formal group law F over R is p-typical if and only* $\log_F(X)$ *is of the form* $\log_F(X) = \sum_{n=0}^{\infty} a_n X^{p^n}$*, where* $a_n \in (R \otimes \mathbb{Q})^{m \times m}$.

10.4 Isomorphisms and homomorphisms between p-typical formal group laws

Not only the p-typical formal group laws themselves are parametrized by infinitely many free indeterminates, but so are the strict isomorphisms between them, too.

Let $\mathcal{R}^{\infty,\infty} := \mathbb{Z}[V,T]$ be short for $\mathbb{Z}[V_i(j,k), T_i(j,k); i = 1,2,\cdots; j,k = 1,2,\cdots,m]$, and $\mathcal{K}^{\infty,\infty} := \mathbb{Q}[V,T]$. Similar to the previous notation of V_i, let T_i stand for the $m \times m$ matrix $(T_i(j,k))$. Extend $\sigma : \mathcal{K}^{\infty} \to \mathcal{K}^{\infty}$ to $\mathcal{R}^{\infty,\infty} \to \mathcal{R}^{\infty,\infty}$ by defining $\sigma(T_i(j,k)) := T_i(j,k)^p$. The triple $(R^{\infty,\infty}, (p), \sigma)$ is a Honda ring, and the natural inclusion $R^{\infty} \hookrightarrow R^{\infty,\infty}$ is an embedding between Honda rings. Define $\eta_V := p - \sum_{i=1}^{\infty} V_i \partial^i \in \mathcal{K}_{\sigma}^{\infty}[[X]]^{m\times m}$, $f_{V,T}(X) := p\eta_V^{-1} * (X + \sum_{i=1}^{\infty} T_i X^{p^i})$, and $F_{V,T}(X,Y) := f_{V,T}^{-1}(f_{V,T}(X) + f_{V,T}(Y))$. Define $\alpha_{V,T}(X) := f_{V,T}^{-1}(f_V(X))$. By (10.2.4), $F_{V,T}$ is an m-dimensional formal group law over $\mathcal{R}^{\infty,\infty}$, and $\alpha_{V,T}$ is a strict isomorphism from F_V to $F_{V,T}$.

Proposition 10.4.1. ([8]19.2.6) *The triple $(F_V(X,Y), \alpha_{V,T}(X), F_{V,T}(X,Y))$ over $\mathcal{R}^{\infty,\infty}$ is universal for triples $(F(X,Y), \alpha(X), G(X,Y))$ consisting of two p-typical (m-dimensional) formal group laws $F(X,Y)$, $G(X,Y)$, and a strict isomorphism $\alpha(X) : F(X,Y) \to G(X,Y)$ over $\mathbb{Z}_{(p)}$-algebras or characteristic zero rings .*

In other words, if $\alpha(X) : F(X,Y) \to G(X,Y)$ is a strict isomorphism between p-typical formal group laws over a ring R, which is a $\mathbb{Z}_{(p)}$-algebra or characteristic zero ring, then there is a unique homomorphism $\phi : \mathcal{R}^{\infty,\infty} \to R$ such that $\phi_* F_V = F, \phi_* F_{V,T} = G$, and $\phi_* \alpha_{V,T} = \alpha$.

In the rest of this section we describe formulas of the logarithms of $F_{V,T}$.

Proposition 10.4.2. ([8]§10.4) *Denote*

$$f_V(X) := \sum_{n=0}^{\infty} a_n(V) X^{p^n}, f_{V,T}(X) := \sum_{n=0}^{\infty} a_n(V,T) X^{p^n}$$

Then

$$pa_n(V,T) = T_n + \sum_{i=1}^{n} V_i a_{n-i}(V,T)^{(p^i)} = T_n + \sum_{i=1}^{n} a_{n-i}(V,T) V_i^{(p^{n-i})}$$

By the definition of $f_{V,T}$ and (10.3.11), $F_{V,T}$ is also a p-typical formal group law. Due to the universality of F_V, there exists a unique homomorphism $\xi : \mathcal{R}^\infty \to \mathcal{R}^{\infty,\infty}$ such that $F_{V,T} = \xi_* F_V$. Denote the image of V_n under ξ by $\overline{V}_n$; there exist polynomials $\Phi_n^{(r,s)}(x_i(j,k), y_i(j,k); 1 \le i \le n, 1 \le j,k \le m)$ for $1 \le r,s \le m$ such that $\overline{V}_n(r,s) = \Phi_n^{(r,s)}(V_i(j,k), T_i(j,k); 1 \le i \le n, 1 \le j,k \le m)$. For simplicity we write $\overline{V}_n = \Phi_n(V_i, T_i; 1 \le i \le n)$.

By the definition of $\overline{V}_n$ we have the following equation:

$$pa_n(V,T) = \sum_{i=1}^{n} a_{n-i}(V,T) \overline{V}_i^{(p^{n-i})}$$

There exists a recursive formula for $\overline{V}_i$ based on V and T:

Proposition 10.4.3. ([8]19.3.7)

$$\begin{aligned}\overline{V}_n &= V_n + pT_n + \sum_{\substack{i+j=n \\ i,j\ge 1}} (V_i T_j^{(p^i)} - T_j \overline{V}_i^{(p^i)}) + \sum_{k=1}^{n-1} a_{n-k}(V)(V_k^{(p^{n-k})} - \overline{V}_k^{(p^{n-k})}) \\ &\quad + \sum_{k=2}^{n-1} a_{n-k}(V)[\sum_{\substack{i+j=k \\ i,j\ge 1}} (V_i^{(p^{n-k})} T_j^{(p^{n-j})} - T_j^{(p^{n-k})} \overline{V}_i^{(p^{n-i})})]\end{aligned}$$

Remark 10.4.4. This recursive formula is not directly applicable if we want a formula of $\overline{V}_n$ modulo p, since the formula of $a_i(V)$ involves a high power of p in denominator (10.3.6(b)).

For the rest of the subsection, we suppose $(R, \mathfrak{a}, \sigma)$ is a Honda ring where $\mathfrak{a} = (p)$ is the principal ideal generated by p. Under such assumptions on R, all p-typical

formal group laws over R are of functional equation type in the following form (c.f. 10.2.6):

Proposition 10.4.5. ([8]20.1.5) *Let $F(X,Y)$ be a p-typical formal group law over R, then there exist unique matrices $v_1, v_2, \cdots \in R^{m\times m}$ such that $\log_F(X) = p\eta^{-1} * X$, where $\eta := p - \sum_{i=1}^{\infty} v_i \partial^i$. In other words, the logarithm of $F(X,Y)$ satisfies the functional equation*

$$\log_F(X) = X + \sum_{i=1}^{\infty} \frac{v_i}{p} \sigma_*^i \log_F(X)$$

Remark 10.4.6. Comparing to (10.2.6), we are not requiring R to be a $\mathbb{Z}_{(p)}$-algebra in (10.4.5) and we have stronger conclusion on the functional equation that $F(X,Y)$ satisfies; this is due to the stronger assumption that $F(X,Y)$ is p-typical.

Definition 10.4.7. Suppose $(R, \mathfrak{a}, \sigma)$ is a Honda ring where $\mathfrak{a} = (p)$ is the principal ideal generated by p. Let F be an m-dimensional p-typical formal group law over R. The sequence of matrices $v_1, v_2, \cdots \in R^{m\times m}$ determined by (10.4.5) is called the *Honda coordinate* of F.

It is easy to see that if $v_1, v_2, \cdots \in R^{m\times m}$ is the Honda coordinate of F, then $\log_F(X) = \sum_{n=0}^{\infty} a_n X^{p^n}$, where $a_n = \sum_{i_1+i_2+\cdots+i_r=n} p^{-t} v_{i_1} v_{i_2}^{\sigma^{i_1}} \cdots v_{i_r}^{\sigma^{i_1+\cdots+i_{r-1}}}$, satisfying the recursive relation $a_n = \frac{1}{p}\sum_{i=1}^{n} v_i a_{n-i}^{\sigma^i} = \frac{1}{p}\sum_{i=1}^{n} a_{n-i} v_i^{\sigma^{n-i}}$ (c.f. 10.3.6).

Under our assumption on R, there exist concrete descriptions on the homomorphisms between p-typical formal group laws in terms of their Honda coordinates.

Proposition 10.4.8. ([8]20.3.9, 20.3.10, 20.4.4) *Let $u = (u_1, u_2, \cdots)$ be a sequence of elements in $R^{m\times m}$ and $v = (v_1, v_2, \cdots)$ be a sequence of elements in $R^{n\times n}$. Denote*

$p - \sum u_i \partial^i$ and $p - \sum v_i \partial^i$ by η_u and η_v, respectively. Let $F(X,Y)$ and $G(X,Y)$ be formal group laws with logarithms

$$f(X) = p\eta_u^{-1} * X, g(X) = p\eta_v^{-1} * X$$

(a) There exists a homomorphism $\alpha : F \to G$ over R if and only if there exists $c \in R^{n\times m}$ and $\theta_c \in R_\sigma[[\partial]]^{n\times m}$ such that $\eta_v c = \theta_c \eta_u$.

(b) F and G are strictly isomorphic if and only if $m = n$ and there exists an element $\xi \in R_\sigma[[\partial]]^{m\times m}$ such that $\eta_u \xi = \theta_v$.

(c) For an arbitrary $\theta \in R_\sigma[[\partial]]^{n\times m}$, set $\alpha_\theta(X) = g^{-1}((\theta * f)(X))$. Then $\alpha_\theta(X) \in R[[X]]^m$ if and only if there exists an $\eta_\theta \in R_\sigma[[\partial]]$ such that $\eta_\theta \eta_u = \eta_v \theta$. If $\alpha_\theta(X) \in R[[X]]^m$, then $\overline{\alpha}_\theta : \overline{F} \to \overline{G}$ is a homomorphism after modulo p, where $\overline{F}, \overline{G}$ stand for the induced formal group laws over R/pR.

(d) When $m = n$ and $F = G$, we have the following ring isomorphism:

$$\begin{aligned} \{\theta \in R_\sigma[[\partial]]^{m\times m} | \eta_u \theta \eta_u^{-1} \in R_\sigma[[\partial]]^{m\times m}\}/R_\sigma[[\partial]]^{m\times m}\eta_u &\xrightarrow{1\text{-}1} \quad \mathrm{End}(\overline{F}) \\ \theta &\mapsto \overline{f^{-1}(\theta * f(X))} \end{aligned}$$

10.5 Cartier theory

Let R be a commutative ring with 1.

Definition 10.5.1. (a) Let G be a formal group over R. A *curve* in G is an element in $G(XR[[X]])$, where $XR[[X]]$ is viewed as a pro-nilpotent R-algebra. The set of curves in G form an abelian group, which is denoted by $\mathcal{C}(G; R)$.

(b) Let $F(X,Y)$ be an m-dimensional (resp. countably infinite dimensional) formal group law over R. A *curve* in F is an m-tuple (resp. countably infinite tuple) of power series $\gamma(t)$ in one variable t with coefficients in R such that $\gamma(0)=0$. Under the addition defined by $\gamma_1(t)+_F\gamma_2(t):=F(\gamma_1(t),\gamma_2(t))$, the set of curves in F becomes an abelian group, which is denoted by $\mathcal{C}(F;R)$. Let $\delta_i(t)$ be the curve $(0,\cdots,0,t,0,\cdots)$ which is t on the i-th component and zero elsewhere.

Remark 10.5.2. If $G\cong \operatorname{Spf} R[[X_1,X_2,\cdots,X_m]]$, and the group structure on G is induced from the formal group law $F(X,Y)$, then $\mathcal{C}(G;R)$ is isomorphic to $\mathcal{C}(F;R)$ as abelian groups.

The curves $\mathcal{C}(G;R)$ (resp. $\mathcal{C}(F;R)$) can be identified as homomorphisms form a free generator of the category of formal groups (resp. formal group laws) to G, as follows:

Definition 10.5.3. Define $\Lambda=\Lambda_R:\mathfrak{Nip}\to\mathfrak{Ab}$ such that for every nipotent R-algebra N, $\Lambda(N)=1+tR[t]\otimes_R N\subset (R\oplus N[t])^\times$, equipped with the group structure as multiplication in $(R\oplus N[t])^\times$.

Definition 10.5.4. For $n=1,2,\cdots$, define a series of polynomials

$$w_n(X)=w_n(X_1,X_2,\cdots,X_n)$$

with coefficients in $\mathbb{Z}$ as $w_n(X):=\sum_{d|n} dX_d^{\frac{n}{d}}$.

The following proposition is classical.

Proposition 10.5.5. *There exist polynomials with coefficients in* $\mathbb{Z}$ *as* $\Sigma_1, \Sigma_2, \cdots$*;* $\prod_1, \prod_2, \cdots$*;* $\iota_1, \iota_2, \cdots$ *such that*

$$w_n(\Sigma) = w_n(X) + w_n(Y), \;\; w_n(\prod) = w_n(X)w_n(Y), \;\; w_n(\iota) = -w_n(X)$$

Definition 10.5.6. (a) Define $\widehat{W} = \widehat{W}_R(X, Y)$ be the infinite dimensional formal group law over R via the sequence of power series $\Sigma_1, \Sigma_2, \cdots$. We abuse the notation to denote the formal group associated to the formal group law $\widehat{W}_R(X, Y)$ by $\widehat{W}$, too.

(b) Define the curve γ_w in $\widehat{W}$ by $\gamma_w(t) := \delta_1(t)$. Define $(\mathbf{f}_n\gamma_w)(t) := \delta_n(t)$, $(\mathbf{v}_n\gamma_w)(t) := \gamma_w(t^n)$, and $(c\gamma_w)(t) := \gamma_w(ct)$ for $c \in R$.

The following proposition is left as an exercise.

Proposition 10.5.7. *The formal group* $\widehat{W}$ *is isomorphic to* Λ *via*

$$\begin{aligned} E_N : \;\; \widehat{W}(N) \;\; &\to \;\; \Lambda(N) \\ (a_1, a_2, \cdots) \;\; &\mapsto \;\; (1 - a_1 t)(1 - a_2 t^2) \cdots \end{aligned}$$

where all but finitely many $a_i = 0$ *for every* $N \in \mathfrak{ProNil}_R$.

Proposition 10.5.8. (*Cartier-Dieudonné*) *Let* G *be an* m*-dimensional smooth formal group over* R*, and* $F(X, Y)$ *be a formal group law attached to* G*. There exists the following commutative diagrams*

$$\begin{array}{ccc} Hom(\Lambda, G) & \xrightarrow[\cong]{Y_G} & \mathcal{C}(G; R) \\ \downarrow \cong & & \downarrow \cong \\ Hom(\widehat{W}, F) & \xrightarrow[\cong]{Y_F} & \mathcal{C}(F; R) \end{array}$$

where $Y_G(\alpha) := \alpha(1 - Xt)$ *for* $\alpha \in Hom(\Lambda, G)$, *and* $Y_F(\beta) := \beta(\gamma_w)$ *for* $\beta \in Hom(\widehat{W}, F)$.

Definition 10.5.9. Define the *Cartier ring* over R as $\mathrm{Cart}(R) := \mathrm{End}(\Lambda)^{\mathrm{opp}} \cong \mathrm{End}(\widehat{W})^{\mathrm{opp}}$. We define some special elements in the Cartier ring $\mathrm{Cart}(R)$ via the isomorphisms Y_Λ and $Y_{\widehat{W}}$ defined in (10.5.8):

$$V_n := Y_\Lambda^{-1}(1 - X^n t) = Y_{\widehat{W}}^{-1}(\mathbf{v}_n \gamma_w), F_n := Y_\Lambda^{-1}(1 - Xt^n) = Y_{\widehat{W}}^{-1}(\mathbf{f}_n \gamma_w)$$

$$[c] := Y_\Lambda^{-1}(1 - cXt) = Y_{\widehat{W}}^{-1}(c\gamma_w)$$

where $c \in R$.

In the explicit terms of curves in a formal group law $F(X, Y)$ of G, the $V_n, F_n, [c]$ defined above can be viewed as operators on $\mathcal{C}(F(X, Y); R)$ in the following way. The operator V_n sends a curve $\gamma(t)$ to $\gamma(t^n)$, and $[c]$ sends a curve $\gamma(t)$ to $\gamma(ct)$. The definition of F_n is slightly complicated: Denote by $R[\xi_n]$ the R-algebra $R[U]/(U^n - 1)$, and let $\xi = \xi_n$ be the image of U in $R[U]/(U^n - 1)$. Denote by $R[\xi][[t^{\frac{1}{n}}]]$ the R-algebra $R[\xi][[T]]/(T^n - t)$, and let $t^{\frac{1}{n}}$ be the image of T in $R[\xi][[T]]/(T^n - t)$. Then $F_n(\gamma(t))$ can be defined as $\gamma(t^{\frac{1}{n}}) +_F \gamma(\xi t^{\frac{1}{n}}) +_F \gamma(\xi^2 t^{\frac{1}{n}}) +_F \cdots +_F \gamma(\xi^{n-1} t^{\frac{1}{n}})$, and one can show that $F_n(\gamma(t)) \in R[[t]]^{m\times 1} \subset R[\xi][[t^{\frac{1}{n}}]]^{m\times 1}$.

Proposition 10.5.10. ([24] 3.13) (*The structure of Cartier ring*)

The elements in $\mathrm{Cart}(R)$ *can be uniquely written in the form* $\sum_{i,j\geq 1} V_i[c_{ij}]F_j$, $c_{ij} \in R$. *The following identities hold in* $\mathrm{Cart}(R)$*:*

(*1*) $V_1 = F_1 = 1, F_i V_i = i$.

(2) $[a][b] = [ab]$, *for* $a, b \in R$.

(3) $[c]V_i = V_i[c^i]$, $F_i[c] = [c^i]F_i$, *for all* $c \in R$, $i \geq 1$.

(4) $V_jV_i = V_iV_j = V_{ji}$, $F_jF_i = F_iF_j = F_{ji}$, *for all* $i, j \geq 1$.

(5) $F_jV_i = V_iF_j$, *if* $(i, j) = 1$.

(6) $(V_i[a]F_i)(V_j[b]F_j) = rV_{\frac{ij}{r}}[a^{\frac{i}{r}}b^{\frac{j}{r}}]F_{\frac{ij}{r}}$, $r = (i, j)$, *for all* $i, j \geq 1$, $a, b \in R$.

The curves $\mathcal{C}(G; R)$ (resp. $\mathcal{C}(F, R)$) thus become a left $\mathrm{Cart}(R)$-module, which will be called as the *Cartier module* of formal group G (resp. formal group law F).

Definition 10.5.11. A *V-reduced* $\mathrm{Cart}(R)$-module is a left $\mathrm{Cart}(R)$-module M that is equipped with a decreasing filtration:

$$M = \mathrm{Fil}^1 M \supset \mathrm{Fil}^2 M \supset \cdots \supset \mathrm{Fil}^n M \supset \mathrm{Fil}^{n+1} M \supset \cdots$$

such that each $\mathrm{Fil}^n M$ is an abelian group, and:

(1) $(M, \mathrm{Fil}^\bullet M)$ is separated and complete with respect to the topology defined by the filtration $\mathrm{Fil}^\bullet M$. In other words, the natural map $\mathrm{Fil}^n M \to \varprojlim_{i \geq n} \mathrm{Fil}^n M/\mathrm{Fil}^i M$ is an isomorphism.

(2) $V_i\mathrm{Fil}^n M \subset \mathrm{Fil}^{in} M$.

(3) The map V_i induces a bijection $V_i : M/\mathrm{Fil}^2 M \xrightarrow{\sim} \mathrm{Fil}^i/\mathrm{Fil}^{i+1} M$ for all $n \geq 1$.

(4) $[c]\mathrm{Fil}^n M \subset \mathrm{Fil}^n M$ for all $c \in R$, $n \geq 1$.

(5) For every $i, j \geq 1$, there exists an $r \geq 1$ such that $F_i\mathrm{Fil}^r M \subset \mathrm{Fil}^n M$.

The *tangent space* of a V-reduced $\mathrm{Cart}(R)$-module M is defined to be the R-module $M/\mathrm{Fil}^1 M$, denoted by t_M.

Remark 10.5.12. (a) As an example, the rank 1 free left $\mathrm{Cart}(R)$-module $\mathrm{Cart}(R)$ has a filtration with $\mathrm{Fil}^n\mathrm{Cart}(R) = \{\sum_{i\geq n, j\geq 1} V_i[c_{ij}]F_j | c_{ij} \in R\}$, and all the conditions above are satisfied.

(b) If a V-reduced $\mathrm{Cart}(R)$-module M is finitely generated, then $\mathrm{Fil}^n M = \mathrm{Fil}^n\mathrm{Cart}(R) \cdot M$.

Definition 10.5.13. A V-reduced $\mathrm{Cart}(R)$-module M is said to be *V-flat*, if t_M is a flat R-module.

Proposition 10.5.14. (*The Main Theorem of Cartier Theory*)

(*a*) *There is a canonical equivalence between the category of formal groups over R and the category of V-flat V-reduced left Cart(R)-modules, defined as follows:*

$$\begin{array}{ccc} \{\textit{formal groups over } R\} & \xrightarrow{\sim} & \{V\textit{-flat } V\textit{-reduced Cart}(R)\textit{-modules}\} \\ G & \mapsto & \mathcal{C}(G;R) \end{array}$$

where the filtration on $\mathcal{C}(G;R) \cong XR[[X]]$ is induced from the natural filtration $XR[[X]] \supset X^2R[[X]] \supset \cdots$.

(*b*) *Under the equivalence in (a), the full subcategory of m-dimensional smooth formal groups over R is equivalent to the full subcategory of V-flat V-reduced left Cart(R)-modules M such that $M/Fil^2M \cong R^m$.*

(*c*) *The category of m-dimensional formal group laws over R is equivalent to the category of V-flat V-reduced left Cart(R)-modules M equipped with an isomorphism $M/Fil^2M \xrightarrow{\cong} R^m$, via $F(X,Y) \mapsto \mathcal{C}(F;R)$, where the filtration $Fil\mathcal{C}(F;R)$ on $\mathcal{C}(F;R)$ is defined such that $Fil^n\mathcal{C}(F;R)$ consists of curves $(\gamma_1(t), \gamma_2(t), \cdots, \gamma_m(t))$*

with $ord_t\gamma_i \geq n$ *for* $i = 1, 2, \cdots, m$, *and the isomorphism* $\mathcal{C}(F;R)/Fil^2\mathcal{C}(F;R) \xrightarrow{\cong} R^m$ *is defined by sending* $\delta_i(t)$ *to the standard basis* e_i *of* R^m.

In the rest of the subsection, we assume R is a commutative $\mathbb{Z}_{(p)}$-algebra.

Definition 10.5.15. The *p-typical elements* in a left $\mathrm{Cart}(R)$-module M are the elements x such that $F_n x = 0$ for all $(n,p) = 1$. A curve $\gamma(t)$ in a formal group G (resp. formal group law F) is said to be a *p-typical curve* if $\gamma(t)$ is a p-typical element in $\mathcal{C}(G;R)$ (resp. $\mathcal{C}(F;R)$). Denote the p-typical curves in G by $\mathcal{C}_p(G;R)$, and the p-typical curves in a formal group law $F(X,Y)$ by $\mathcal{C}_p(F(X,Y);R)$.

Definition 10.5.16. Define the element ϵ_p in $\mathrm{Cart}(R)$ by $\epsilon_p := \prod_{\substack{l \neq p \\ l \text{ prime}}} (1 - \frac{1}{l}V_l F_l)$.

Proposition 10.5.17. *The following properties hold:*

(a) ϵ_p *is an idempotent, i.e.,* $\epsilon_p^2 = \epsilon_p$.

(b) $\epsilon_p V_n = F_n \epsilon_p = 0$ *for all* $(n,p) = 1$.

(c) $\epsilon_p[c] = [c]\epsilon_p$ *for all* $c \in R$.

Definition 10.5.18. Define the *local Cartier ring* $\mathrm{Cart}_p(R) := \epsilon_p \mathrm{Cart}(R) \epsilon_p$. Define $F := F_p$ and $V := V_p$ in $\mathrm{Cart}_p(R)$. Define $\langle c \rangle := \epsilon_p[c]\epsilon_p \in \mathrm{Cart}_p(R)$.

Proposition 10.5.19. *The set of p-typical elements in a left Cart*(R)*-module* M *is equal to* $\epsilon_p M$, *and is a left Cart*$_p(R)$*-module.*

The definition of V-reducedness and V-flatness can be naturally generalized to $\mathrm{Cart}_p(R)$-modules:

Definition 10.5.20. A left $\mathrm{Cart}_p(R)$-module M is said to be *V-reduced* if $V : M \to M$ is injective and the natural map $M \to \varprojlim_{n\geq 1} M/V^n M$ is an isomorphism. A V-reduced left $\mathrm{Cart}_p(R)$-module M is said to be *V-flat* if M/VM is a flat R-module.

Proposition 10.5.21. *Let R be a $\mathbb{Z}_{(p)}$-algebra. There is an equivalence between the category of V-reduced Cart(R)-modules and the category of V-reduced Cart$_p(R)$-modules, defined as follows:*

$$\begin{array}{ccc} \{V\text{-reduced } Cart(R)\text{-modules}\} & \xrightarrow{\sim} & \{V\text{-reduced } Cart_p(R)\text{-modules}\} \\ M & \mapsto & M_p := \epsilon_p M \end{array}$$

Moreover, $M/Fil^2 M$ is canonically isomorphic to M_p/VM_p, and M is V-flat if and only if M_p is V-flat.

As a corollary, one can easily obtain the counterpart of (10.5.14) via an application of (10.5.21):

Proposition 10.5.22. (*The Main Theorem of Local Cartier Theory*)

(*a*) *Let R be a $\mathbb{Z}_{(p)}$-algebra. There is a canonical equivalence between the category of commutative smooth formal groups over R and the category of V-flat V-reduced left Cart$_p(R)$-modules, defined as follows:*

$$\begin{array}{ccc} \{formal\ groups\ over\ R\} & \xrightarrow{\sim} & \{V\text{-flat } V\text{-reduced } Cart(R)\text{-modules}\} \\ G & \mapsto & \mathcal{C}_p(G; R) \end{array}$$

(*b*) *Under the equivalence in (a), the full subcategory of m-dimensional smooth formal groups over R is equivalent to the full subcategory of V-flat V-reduced left Cart$_p(R)$-modules M such that $M/VM \cong R^m$.*

(*c*) *The category of m-dimensional formal group laws over R is equivalent to the category of V-flat V-reduced left Cart(R)-modules M equipped with an isomorphism $M/VM \xrightarrow{\cong} R^m$, via $F(X,Y) \mapsto \mathcal{C}_p(F;R)$.*

Definition 10.5.23. Let M be a V-flat V-reduced left $\mathrm{Cart}_p(R)$-module such that $M/VM \cong R^m$. We say a set of elements $\{e_i | i = 1, 2, \cdots, m\}$ in M is a *V-basis*, if $\{\overline{e_i} | i = 1, 2, \cdots, m\}$ is a basis of the free R-module M/VM.

If $\{e_i | i = 1, 2, \cdots, m\}$ is a V-basis of M, then every element in M can be uniquely written in the form of $\sum_{i=1}^{m} \sum_{n \geq 0} V^n \langle a_{n,i} \rangle e_i$, where $a_{in} \in R$. In particular, we find the identities

$$Fe_i = \sum_{j=1}^{m} \sum_{n \geq 0} V^n \langle c_{n,i,j} \rangle e_j, \quad c_{n,i,j} \in R$$

We call these identities the *structure equations* of M, and the elements $\{c_{n,i,j} | i, j = 1, 2, \cdots, m, n = 1, 2, \cdots\}$ the *structure coefficients* of M. Obviously the structure equations (or equivalently speaking, the structure coefficients) determines the isomorphism class of the V-flat V-reduced left $\mathrm{Cart}_p(R)$-module equipped with the isomorphism $M/VM \xrightarrow{\cong} R^m$.

Example 10.5.24. We describe the local Cartier module of the m-dimensional universal p-typical formal group law $F_V(X,Y)$ over $\mathbb{Z}[V]$(10.3.5). Let $\mathbb{Z}_{(p)}[V]$ be the localization of $\mathbb{Z}[V]$. We still denote by $F_V(X,Y)$ the base change to $\mathbb{Z}_{(p)}[V]$ when there is no danger of confusion. Then $\delta_1, \delta_2, \cdots, \delta_m$ (see 10.5.1 for their definitions) is a V-basis of the local Cartier module $\mathrm{Cart}_p(F_V; \mathbb{Z}_{(p)}[V])$, and the structure

equations are

$$F\delta_i = \sum_{j=1}^{m} \sum_{n\geq 0} V^n \langle V_{n+1}(j,i)\rangle \delta_j$$

In particular, the structure coefficients of $\mathrm{Cart}_p(F_V(X,Y);\mathbb{Z})$ are the free indeterminates of $\mathbb{Z}[V]$. This allows us to write down the p-typical coordinate for every p-typical formal group law $F(X,Y)$ over a $\mathbb{Z}_{(p)}$-algebra from the structure coefficients of the local Cartier module $\mathcal{C}_p(F;R)$.

Proposition 10.5.25. *Let R be a $\mathbb{Z}_{(p)}$-algebra, $F(X,Y)$ be an m-dimensional formal group law over R. Let $c_{n,i,j} \in R$ for $1 \leq i,j \leq m$ and $n = 1,2,\cdots$ be the structure coefficents of $\mathcal{C}_p(F(X,Y);R)$. Then $F = \alpha_* F_V$, where $\phi : \mathbb{Z}[V] \to R$ sends $V_{n+1}(j,i)$ to $c_{n,i,j}$.*

10.6 The relation between formal groups and p-divisible groups

Throughout this subsection, we assume R is a Noetherian complete local ring with residue field κ of characteristic p.

Let $F = F(X,Y)$ be an m-dimensional formal group law over R. For every positive integer n, we inductively define $[1]_F(X) := X$, and $[n]_F(X) := F(X,[n-1]_F(X))$ for $n \geq 2$; it is clear that $[n_1 n_2]_F(X) = [n_1]_F([n_2]_F(X))$. Denote the induced R-endomorphism on $R[[X]] = R[[X_1, X_2, \cdots, X_m]]$ by $[n]_F$.

Definition 10.6.1. We say a formal group law F over R is *p-divisible*, if $R[[X]]$ is a free module of finite rank over itself via $[p]_F : R[[X]] \to R[[X]]$.

If F is p-divisible, the rank of $R[[X]]$ over $[p]_F(R[[X]])$ is necessarily equal to p^r for some non-negative integer r; this r is defined to be the *height* of F. Let $\mathcal{J}_n$ be the ideal of $R[[X]]$ generated by $[p^n]_F(XR[[X]])$; it is clear that $\mathcal{J}_{n_1} \subset \mathcal{J}_{n_2}$ if $n_1 > n_2$. Define $\Gamma_n := \operatorname{Spec} R[[X]]/\mathcal{J}_n$. Let $i_n : \Gamma_n \to \Gamma_{n+1}$ be the natural embedding.

Proposition 10.6.2. ([23] §2.2, [17] II, 3.3.18, 4.5) *The inductive system* $(\Gamma_n, i_n : \Gamma_n \hookrightarrow \Gamma_{n+1})$ *is a connected p-divisible group over R, and the functor* $F \rightsquigarrow (\Gamma_n, i_n)$ *is an equivalence between the category of p-divisible formal group laws and the category of connected p-divisible groups over R. The quasi-inverse functor is* $G = (G_n, i_n) \rightsquigarrow \varprojlim_n \mathcal{O}(G_n)$. *Under such correspondence, the height of F is equal to the height of the associated p-divisible group.*

Chapter 11

Integral recursive formulas

Throughout this section, $(R, \mathfrak{a}, \sigma)$ is a Honda ring (10.2) where $\mathfrak{a} = (p)$ is the principal ideal generated by p. From the last section we have seen two ways to describe a m-dimensional p-typical formal group law F over R: using the unique homomorphism $\alpha : \mathcal{R}^\infty \to R$ such that $\alpha_* F_V = F$ (10.3), or using the functional equation that $\log F$ satisfies: $\log_F(X) = p\eta^{-1} * X$ for some $\eta \in R_\sigma[[\partial]]^{m\times m}$ (10.2). These two descriptions give rise to two infinite sequences of $m \times m$ matrices over R, which are called the p-typical coordinate (10.3.5) and the Honda coordinate (10.4.7) of F, respectively. Note that different p-typical coordinates can give isomorphic p-typical formal group laws (10.4.1); so do different Honda coordinates (10.4.8).

In this section we derive some formulas to relate the various coordinates of isomorphic p-typical formal group laws over R. The formulas are recursive based on the p-typical or Honda coordinates, and are *integral* (see 11.1.2 for its meaning)

so that they are applicable to trace the change of coordinates after modulo p.

11.1 An integral recursive formula between the p-typical coordinate and the Honda coordinate

We start with the relation between the p-typical and Honda coordinates of an m-dimensional formal group law F over R. Let $\log_F(X) = \sum_{n=0}^{\infty} a_n X^{p^n}$. Let $w_1, w_2, \cdots$ and $v_1, v_2, \cdots$ be the p-typical coordinate and the Honda coordinate for F, respectively. By (10.3.6) and (10.4.7), we have the following different formulas of a_n:

$$a_n = \frac{1}{p}\sum_{i=1}^{n} w_i a_{n-i}^{(p^i)} = \frac{1}{p}\sum_{i=1}^{n} a_{n-i} w_i^{(p^{n-i})} = \frac{1}{p}\sum_{i=1}^{n} v_i a_{n-i}^{\sigma^i} = \frac{1}{p}\sum_{i=1}^{n} a_{n-i} v_i^{\sigma^{n-i}}$$

$$a_n = \sum_{i_1+i_2+\cdots+i_r=n} p^{-t} w_{i_1} w_{i_2}^{(p^{i_1})} \cdots w_{i_r}^{(p^{i_1+\cdots+i_{r-1}})} = \sum_{i_1+i_2+\cdots+i_r=n} p^{-t} v_{i_1} v_{i_2}^{\sigma^{i_1}} \cdots v_{i_r}^{\sigma^{i_1+\cdots+i_{r-1}}}$$

Proposition 11.1.1 (Integral recursive formula (I))**.**

$$w_n = v_n + \frac{1}{p}\sum_{k=1}^{n-1} v_k \sum_{l=1}^{n-k} a_{n-k-l}^{\sigma^k}((w_l^{\sigma^k})^{(p^{n-k-l})} - w_l^{(p^{n-l})})$$

Remark 11.1.2. Before proving this formula, we first explain why it is called an "integral" recursive formula. Due to the elementary lemma below (11.1.4) and its corollary (11.1.5), we know that $p^{n-k-l+1} | (w_l^{\sigma^k})^{(p^{n-k-l})} - w_l^{(p^{n-l})}$. Note that $a_n \in p^{-n}R$ by its explicit formula, therefore each term $\frac{1}{p} v_k a_{n-k-l}^{\sigma^k}((w_l^{\sigma^k})^{(p^{n-k-l})} - w_l^{(p^{n-l})})$ is in R. This integral property allows us to apply the formula after modulo p in the future.

Definition 11.1.3. Let p be a prime, and n be an integer. We say n is *exactly divisible by* p^k, denoted by $p^k||n$, if $p^k|n$ but $p^{k+1} \nmid n$.

Lemma 11.1.4. *Suppose* $p^\alpha|x$, $p^\beta||y$, *and* $\alpha \geq \beta$. *Then* $p^{\alpha-\beta}|\binom{x}{y}$.

Proof. By the explicit formula of $\binom{x}{y}$, we have $\binom{x}{y} = \frac{x}{y}\binom{x-1}{y-1} = p^{\alpha-\beta}\frac{p^{-\alpha}x}{p^{-\beta}y}\binom{x-1}{y-1}$. Since $\frac{p^{-\alpha}x}{p^{-\beta}y}\binom{x-1}{y-1}$ is in $\mathbb{Z}_{(p)}$, we deduce that $p^{\alpha-\beta}|\binom{x}{y}$. □

Corollary 11.1.5. *Let* Γ *be a ring,* $a, b \in \Gamma$ *such that* $a \equiv b \mod (p^c)$ *for some integer* $c \geq 1$. *Then* $a^{p^k} \equiv b^{p^k} \mod p^{c+k}$ *for all integers* $k \geq 0$.

Proof. Write $a = b + p^c x$, then $a^{p^k} = (b + p^c x)^{p^k} = b^{p^k} + \sum_{i=1}^{p^k} \binom{p^k}{i} b^{p^k - i} p^{ci} x^i$. Suppose $p^{\alpha(i)}||i$ where $\alpha(i)$ is a non-negative integer, then by Lemma (11.1.4), $p^{k-\alpha(i)}|\binom{p^k}{i}$, therefore $\binom{p^k}{i} b^{p^k-i} p^{ci} x^i$ is divisible by $p^{k-\alpha(i)+ci}$. When $\alpha(i) = 0$, $k - \alpha(i) + ci = k + ci \geq k + c$. When $\alpha(i) \geq 1$, $k - \alpha(i) + ci \geq k + c - \alpha(i) + c(p^{\alpha(i)} - 1) \geq k + c - \alpha(i) + c\alpha(i) \geq k + c$.This proves $a^{p^k} \equiv b^{p^k} \mod p^{c+k}$. □

Now we prove (11.1.1).

Proof. By the recursive formula for a_n, we have $w_n = pa_n - \sum_{k=1}^{n-1} a_{n-k} w_k^{(p^{n-k})}$. Use the recursive formula for a_{n-k} based on the Honda coordinate, we deduce

$$\begin{aligned} w_n &= \sum_{j=1}^{n} v_j a_{n-j}^{\sigma^j} - \sum_{k=1}^{n-1} (\tfrac{1}{p} \sum_{j=1}^{n-k} v_j a_{n-k-j}^{\sigma^j}) w_k^{(p^{n-k})} \\ &= v_n + \sum_{j=1}^{n-1} v_j a_{n-j}^{\sigma^j} - \tfrac{1}{p} \sum_{k=1}^{n-1} \sum_{j=1}^{n-k} v_j a_{n-k-j}^{\sigma^j} w_k^{(p^{n-k})} \end{aligned}$$

Replace the a_{n-j} in the second term with $\frac{1}{p}\sum_{l=1}^{n-j} a_{n-j-l}w_l^{(p^{n-j-l})}$, we get

$$\begin{aligned} w_n &= v_n + \sum_{j=1}^{n-1} v_j(\tfrac{1}{p}\sum_{l=1}^{n-j} a_{n-j-l}^{\sigma^j}(w_l^{\sigma^j})^{(p^{n-j-l})}) - \tfrac{1}{p}\sum_{k=1}^{n-1}\sum_{l=1}^{n-k-1} v_l a_{n-k-l}^{\sigma^l} w_k^{(p^{n-k})} \\ &= v_n + \tfrac{1}{p}\sum_{k=1}^{n-1} v_k \sum_{l=1}^{n-k} a_{n-k-l}^{\sigma^k}((w_l^{\sigma^k})^{(p^{n-k-l})} - w_l^{(p^{n-l})}) \end{aligned}$$

□

Remark 11.1.6. In particular, if $w_i^\sigma = w_i^p$, then $v_i = w_i$, i.e., the p-typical coordinate and the Honda coordinate coincide with each other.

11.2 A formula between the Honda coordinates of isomorphic formal group laws

Let F, F' be two p-typical formal group laws over R, with Honda coordinates $v_1, v_2, \cdots$ and $v_1', v_2', \cdots$, respectively; i.e., if we define $\eta := p - \sum_{i=1}^{\infty} v_i\partial^i$ and $\eta' := p - \sum_{i=1}^{\infty} v_i'\partial^i$ in $R_\sigma[[\partial]]^{m\times m}$, then $\log_F(X) = (p\eta)^{-1} * X$ and $\log_{F'}(X) := (p\eta')^{-1} * X$. By (10.4.8), we know F and F' are isomorphic if and only if there exists $\eta_c := \sum_{n=0}^{\infty} c_n\partial^n \in R_\sigma[[\partial]]^{m\times m}$ with $c_0 \in (R^{m\times m})^\times$, such that $\eta c_0 = \eta_c\eta'$. By the definition of η and η' using the Honda coordinates, it is easy to deduce the following relation between $v_1, v_2, \cdots$ and $v_1', v_2', \cdots$:

Proposition 11.2.1.

$$v_n = \sum_{i=0}^{n-1} c_i(v_{n-i}')^{\sigma^i} c_0^{-\sigma^n} - pc_n c_0^{-\sigma^n}$$

We also have a similar relation between the coefficients of $\log_F(X) = \sum_{n=0}^{\infty} a_n X^{p^n}$ and $\log_{F'}(X) = \sum_{n=0}^{\infty} a'_n X^{p^n}$:

Proposition 11.2.2.

$$a'_n = c_0^{-1} \sum_{i=0}^{n} a_i c_{n-i}^{\sigma^i}$$

Proof. Prove by induction on n. When $n = 0$, $a'_0 = a_0 = 1 = c_0^{-1} a_0 c_0$. Suppose this is true for smaller n. Since $\log_{F'}(X) = p(\eta')^{-1} * X = (c_0^{-1}(p\eta^{-1})\eta_c) * X$, we have $(p^{-1}\eta) * c_0 * \log_{F'}(X) = \eta_c * X$. Compare the coefficients of X^{p^n} on both sides we deduce that

$$\begin{aligned}
c_0 a'_n - \tfrac{1}{p} \sum_{k=1}^{n} v_k c_0^{\sigma^k} (a'_{n-k})^{\sigma^k} &= c_n \\
a'_n &= c_0^{-1} c_n + \sum_{k=1}^{n} c_0^{-1} \tfrac{v_k}{p} c_0^{\sigma^k} (a'_{n-k})^{\sigma^k} \\
&= c_0^{-1} c_n + \sum_{k=1}^{n} c_0^{-1} \tfrac{v_k}{p} c_0^{\sigma^k} (c_0^{-1} \sum_{i=0}^{n-k} a_i c_{n-k-i}^{\sigma^i})^{\sigma^k} \\
&= c_0^{-1} c_n + \sum_{k=1}^{n} c_0^{-1} \tfrac{v_k}{p} \sum_{i=0}^{n-k} a_i^{\sigma^k} c_{n-k-i}^{\sigma^{i+k}} \\
&= c_0^{-1} c_n + \sum_{l=1}^{n} c_0^{-1} (\sum_{k=1}^{l} \tfrac{v_k}{p} a_{l-k}^{\sigma^k}) c_{n-l}^{\sigma^l} \quad (\text{let } l = i + k) \\
&= c_0^{-1} c_n + \sum_{l=1}^{n} c_0^{-1} a_l c_{n-l}^{\sigma^l} \\
&\qquad (\text{by the recursive relation for } a_n) \\
&= \sum_{l=0}^{n} c_0^{-1} a_l c_{n-l}^{\sigma^l}
\end{aligned}$$

□

11.3 An integral recursive formula between the p-typical coordinate and the Honda coordinate of isomorphic formal group laws

Notations of F, F' and their Honda coordinates are the same as the previous subsection. The following formula relates the p-typical coordinate $w'_1, w'_2, \cdots$ of F' with the Honda coordinate $v_1, v_2, \cdots$ of F in terms of $c_0, c_1, \cdots$. It is also an integral recursive formula in the sense of (11.1.2).

Proposition 11.3.1 (Integral recursive formula (II))**.**

$$\begin{aligned} w'_n &= c_0^{-1} v_n c_0^{\sigma^n} - \sum_{i=1}^{n-1} c_0 c_{n-i} (w'_i)^{(p^{n-i})} + p c_0^{-1} c_n + \\ &\quad \tfrac{1}{p} \sum_{k=1}^{n-1} \sum_{l=1}^{n-k} c_0^{-1} v_k c_0^{\sigma^k} (a'_{n-k-l})^{\sigma^k} (((w'_l)^{\sigma^k})^{(p^{n-k-l})} - (w'_l)^{(p^{n-l})}) \end{aligned}$$

where $a'_n \in R^{m\times m}$ *such that* $\log_{F'}(X) = \sum_{n=0}^{\infty} a'_n X^{p^n}$.

Proof. By (11.1.1),

$$w'_n = v'_n + \frac{1}{p} \sum_{k=1}^{n-1} v'_k \sum_{l=1}^{n-k} (a'_{n-k-l})^{\sigma^k} (((w'_l)^{\sigma^k})^{(p^{n-k-l})} - (w'_l)^{(p^{n-l})})$$

By (11.2.1), replace v'_n with $c_0^{-1} v_n c_0^{\sigma^n} - \sum_{i=1}^{n} c_0^{-1} c_i (v'_{n-i})^{\sigma^i}$, where we define $v'_0 := -p$ for simplicity in notations. From the equation above, we deduce

$$\begin{aligned} w'_n &= c_0^{-1} v_n c_0^{\sigma^n} - \sum_{i=1}^{n} c_0^{-1} c_i (v'_{n-i})^{\sigma^i} + \\ &\quad \tfrac{1}{p} \sum_{k=1}^{n-1} c_0^{-1} v_k c_0^{\sigma^k} \sum_{l=1}^{n-k} (a'_{n-k-l})^{\sigma^k} (((w'_l)^{\sigma^k})^{(p^{n-k-l})} - (w'_l)^{(p^{n-l})}) \\ &\quad - \tfrac{1}{p} \sum_{k=1}^{n-1} \sum_{i=1}^{k} c_0^{-1} c_i (v'_{k-i})^{\sigma^i} \sum_{l=1}^{n-k} (a'_{n-k-l})^{\sigma^k} (((w'_l)^{\sigma^k})^{(p^{n-k-l})} - (w'_l)^{(p^{n-l})}) \end{aligned}$$

In the second term on the first line, when $i < n$ we replace v'_{n-i} with $w'_{n-i} - \frac{1}{p}\sum_{\substack{t+s+r=n-i \\ t,r\geq 1, s\geq 0}} v'_t(a'_s)^{\sigma^t}(((w'_r)^{\sigma^t})^{(p^s)} - (w'_r)^{(p^{s+t})})$ by (11.1.1); when $i = n$ then $v'_0 = -p$ according to our convention. We deduce

$$\begin{aligned} w'_n &= c_0^{-1}v_n c_0^{\sigma^n} + pc_0^{-1}c_n - \sum_{i=1}^{n-1} c_0^{-1}c_i(w'_{n-i})^{\sigma^i} \\ &\quad + \frac{1}{p}\sum_{\substack{i+t+s+r=n \\ i,t,r\geq 1, s\geq 0}} c_0^{-1}c_i(v'_t)^{\sigma^i}(a'_s)^{\sigma^{i+t}}(((w'_r)^{\sigma^{i+t}})^{(p^s)} - ((w'_r)^{\sigma^i})^{(p^{s+t})}) \\ &\quad + \frac{1}{p}\sum_{k=1}^{n-1} c_0^{-1}v_k c_0^{\sigma^k}\sum_{l=1}^{n-k}(a'_{n-k-l})^{\sigma^k}(((w'_l)^{\sigma^k})^{(p^{n-k-l})} - (w'_l)^{(p^{n-l})}) \\ &\quad - \frac{1}{p}\sum_{k=1}^{n-1}\sum_{i=1}^{k} c_0^{-1}c_i(v'_{k-i})^{\sigma^i}\sum_{l=1}^{n-k}(a'_{n-k-l})^{\sigma^k}(((w'_l)^{\sigma^k})^{(p^{n-k-l})} - (w'_l)^{(p^{n-l})}) \end{aligned}$$

Note that the second line does not change if we add $t = 0$ to the index of the sum.

Combine the second and the fourth lines we obtain

$$\text{The sum of the second and fourth lines} =$$

$$-\frac{1}{p}\sum_{\substack{i+t+s+r=n \\ i,r\geq 1, t,s\geq 0}} c_0^{-1}c_i(v'_t)^{\sigma^i}(a'_s)^{\sigma^{i+t}}(((w'_r)^{\sigma^i})^{(p^{s+t})} - (w'_r)^{(p^{i+s+t})})$$

Separate the term with $t = 0$ from the others, we get

$$\begin{aligned} &\text{The sum of the second and fourth lines} = \\ &\sum_{\substack{i+r=2 \\ i,r\geq 1}}^{n} c_0^{-1}c_i(a'_{n-i-r})^{\sigma^i}(((w'_r)^{\sigma^i})^{(p^{n-i-r})} - (w'_r)^{(p^{n-r})}) - \\ &\sum_{\substack{i+r=2 \\ i,r\geq 1}}^{n-1} c_0^{-1}c_i(\frac{1}{p}\sum_{\substack{t+s=n-i-r \\ t\geq 1, s\geq 0}}(v'_t)(a'_s)^{\sigma^t})^{\sigma^i}(((w'_r)^{\sigma^i})^{(p^{n-i-r})} - (w'_r)^{(p^{n-r})}) \end{aligned}$$

Since $\frac{1}{p}\sum_{\substack{t+s=n-i-r \\ t\geq 1, s\geq 0}}(v'_t)(a'_s)^{\sigma^t} = a'_{n-i-r}$, only the terms whose indices satisfy $i + r = n$ in the first line survive. The sum of the second and fourth lines thus simplifies into

$\sum_{i=1}^{n-1} c_0^{-1}c_i((w'_{n-i})^{\sigma^i} - (w'_r)^{(p^i)})$. Plug this into the formula of w'_n, we deduce

$$\begin{aligned} w'_n &= c_0^{-1}v_n c_0^{\sigma^n} + pc_0^{-1}c_n - \sum_{i=1}^{n-1} c_0^{-1}c_i(w'_{n-i})^{\sigma^i} + \sum_{i=1}^{n-1} c_0^{-1}c_i((w'_{n-i})^{\sigma^i} - (w'_r)^{(p^i)}) \\ &\quad + \tfrac{1}{p}\sum_{k=1}^{n-1} c_0^{-1}v_k c_0^{\sigma^k} \sum_{l=1}^{n-k}(a'_{n-k-l})^{\sigma^k}(((w'_l)^{\sigma^k})^{(p^{n-k-l})} - (w'_l)^{(p^{n-l})}) \\ &= c_0^{-1}v_n c_0^{\sigma^n} + pc_0^{-1}c_n - \sum_{i=1}^{n-1} c_0^{-1}c_i(w'_{n-i})^{(p^i)} + \\ &\quad \tfrac{1}{p}\sum_{k=1}^{n-1} c_0^{-1}v_k c_0^{\sigma^k} \sum_{l=1}^{n-k}(a'_{n-k-l})^{\sigma^k}(((w'_l)^{\sigma^k})^{(p^{n-k-l})} - (w'_l)^{(p^{n-l})}) \end{aligned}$$

□

11.4 Universal p-typical twist of p-typical formal group laws

Let Γ be a ring. An isomorphism between m-dimensional formal group laws over Γ decomposes into a strict isomorphism and a scalar multiplication $X \mapsto uX$, where $u \in (\Gamma^{m\times m})^\times$ is the Jacobian matrix. Let F be an m-dimensional formal group law over Γ. Define the *twist of F by u* defined by $F_u(X,Y) := uF(u^{-1}X, u^{-1}Y)$.

Let us have a closer look at F_u in the special case when Γ is of characteristic 0 and F is p-typical. Write the logarithm of F as $f(X) = \sum_{n=0}^{\infty} a_n X^{p^n}$, then the logarithm of F_u is $f_u(X) := uf(u^{-1}X) = u\sum_{n=0}^{\infty} a_n(u^{-1}X)^{p^n}$. If $m = 1$, then F_u is again a p-typical formal group law. This can be seen by (10.3.11) and a direct computation: $f_u(X) = u\sum_{n=0}^{\infty} a_n(u^{-1}X)^{p^n} = \sum_{n=0}^{\infty}(ua_n u^{-p^n})X^{p^n}$. However, in the higher dimensional cases, F_u may no longer be p-typical due to the fact that $(u^{-1}X)^{p^n}$ may introduce

mixed products between the X_i's, hence $f_u(X)$ may not have the form of $\sum_{n=0}^{\infty} b_n X^{p^n}$ with $b_n \in R^{m\times m}$.

To fix this unsatisfactory defect, we make the following definition:

Definition 11.4.1. Suppose Γ is a ring of characteristic 0. Let F be a p-typical formal group law over Γ with logarithm $f(X) = \sum_{n=0}^{\infty} a_n X^{p^n}$. For $u \in (\Gamma^{m\times m})^{\times}$, define $\tilde{f}_u(X) := \sum_{n=0}^{\infty} \tilde{a}_n X^{p^n}$, where $\tilde{a}_n := u a_n (u^{-1})^{(p^n)}$. The *$p$-typical twist of F by u* is the p-typical formal group law $\tilde{F}_u(X,Y) := \tilde{f}_u^{-1}(\tilde{f}_u(X) + \tilde{f}_u(Y))$.

By (10.3.11), $\tilde{F}_u$ is a p-typical formal group law over Γ. If moreover Γ is a $\mathbb{Z}_{(p)}$-algebra of characteristic 0, then $\tilde{F}_u$ is strictly isomorphic to F_u thanks to (10.3.8), hence also isomorphic to F. We mimic the definition of universal strict isomorphism between p-typical formal group laws to understand the isomorphism between a p-typical formal group law and its p-typical twist by u.

Definition 11.4.2. Let $\mathcal{R}^{\infty,U} := \mathbb{Z}[V, U, \det(U)^{-1}]$ be short for

$$\mathbb{Z}[V_i(j,k), U(j,k), \det(U)^{-1}; i = 1, 2, \cdots, 1 \le j, k \le m]$$

where $\det(U)$ is the determinant of the $m \times m$ matrix $(U(j,k))_{1\le j,k\le m}$. Denote $\mathbb{Q}[V, U, \det(U)^{-1}]$ by $\mathcal{K}^{\infty,U}$. Define

$$f_{V,U}(X) := \sum_{n=0}^{\infty} a_n(V,U) X^{p^n}$$

where $a_n(V,U) := U a_n(V)(U^{-1})^{(p^n)} X^{p^n} \in \mathcal{K}^{\infty,1}[[X]]^{m\times 1}$, and $a_n(V)$ is defined in (10.3.6). Let $F_{V,U}(X,Y) := f_{V,U}^{-1}(f_{V,U}(X) + f_{V,U}(Y))$. Let $\alpha_{V,U}(X) := f_{V,U}^{-1}(f_V(X))$, where $f_V(X)$ is the logarithm of the universal p-typical formal group law F_V.

By the same reason as before, $F_{V,U}(X,Y)$ is a p-typical formal group law over $\mathcal{R}_{\infty,1}$. If we embed $\mathcal{R}^{\infty} = \mathbb{Z}[V] \hookrightarrow \mathcal{R}^{\infty,U} = \mathbb{Z}[V,U,\det(U)^{-1}]$ in the obvious way, then $\alpha_{V,U}$ is an isomorphism from F_V to $F_{V,U}$ over the localization $\mathcal{R}^{\infty,U}_{(p)}$. However, by the definition of $f_V(X)$ and $f_{V,U}(X)$, it is obvious that $\alpha_{V,U}(X) \in \mathcal{R}^{\infty,U}[\frac{1}{p}]$. Since $\mathcal{R}^{\infty,U}[\frac{1}{p}] \cap \mathcal{R}^{\infty,U}_{(p)} = \mathcal{R}^{\infty,U}$, we deduce that $\alpha_{V,U}$ is an isomorphism from F_V to $F_{V,U}$ over $\mathcal{R}^{\infty,U}$. We call $F_{V,U}$ the *universal p-typical twist* formal group law. This allows us to generalize the definition of p-typical twist (see 11.4.1) of a formal group law over an arbitrary ring (not necessarily of characteristic 0).

Definition 11.4.3. Let Γ be an arbitrary ring, and F be an m-dimensional formal group law over Γ. A formal group law $\tilde{F}$ over Γ is said to be a *p-typical twist of F by u*, where $u \in (\Gamma^{m\times m})^{\times}$, if there exists a homomorphism $\phi : \mathcal{R}^{\infty,U} \to \Gamma$, such that $\phi_* F_V = F$, $\phi_* F_{V,U} = \tilde{F}$, and $\phi(U) = u$.

It is easy to see that in the case when Γ is of characteristic 0, the definition (11.4.3) is equivalent to the definition (11.4.1).

By the universality of F_V, there exists a unique homomorphism $\tau_U : \mathcal{R}^{\infty} \to \mathcal{R}^{\infty,U}$ such that $(\tau_U)_* F_V = F_{V,U}$. Let $\tilde{V}_{U,n} := \tau_U(V_n)$.

We are particularly interested in the case when Γ is an $\mathfrak{I}$-adic ring, where $\mathfrak{I}$ is an ideal of Γ, and $u \in (\Gamma^{m\times m})^{\times}$ can be written as $I + \Delta$ with the entries of Δ in $\mathfrak{I}$. In this case, the homomorphism $\phi : \mathcal{R}^{\infty,U} \to \Gamma$, which induces F_u from $F_{V,U}$, factors through the following ring:

Definition 11.4.4. Define $\mathcal{R}^{\infty,1} := \mathbb{Z}[V][[D]]$ be short for

$$\mathbb{Z}[V_i(j,k)][[D(j,k)]]_{i=1,2,\cdots,1\leq j,k\leq m}$$

Define $\delta : \mathcal{R}^{\infty,U} \to \mathcal{R}^{\infty,1}$ by $\delta(V_n) := V_n$, $\delta(U(j,j)) := 1 + D(j,j)$ for $1 \leq j \leq m$, and $\delta(U(j,k)) := D(j,k)$ for $1 \leq j \neq k \leq m$.

Under the definition above, $\phi : \mathcal{R}^{\infty,U} \to \Gamma$ factors through $\delta : \mathcal{R}^{\infty,U} \to \mathcal{R}^{\infty,1}$. Let $F_{V,D} := \delta_* F_{V,U}$. If we denote $a_n(V,D) := \delta(a_n(V,U))$, the logarithm of $F_{V,D}$ is $f_{V,D} := \sum_{n=0}^{\infty} a_n(V,D)X^{p^n}$.

By the universality of F_V, there exists a unique homomorphism $\tau : \mathcal{R}^{\infty} \to \mathcal{R}^{\infty,1}$ such that $\tau_* F_V = F_{V,D}$. Let $\tilde{V}_n := \tau(V_n)$. It follows directly from (10.3.6) that

$$\tilde{V}_n = pa_n(V,D) - \sum_{i=1}^{n-1} a_i(V,D)\tilde{V}_{n-i}^{(p^i)}$$

Definition 11.4.5. Let Γ be a ring, and $A = (a_{ij}), B = (b_{ij}) \in \Gamma^{r\times s}$ be two matrices over Γ with the same dimensions. The *Hadamard product* of A and B is defined to be $(a_{ij}b_{ij})$, denoted by $A * B$.

Proposition 11.4.6 (first order recursive formula for $\tilde{V}_n$ in char. p)**.**

$$\begin{aligned}\tilde{V}_n \equiv\ & V_n + DV_n + \sum_{\substack{s_1+s_2+\cdots+s_r+j=n\\ r\geq 1}} \\ & (-1)^r(((DV_j) * V_{n-s_1-\cdots-s_r}^{(p^{s_r}-1)} - DV_j^{(p^{s_r})}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_r-1})}))* \\ & V_{n-s_1-\cdots-s_{r-1}}^{(p^{s_{r-1}}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_{r-1}-1})})) \cdots * V_{n-s_1}^{(p^{s_1}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1}-1)})) \\ & \mod (p)(D) + (D)^2\end{aligned}$$

where (D) *is the ideal generated by* $D(j,k)$, $1 \leq j,k \leq m$.

Proof. We prove by induction. When $n = 1$, $\tilde{V}_1 = pa_1(V, D) = (1+D)a_1(V)(p((1+D)^{-1})^{(p)})$. Since $(1+D)^{-1} = 1 - D + D^2 - D^3 + \cdots$, $p((1+D)^{-1})^{(p)} \equiv p \mod (p^2)(D) + (D)^2$, and $(1+D)^{-1}a_1(V) \in p^{-1}\mathcal{R}$. Note that if $x \in \mathcal{R}^{\infty,1}$ and $px \in (D)$, then $x \in (D)$. This proves

$$\tilde{V}_1 \equiv (1+D)a_1(V) \cdot p = V_1 + DV_1 \mod (p)(D) + (D)^2$$

The case when $n = 1$ is thus proved. Suppose we have proved for smaller n's. In the recursive formula $\tilde{V}_n = pa_n(V, D) - \sum_{i=1}^{n-1} a_i(V, D)\tilde{V}_{n-i}^{(p^i)}$, note that $pa_n(V, D) = (1+D)a_n(V)(p((1+D)^{-1})^{(p^n)})$, and $p((1+D)^{-1})^{(p^n)} - p \in (p^{n+1})(D) + (D)^2$, while $a_n(V) \in p^{-n}\mathcal{R}^{\infty,1}$, this implies

$$pa_n(V, D) \equiv (1+D)a_n(V) \cdot p = (1+D)(pa_n(V)) \mod (p)(D) + (D)^2$$

For $1 \leq i \leq n-1$, $a_i(V, D) = (1+D)a_i(V)((1+D)^{-1})^{(p^i)}$, $a_i(V) \equiv \frac{V_1 V_1^{(p)} \cdots V_1^{(p^{i-1})}}{p^i}$ mod $p^{-(i-1)}\mathcal{R}^{\infty,1}$, and $((1+D)^{-1})^{(p^i)} \equiv 1 - p^i D \mod (D)^2$, therefore $a_i(V, D) \equiv$

$(1+D)a_i(V) - V_1 V_1^{(p)} \cdots V_1^{(p^{i-1})} D \mod (p)(D)+(D)^2$. Thus we deduce

$$\begin{aligned}
\tilde{V}_n &\equiv (1+D)(pa_n(V) - \sum_{i=1}^{n-1} a_i(V)\tilde{V}_{n-i}^{(p^i)}) + \sum_{i=1}^{n-1} V_1 V_1^{(p)} \cdots V_1^{(p^{i-1})} D\tilde{V}_{n-i}^{(p^i)} \\
&\equiv (1+D)(pa_n(V) - \sum_{i=1}^{n-1} a_i(V)V_{n-i}^{(p^i)}) + \\
&\quad \sum_{i=1}^{n-1} V_1 V_1^{(p)} \cdots V_1^{(p^{i-1})} DV_{n-i}^{(p^i)} - \sum_{i=1}^{n-1} a_i(V)\{p^i V_{n-i}^{(p^i-1)} * (DV_{n-i} + \\
&\quad \sum_{\substack{s_1'+s_2'+\cdots+s_{r'}'+j'=n-i \\ r'\geq 1}} (-1)^{r'}(((DV_{j'} - DV_{j'}^{(p^{s_{r'}'})}) * V_{n-i-s_1'-\cdots-s_{r'}'}^{(p^{s_{r'}'}-1)}) \cdots V_{n-i-s_1'}^{(p^{s_1'}-1)}) \cdot \\
&\quad (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1-1})}))) \\
&\equiv (1+D)V_n - \sum_{i=1}^{n-1} V_1 V_1^{(p)} \cdots V_1^{(p^{i-1})}((DV_{n-i}) * V_{n-i}^{(p^i-1)} - DV_{n-i}^{(p^i)}) + \\
&\quad \sum_{\substack{s_1+s_2+\cdots+s_r+j=n \\ r\geq 2}} (-1)^r(((DV_j) * V_{n-s_1-\cdots-s_r}^{(p^{s_r}-1)} - DV_j^{(p^{s_r})}) \cdot \\
&\quad (V_1 V_1^{(p)} \cdots V_1^{(p^{s_{r-1}-1})})) * \cdots * V_{n-i-s_1}^{(p^{s_1}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1-1})})) \\
&\equiv (1+D)V_n + \sum_{s_1+s_2+\cdots+s_r+j=n} (-1)^r(((DV_j) * V_{n-s_1-\cdots-s_r}^{(p^{s_r}-1)} - DV_j^{(p^{s_r})}) \cdot \\
&\quad (V_1 V_1^{(p)} \cdots V_1^{(p^{s_{r-1}-1})})) * \cdots * V_{n-i-s_1}^{(p^{s_1}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1-1})})) \\
&\quad \mod (p)(D)+(D)^2
\end{aligned}$$

This finishes the induction. □

Remark 11.4.7. In particular, when $m = 1$ we have $(DV_j) * V_{n-s_1-\cdots-s_r}^{(p^{s_r}-1)} - DV_j^{(p^{s_r})} = 0$, hence the formula simplifies into $\tilde{V}_n \equiv V_n + DV_n \mod (p)(D)+(D)^2$. This agrees with the fact that $a_n(V,D) = (I+D)a_n(V)(I+D)^{-1}$, and $\tilde{V}_n = (I+D)V_n(I+D)^{-1}$ in the one-dimensional case.

11.5 Integral recursive formulas for strictly isomorphic p-typical formal group laws

After studying the p-typical twists, in this subsection we look at strict isomorphisms between p-typical formal group laws. Recall that F_V is the (m-dimensional) universal p-typical formal group law over $\mathcal{R}^\infty = \mathbb{Z}[V]$, which is short for $\mathbb{Z}[V_i(j,k)|i = 1,2,\cdots,j,k = 1,2,\cdots,m]$. There is a p-typical formal group law $F_{V,T}$ over $\mathcal{R}^{\infty,\infty} := \mathbb{Z}[V,T]$, which is short for

$$\mathbb{Z}[V_i(j,k), T_i(j,k)|i = 1,2,\cdots,j,k = 1,2,\cdots,m]$$

If we embed $\mathcal{R}^\infty = \mathbb{Z}[V] \subset \mathcal{R}^{\infty,\infty} = \mathbb{Z}[V,T]$ in the obvious way, the formal group law $F_{V,T}$ is strictly isomorphic to F_V over $\mathcal{R}^{\infty,\infty}$. The isomorphism $\alpha_{V,T} : F_V \to F_{V,T}$ is universal in the sense of (10.4.1).

By the universality of F_V, there exists a unqiue homomorphism $\xi : \mathcal{R}^\infty \to \mathcal{R}^{\infty,\infty}$ such that $\xi_* F_V = F_{V,T}$. If we denote $\xi(V_i)$ by $\overline{V}_i$, then

$$\overline{V}_i = \Phi_i(V_1, V_2, \cdots, V_n, T_1, T_2, \cdots, T_n)$$

is a polynomial in the entries of $V_1, V_2, \cdots, V_n$ and $T_1, T_2, \cdots, T_n$. There is a recursive formula (10.4.3) for $\overline{V}_i$ based on T and V.

We derive a variation of (10.4.3), with the advantage of being "integral" in the sense of (11.1.2). Let $a_n(V)$ be the coefficients of $\log_{F_V}$ defined in (10.3.6), and recall that the endomorphism $\sigma : \mathcal{R}^{\infty,\infty} \to \mathcal{R}^{\infty,\infty}$ sends V_i, T_i to $V_i^{(p)}$, $T_i^{(p)}$, respectively.

Proposition 11.5.1 (Integral recursive formula (III))**.**

$$\begin{aligned}\overline{V}_n &= V_n + pT_n - \sum_{i+j=n,i,j\geq 1} T_j \overline{V}_i^{(p^j)} + \sum_{l=1}^{n-1} V_l \sum_{k=1}^{n-l-1} \tfrac{1}{p} a_{n-k-l}(V)^{\sigma^l} \{((\overline{V}_k^{\sigma^l})^{(p^{n-l-k})} \\ &\quad -(\overline{V}_k^{(p^l)})^{(p^{n-l-k})}) + \sum_{i+j=k,i,j\geq 1} T_j^{(p^{n-k})}((\overline{V}_i^{\sigma^l})^{(p^{n-l-i})} - (\overline{V}_i^{(p^l)})^{(p^{n-l-i})})\} \\ &\quad + \sum_{l=1}^{n-1} V_l \{\tfrac{1}{p}(\overline{V}_{n-l}^{\sigma^l} - \overline{V}_{n-l}^{(p^l)}) + \sum_{i+j=n-l,i,j\geq 1} T_j^{(p^l)}(\tfrac{1}{p}((\overline{V}_i^{\sigma^l})^{(p^j)} - (\overline{V}_i^{(p^l)})^{(p^j)}))\}\end{aligned}$$

Proof. From (10.4.3), if we make the convention that $T_0 := 1$, then the recursive formula for $\overline{V}_n$ can be written as

$$\begin{aligned}\overline{V}_n &= V_n + pT_n + \sum_{\substack{i+j=n \\ i,j\geq 1}} (V_i T_j^{(p^i)} - T_j \overline{V}_i^{(p^i)}) \\ &\quad + \sum_{k=1}^{n-1} a_{n-k}(V)(\sum_{\substack{i+j=k \\ i\geq 1, j\geq 0}} (V_i^{(p^{n-k})} T_j^{(p^{n-j})} - T_j^{(p^{n-k})} \overline{V}_i^{(p^{n-i})}))\end{aligned}$$

Let S be the second line in this equation. Replace $a_{n-k}(V)$ with $\sum_{l=1}^{n-k} \frac{1}{p} V_l a_{n-k-l}(V)^{\sigma^l}$ (10.3.6), we obtain

$$S = \sum_{l=1}^{n-1} \sum_{k=1}^{n-l} \tfrac{1}{p} V_l a_{n-k-l}(V)^{\sigma^l} \sum_{\substack{i+j=k \\ i\geq 1, j\geq 0}} (V_i^{(p^{n-k})} T_j^{(p^{n-j})} - T_j^{(p^{n-k})} \overline{V}_i^{(p^{n-i})})$$

On the other hand, from the (non-integral) recursive formula for $\overline{V}_{n-l}$ we deduce that

$$\sum_{k=1}^{n-l} a_{n-k-l} \sum_{\substack{i+j=k \\ i\geq 1, j\geq 0}} (V_i^{(p^{n-k-l})} T_j^{(p^{n-j-l})} - T_j^{(p^{n-k-l})} \overline{V}_i^{(p^{n-i-l})}) = -pT_{n-l}$$

Note that when $k = 1$ the index "$i + j = k, i, j \geq 1$" is empty; in this way we have combined all the terms in formula (10.4.3). If we apply the σ^l operation to both sides, we get:

$$\begin{aligned}&\sum_{k=1}^{n-l-1} a_{n-k-l}(V)^{(\sigma^l)}[(V_k^{(p^{n-k})} - (\overline{V}_k^{\sigma^l})^{(p^{n-k-l})} + \sum_{i+j=k,i,j\geq 1} (V_i^{(p^{n-k})} T_j^{(p^{n-j})} - \\ &T_j^{(p^{n-k})}(\overline{V}_i^{\sigma^l})^{(p^{n-i-l})})] = -pT_{n-l}^{(p^l)}\end{aligned}$$

Compare with the formula for S we deduce

$$\begin{aligned} S &= \sum_{l=1}^{n-1} \tfrac{1}{p} V_l(-pT_{n-l}^{(p^l)}) + \sum_{l=1}^{n-1}\sum_{k=1}^{n-l} \tfrac{1}{p} V_l a_{n-k-l}(V)^{\sigma^l} + \\ &\quad \sum_{\substack{i+j=k \\ i\geq 1, j\geq 0}} T_j^{(p^{n-k})}((\overline{V}_i^{\sigma^l})^{(p^{n-l-i})} - (\overline{V}_i^{(p^l)})^{(p^{n-l-i})})\} \end{aligned}$$

Plug S into the formula for $\overline{V}_n$ and the integral recursive formula follows. $\square$

We are mainly interested in tracking the change of coordinates after modulo p. The following lemma is a finer result comparing to (11.1.5). Recall that the Hadamard product $A * B$ for two matrices $A = (a_{ij})$ and $B = (b_{ij})$ with the same dimensions is defined to be the entry-wise product $(a_{ij}b_{ij})$.

Lemma 11.5.2. *For $A \in R^{r\times s}$ and $i, j \geq 0$,*

$$(A^{\sigma^i})^{(p^j)} - A^{(p^{i+j})} \equiv p^{j+1} A^{(p^i(p^j-1))} * (\frac{A^\sigma - A^{(p)}}{p})^{(p^{i-1})} \mod p^{j+2}$$

Proof. Write

$$A^{\sigma^i} - A^{(p^i)} = (A^{\sigma^i} - (A^{\sigma^{i-1}})^{(p)}) + ((A^{\sigma^{i-1}})^{(p)} - (A^{\sigma^{i-2}})^{(p^2)}) + \cdots + ((A^\sigma)^{(p^{i-1})} - A^{(p^i)})$$

By (11.1.5), all but the first term on the right hand side is divisible by p^2. Hence

$$A^{\sigma^i} - A^{(p^i)} \equiv A^{\sigma^i} - (A^{\sigma^{i-1}})^{(p)} = p(\frac{A^\sigma - A^{(p)}}{p})^{\sigma^{i-1}} \equiv p(\frac{A^\sigma - A^{(p)}}{p})^{(p^{i-1})} \mod p^2$$

This proves the case when $j = 0$. Now in general we consider

$$\begin{aligned} (A^{\sigma^i})^{(p^j)} - A^{(p^{i+j})} &= (A^{(p^i)} + (A^{\sigma^i} - A^{(p^i)}))^{(p^j)} - A^{(p^{i+j})} \\ &= \sum_{k=1}^{p^j} \tbinom{p^j}{k} A^{p^i(p^j-k)} * (A^{\sigma^i} - A^{(p^i)})^{(k)} \end{aligned}$$

Suppose $p^\alpha||k$ (see 11.1.3 for this notation), then $p^{j-\alpha}|\binom{p^j}{k}$ by (11.1.4). Since $p^k|(A^{\sigma^i}-A^{(p^i)})^{(k)}$, we deduce that $p^{j-\alpha+k}|\binom{p^j}{k}A^{p^i(p^j-k)}*(A^{\sigma^i}-A^{(p^i)})^{(k)}$. When $k\geq 2$, $p^\alpha||k$ implies $k\geq\alpha+2$ (note that we have assumed $p>2$). When $k=1$, we have $\alpha=0$, and $j-\alpha+k=j+1$. Therefore

$$\begin{aligned}(A^{\sigma^i})^{(p^j)}-A^{(p^{i+j})} &\equiv p^{j+1}A^{(p^i(p^j-1))}*\tfrac{A^{\sigma^i}-A^{(p^i)}}{p}\equiv p^{j+1}A^{(p^i(p^j-1))}*(\tfrac{A^\sigma-A^{(p)}}{p})^{(p^{i-1})}\\ &\mod p^{j+2}\end{aligned}$$

□

Proposition 11.5.3 (Recursive formula for $\overline{V}_n mod p\mathfrak{T}_n$)**.**

$$\begin{aligned}\overline{V}_n \equiv\ & V_n-\sum_{j=1}^{n-1}T_j\overline{V}_{n-j}^{(p^j)}+\sum_{l=1}^{n-1}V_l\sum_{k=1}^{n-l}V_1^{(p^l)}V_1^{(p^{l+1})}\cdots V_1^{(p^{n-k-1})}\\ &(\overline{V}_k^{(p^l(p^{n-k-l}-1))}*(\tfrac{\overline{V}_k^\sigma-\overline{V}_k^{(p)}}{p})^{(p^{l-1})})\mod (p)\mathfrak{T}_n\end{aligned}$$

where $\mathfrak{T}_n$ stands for the ideal of $\mathcal{R}^{\infty,\infty}=\mathbb{Z}[V,T]$ generated by $T_i(j,k)$ for all $1\leq i\leq n$ and $1\leq j,k\leq m$.

Proof. In the integral recursive formula (11.5.1), the term

$$((\overline{V}_i^{\sigma^l})^{(p^{n-l-i})}-(\overline{V}_i^{(p^l)})^{(p^{n-l-i})})$$

is divisible by $p^{n-l-i+1}$ according to (11.1.5). Because of the range of the indices, $n-l-i+1\geq n-l-k+2$. On the other hand, $\frac{1}{p}a_{n-k-l}(V)^{(p^l)}\in p^{-(n-l-k)}\mathcal{R}^{\infty,\infty}=\mathbb{Z}[V,T]$ by (10.3.6). This proves

$$\frac{1}{p}a_{n-k-l}(V)^{\sigma^l}T_j^{(p^{n-k})}((\overline{V}_i^{\sigma^l})^{(p^{n-l-i})}-(\overline{V}_i^{(p^l)})^{(p^{n-l-i})})\in(p)\mathfrak{T}_n$$

Similarly, the term $T_j^{(p^l)}(\frac{1}{p}((\overline{V}_i^{\sigma^l})^{(p^j)}-(\overline{V}_i^{(p^l)})^{(p^j)})\in(p)\mathfrak{T}_n$, too.

By (11.5.2),

$$((\overline{V}_k^{\sigma^l})^{(p^{n-l-k})} - (\overline{V}_k^{(p^l)})^{(p^{n-l-k})}) \equiv p^{n-l-k+1}\overline{V}_k^{(p^l(p^{n-l-k}-1))} * (\tfrac{\overline{V}_k^{\sigma} - \overline{V}_k^{(p)}}{p})^{(p^{l-1})} \mod p^{n-l-k+2}$$

On the other hand, $\frac{1}{p}a_{n-k-l}(V)^{(p^l)} \equiv \frac{1}{p^{n-l-k+1}}V_1^{(p^l)}V_1^{(p^{l+1})}\cdots V_1^{(p^{n-k+1})}$ by (10.3.6), therefore

$$\frac{1}{p}a_{n-k-l}(V)^{\sigma^l}((\overline{V}_k^{\sigma^l})^{(p^{n-l-k})} - (\overline{V}_k^{(p^l)})^{(p^{n-l-k})}) \equiv$$
$$V_1^{(p^l)}V_1^{(p^{l+1})}\cdots V_1^{(p^{n-k+1})}(\overline{V}_k^{(p^l(p^{n-l-k}-1))} * (\tfrac{\overline{V}_k^{\sigma} - \overline{V}_k^{(p)}}{p})^{(p^{l-1})}) \mod p$$

At the same time, by (10.4.3) $\overline{V}_n \equiv V_n \mod \mathfrak{T}_n$. Therefore

$$(\overline{V}_k^{\sigma^l})^{(p^{n-l-k})} - (\overline{V}_k^{(p^l)})^{(p^{n-l-k})}, \frac{\overline{V}_{n-l}^{\sigma^l} - \overline{V}_{n-l}^{(p^l)}}{p}$$

are both in $\mathfrak{T}_n$, too. Since $(p)\cap\mathfrak{T}_n = (p)\mathfrak{T}_n$ in $\mathbb{Z}[V,T]$, we deduce that

$$\frac{1}{p}a_{n-k-l}(V)^{\sigma^l}((\overline{V}_k^{\sigma^l})^{(p^{n-l-k})} - (\overline{V}_k^{(p^l)})^{(p^{n-l-k})})$$
$$\equiv V_1^{(p^l)}V_1^{(p^{l+1})}\cdots V_1^{(p^{n-k+1})}(\overline{V}_k^{(p^l(p^{n-l-k}-1))} * (\tfrac{\overline{V}_k^{\sigma} - \overline{V}_k^{(p)}}{p})^{(p^{l-1})}) \mod (p)\mathfrak{T}_n$$

Similarly we can deduce

$$V_l\frac{\overline{V}_{n-l}^{\sigma^l} - \overline{V}_{n-l}^{(p^l)}}{p} \equiv V_l(\frac{\overline{V}_{n-l}^{\sigma} - \overline{V}_{n-l}^{(p)}}{p})^{(p^{l-1})} \mod (p)\mathfrak{T}_n$$

The proposition now follows. □

Proposition 11.5.4 (First order recursive formula for $\overline{V}_n \mod p\mathfrak{T}_n$)**.**

$$\overline{V}_n \equiv V_n - \sum_{i=1}^{n-1} T_i V_{n-i}^{(p^i)} + \sum(-1)^r(((-T_iV_j^{(p^{s_r})}) * V_{n-s_1-\cdots-s_r}^{(p^{s_r}-1)}\cdot$$
$$(V_1V_1^{(p)}\cdots V_1^{(p^{s_r-1})})) * V_{n-s_1-\cdots-s_{r-1}}^{(p^{s_{r-1}}-1)})\cdot(V_1V_1^{(p)}\cdots V_1^{(p^{s_{r-1}-1})}))\cdots *$$
$$V_{n-s_1}^{(p^{s_1}-1)})\cdot(V_1V_1^{(p)}\cdots V_1^{(p^{s_1}-1)})) \mod (p)\mathfrak{T}_n + \mathfrak{T}_{n-1}^2$$

where in the second line, the sum is over all $s_1 + s_2 + \cdots + s_r + i + j = n$ *with* $i, j, r, s_1, s_2, \cdots, s_r \geq 1$.

Proof. Prove by induction. When $n = 1$ this is obviously true. Now suppose it is true for smaller n's.

In the formula of (11.5.3), $(\frac{\overline{V}_k^\sigma - \overline{V}_k^{(p)}}{p})^{(p^{l-1})}$ and $(\frac{\overline{V}_{n-l}^\sigma - \overline{V}_{n-l}^{(p)}}{p})^{(p^{l-1})}$ are in $\mathfrak{T}_{n-1}^2$ when $l > 1$. Therefore only the terms with $l = 1$ survive modulo $(p)\mathfrak{T}_n + \mathfrak{T}_{n-1}^2$:

$$\overline{V}_n \equiv V_n - \sum_{j=1}^{n-1} T_j \overline{V}_{n-j}^{(p^j)} + V_1 \sum_{k=1}^{n-1} V_1^{(p)} V_1^{(p^2)} \cdots V_1^{(p^{n-k-1})} (V_k^{(p^{n-k}-p)} * (\frac{\overline{V}_k^\sigma - \overline{V}_k^{(p)}}{p}))$$

By the inductive hypothesis,

$$\begin{aligned} \overline{V}_k &\equiv V_k - \sum_{j=1}^{k-1} T_j V_{k-j}^{(p^j)} + \sum (-1)^{r'} (((-T_{i'} V_{j'}^{(p^{i'})}) * V_{k-s_1'-\cdots-s_{r'}'}^{(p^{s_t'}-1)}) \cdots * (V_{k-s_1'}^{(p^{s_1'}-1)}) \cdot \\ &\quad (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1'-1})}) \end{aligned}$$

where the sum is over $s_1' + s_2' + \cdots s_{r'}' + i' + j' = k$, $i', j', r', s_1', s_2', \cdots, s_{r'}' \geq 1$. So $\overline{V_k}^\sigma \equiv V_k^{(p)} \mod \mathfrak{T}_{n-1}^2$, and

$$\begin{aligned} \overline{V}_k^{(p)} &\equiv V_k^{(p)} - pV_k^{(p-1)} * (\sum_{j=1}^{k-1} T_j V_{k-j}^{(p^j)} + \sum (-1)^{r'+1} (((-T_{i'} V_{j'}^{(p^{i'})}) * V_{k-s_1'-\cdots-s_{r'}'}^{(p^{s_{r'}'}-1)}) \cdots \\ &\quad * (V_{k-s_1'}^{(p^{s_1'}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1'-1})}) \mod (p)^2 \mathfrak{T}_n + \mathfrak{T}_{n-1}^2 \end{aligned}$$

Thus

$$\begin{aligned}
& V_1 \sum_{k=1}^{n-1} V_1^{(p)} V_1^{(p^2)} \cdots V_1^{(p^{n-k-1})} (V_k^{(p^{n-k}-p)} * (\tfrac{\overline{V}_k^{\sigma} - \overline{V}_k^{(p)}}{p})) \\
\equiv\ & V_1 \sum_{k=1}^{n-1} V_1^{(p)} V_1^{(p^2)} \cdots V_1^{(p^{n-k-1})} (V_k^{(p^{n-k}-p)} * (V_k^{(p-1)} * (\sum_{j=1}^{k-1} T_j V_{n-j}^{(p^j)} + \\
& \sum (-1)^{r'+1} (((-T_{i'} V_{j'}^{(p^{i'})}) * V_{k-s_1'-\cdots-s_{r'}'}^{(p^{s_t'}-1)}) \cdots * (V_{k-s_1'}^{(p^{s_1'}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1'-1})}) \\
\equiv\ & V_1 \sum_{k=1}^{n-2} V_1^{(p)} V_1^{(p^2)} \cdots V_1^{(p^{n-k-1})} (V_k^{(p^{n-k}-1)} * (\sum_{j=1}^{k-1} T_j V_{n-j}^{(p^j)} + \\
& \sum (-1)^{r'+1} (((-T_{i'} V_{j'}^{(p^{i'})}) * V_{k-s_1'-\cdots-s_{r'}'}^{(p^{s_{r'}'}-1)}) \cdots * (V_{k-s_1'}^{(p^{s_1'}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1'-1})}) \\
& \quad \bmod (p)\mathfrak{T}_n + \mathfrak{T}_{n-1}^2
\end{aligned}$$

If we take $s_1 := n-k$, and $s_l := s_{l-1}'$ for $l \geq 2$, this sum is exactly equal to $\sum (-1)^r (((-T_i V_j^{(p^i)}) * V_{k-s_1-\cdots-s_r}^{(p^{s_r}-1)}) \cdots * (V_{k-s_1}^{(p^{s_1}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1-1})})$ with the sum over $s_1 + s_2 + \cdots + s_r + i + j = n$ with $i, j, r, s_1, s_2, \cdots, s_r \geq 1$. The proposition now follows by induction. □

11.6 The universal isomorphism between p-typical formal group laws

Combine the results of the previous two subsections, we now define a universal (not necessarily strict) isomorphism between p-typical formal group laws. Recall that Φ_n is the polynomial such that $F_{V,T}$ is induced from F_V via

$$\xi : V_n \mapsto \Phi_n(V_1, V_2, \cdots, V_n, T_1, T_2, \cdots, T_n)$$

Definition 11.6.1. (a) Let $\mathcal{R}^{\text{univ}} := \mathbb{Z}[V, T, U, \det(U)^{-1}]$ be short for

$$\mathbb{Z}[V_i(j,k), T_i(j,k), U(j,k), \det(U)^{-1}; i = 1, 2, \cdots, 1 \leq j, k \leq m]$$

where $\det(U)$ is the determinant of the $m \times m$ matrix $(U(j,k))_{1\leq j,k\leq m}$. Denote $\mathbb{Q}[V,T,U,\det(U)^{-1}]$ by $\mathcal{K}^{\mathrm{univ}}$. Define $V'_{U,n} := \Phi_n(\tilde{V}_{U,1},\cdots,\tilde{V}_{U,n},T_1,\cdots,T_n)$, and $\rho_U : \mathcal{R}^\infty \to \mathcal{R}^{\mathrm{univ}}$ by $\rho_U(V_n) := V'_{U,n}$. Let $F_{V,T,U} := (\rho_U)_* F_V$, and denote its logarithm by $f_{V,T,U}(X) = \sum_{n=0}^{\infty} a_n(V,T,U)X^{p^n}$. Let $\alpha_{V,T,U}(X) := f^{-1}_{V,T,U}(f_{V,T,U}(X) + f_{V,T,U}(Y))$.

(b) Let $\mathcal{R}^{\mathrm{univ},1} := \mathbb{Z}[V,T][[D]]$ be short for

$$\mathbb{Z}[V_i(j,k),T_i(j,k)][[D(j,k)]]_{i=1,2,\cdots,1\leq j,k\leq m}$$

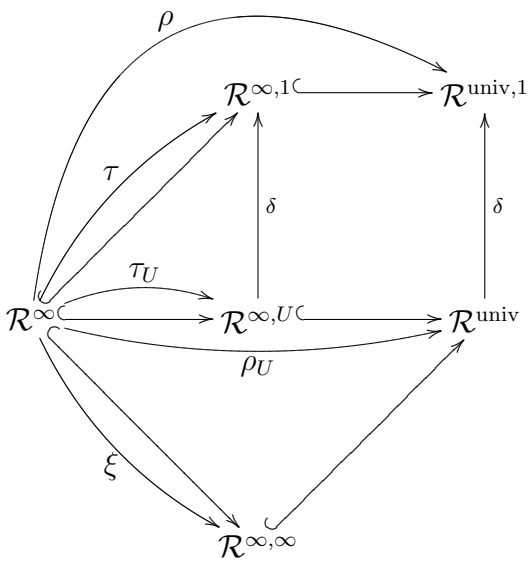
Denote $\mathbb{Q}[V,T][[D]]$ by $\mathcal{K}^{\mathrm{univ},1}$. Define $V'_n := \Phi_n(\tilde{V}_1,\cdots,\tilde{V}_n,T_1,\cdots,T_n)$, and $\rho : \mathcal{R}^\infty \to \mathcal{R}^{\mathrm{univ},1}$ by $\rho(V_n) := V'_n$. Let $F_{V,T,D} := \rho_* F_V$, and denote its logarithm by $f_{V,T,D}(X) = \sum_{n=0}^{\infty} a_n(V,T,D)X^{p^n}$. Let $\alpha_{V,T,D}(X) := f^{-1}_{V,T,D}(f_{V,T,D}(X) + f_{V,T,D}(Y))$.

(c) (c.f. 11.4.4) Let $\delta : \mathcal{R}^{\mathrm{univ}} \to \mathcal{R}^{\mathrm{univ},1}$ be the homomorphism such that $\delta(V_i) = V_i$, $\delta(T_i) = T_i$, and $\delta(U) = 1 + D$.

Remark 11.6.2. For the definition of Φ_n, see the paragraph below 10.3.6. For the definitions of $\tilde{V}_{U,n}$ and $\tilde{V}_n$, see the paragraphs below (11.4.1) and (11.4.4). The definition of $V'_{U,n}$ and V'_n amounts to replacing the V_i in the definition of $\overline{V}_n$ with $\tilde{V}_{U,i}$ and V_i, respectively.

The relations of the various polynomial rings over $\mathbb{Z}$ with countably infinitely

many variables are shown in the following diagram:



$$\xi_* F_V = F_{V,T}$$

$$(\tau_U)_* F_V = F_{V,U}$$

$$(\rho_U)_* F_V = F_{V,T,U}$$

$$\tau_* F_V = F_{V,D}$$

$$\rho_* F_V = F_{V,T,D}$$

Note that the homomorphisms $\xi, \tau_U, \rho_U, \tau, \rho$ do not commute with the arrows in the diagram.

Proposition 11.6.3. *Let Γ be a ring, F, F' be (m-dimensional) p-typical formal group laws over Γ, and $\alpha : F \to F'$ be an isomorphism. Let $u \in (\Gamma^{m\times m})^\times$ be the Jacobian of α. Then:*

(a) There exists a unique homomorphism $\phi : \mathcal{R}^{univ} \to \Gamma$, such that $\phi_* F_V = F$, $\phi_* F_{V,T,U} = F'$, $\phi(U) = u$, and $\phi_* \alpha_{V,T,U} = \alpha$.

(b) If moreover, Γ is an $\mathfrak{I}$-adic ring where $\mathfrak{I}$ is an ideal of Γ, and $u \in 1 + \mathfrak{I}^{m\times m}$, then the homomorphism $\phi : \mathcal{R}^{univ} \to \Gamma$ factors through $\mathcal{R}^{univ,1}$ via $\delta : \mathcal{R}^{univ} \to \mathcal{R}^{univ,1}$.

Proof. Recall that we have the chain of natural inclusions $\mathcal{R}^{\infty} = \mathbb{Z}[V] \subset \mathcal{R}^{\infty,U} = \mathbb{Z}[V,U] \subset \mathcal{R}^{\text{univ}} = \mathbb{Z}[V,T,U]$, and we have defined $\tau_U : \mathcal{R}^{\infty} \to \mathcal{R}^{\infty,U}$, $\rho_U : \mathcal{R}^{\infty} \to$

$\mathcal{R}^{\text{univ}}$ such that $(\tau_U)_* F_V = F_{V,U}$, $(\rho_U)_* F_V = F_{V,T,U}$. Let $\phi_0 : \mathcal{R}^\infty \to \Gamma$ be the homomorphism such that $F = (\phi_0) * F_V$. Extend ϕ_0 over $\mathcal{R}^{\infty,U}$ by defining $\phi_0(U) := u$. Denote $(\phi_0 \circ \tau_U)_* F_V$ by $\tilde{F}$, then $\tilde{F}$ is the p-typical twist of F by u (11.4.3). The isomorphism $\alpha_{V,U} : F_V \to F_{V,U}$ over $\mathcal{R}^{\infty,U}$ pushes forward to an isomorphism $\alpha_0 := (\phi_0)_* \alpha_{V,U} : F \to \tilde{F}$ over Γ, and the Jacobian of α_0 is u. Since $\alpha : F \to F'$ is an isomorphism between p-typical formal group laws with the same Jacobian, we deduce that $\tilde{F}$ is strictly isomorphic to F' via $\alpha \circ \alpha_0^{-1}$. By (10.4.1), there exists a unique homomorphism $\phi_1 : \mathcal{R}^{\infty,\infty} \to \Gamma$ such that $(\phi_1)_* F_V = \tilde{F}$, $(\phi_1)_* F_{V,T} = F'$, and $(\phi_1)_* \alpha_{V,T} = \alpha \circ \alpha_0^{-1}$.

Define $\phi : \mathcal{R}^{\text{univ}} \to \Gamma$ by $\phi(V_i) := \phi_0(V_i)$, $\phi(T_i) := \phi_1(T_i)$, and $\phi(U) := \phi_0(U) = u$. By the definition of ϕ_0 we have $\phi_* F_V = (\phi_0)_* F_V = F$. Now it suffices to check $\phi_* F_{V,T,U} = F'$. Recall that $F_{V,T,U} = (\rho_U)_* F_V$, and $F' = (\phi_1)_* F_{V,T} = (\phi_1 \circ \xi)_* F_V$, hence we are reduced to showing $\phi \circ \rho_U = \phi_1 \circ \xi$ over $\mathcal{R}^\infty$. For every V_i, $(\phi \circ \rho_U)(V_i) = \phi(\Phi_i(\tilde{V}_U, T)) = \Phi_i(\phi_0(\tilde{V}_U), \phi_1(T))$, and $(\phi_1 \circ \xi)(V_i) = \phi_1(\Phi_i(V, T)) = \Phi_i(\phi_1(V), \phi_1(T))$, therefore it suffices to show $\phi_1(V) = \phi_0(\tilde{V}_U)$. Since $\tilde{F} = (\phi_1)_* F_V = (\phi_0 \circ \tau_U)_* F_V$, we deduce that $\phi_1(V) = \phi_0(\tau_U(V)) = \phi_0(\tilde{V}_U)$. This proves part (a). Part (b) follows directly due to the act that $\phi(U) = u$ in part (a) and the assumption on u in part (b). $\square$

Definition 11.6.4. Denote the composition of polynomial $\Phi_n(\tilde{V}_1, \cdots, \tilde{V}_n, T_1, \cdots, T_n)$ and $\tilde{V}_n = \tau(V_1, \cdots, V_n) \in \mathcal{R}^{\infty,1}$ by

$$\Theta_n(D, V_1, \cdots, V_n, T_1, \cdots, T_n)$$

denote its (i,j)-th entry by $\Theta_{n,i,j}(D, V_1, \cdots, V_n, T_1, \cdots, T_n)$.

Let $(\mathfrak{D}, \mathfrak{T})_n$ be the ideal of $\mathcal{R}^{\mathrm{univ},1}$ that is generated by $D(i,j)$ and $T_l(i,j)$, where $1 \leq i, j \leq m$ and $l = 1, 2, \cdots, n$. Combine (11.4.6) and (11.5.4), we can have the following first order recursive formula of Θ_n after modulo $p(D,T)$:

Proposition 11.6.5.

$$\Theta_n(D, V_1, \cdots, V_n, T_1, \cdots, T_n) \equiv V_n + DV_n - T_1 V_{n-1}^{(p)} - T_2 V_{n-2}^{(p^2)} - \cdots - T_{n-1} V_1^{(p^{n-1})}$$
$$+ \sum (-1)^r (((DV_k) * V_{n-s_1-\cdots-s_r}^{(p^{s_r}-1)} - DV_k^{(p^{s_r})} - \sum_{i+j=k} T_i V_j^{(p^i)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_r-1})})*$$
$$V_{n-s_1-\cdots-s_{r-1}}^{(p^{s_{r-1}}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_{r-1}-1})})) \cdots * V_{n-s_1}^{(p^{s_1}-1)}) \cdot (V_1 V_1^{(p)} \cdots V_1^{(p^{s_1}-1)}))$$
$$\mathrm{mod}\ (p)(\mathfrak{D}, \mathfrak{T})_n + (\mathfrak{D}, \mathfrak{T}_{n-1})^2$$

where in the second line, the sum is over all $s_1 + s_2 + \cdots + s_r + k = n$ *with* $i, j, r, s_1, s_2, \cdots, s_r \geq 1$.

Chapter 12

Infinite dimensional matrices Over an $\mathfrak{a}$-adic ring

We have seen the p-typical coordinate of a p-typical formal group law involves infinitely many variables, and the p-typical coordinates of isomorphic p-typical formal group laws are connected by infinitely many polynomial equations. In this section we introduce some basic properties about infinite dimensional matrices over an $\mathfrak{a}$-adic ring $\mathfrak{R}$, where $\mathfrak{a}$ is an ideal. The case when $\mathfrak{R}$ is equipped with the discrete topology can be treated as taking $\mathfrak{a} = 0$. For $x \in \mathfrak{R}$, let $v(x)$ be the integer v such that $x \in \mathfrak{a}^v \backslash \mathfrak{a}^{v+1}$ if $x \neq 0$, and define $v(0) := \infty$.

12.1 Definitions and basic properties

We start with some definitions and properties of (countably) infinite dimensional matrices over $\mathfrak{a}$-adic rings.

Definition 12.1.1. Let $\mathfrak{R}$ be an $\mathfrak{a}$-adic ring. Let $A = (a_{i,j})_{i,j\in\mathbb{N}}, B = (b_{i,j})_{i,j\in\mathbb{N}}$ be infinite dimensional matrices over $\mathfrak{R}$. The product AB is defined when for any pair of $i, j \in \mathbb{N}$, $\sum_{l=1}^{\infty} a_{i,l}b_{l,j}$ converges. We say A is *row-converging (resp. column-converging)*, if for every i, the sequence $(a_{i,j})_{j\in\mathbb{N}}$ converges in $\mathfrak{R}$.

Note that when $\mathfrak{a} = 0$, hence $\mathfrak{R}$ is equipped with the discrete topology, being row-converging (resp. column-converging) just means there are only finitely many nonzero entries on every row (resp. column).

Proposition 12.1.2. *Let $\mathfrak{R}$ be an $\mathfrak{a}$-adic ring. The matrices here are all infinite dimensional matrices over $\mathfrak{R}$.*

(a) Let $n_l :=$ the smallest integer n such that the entries of A_l are all in $\mathfrak{a}^n$. If $\lim_{l\to\infty} n_l = \infty$, then $A_1 + A_2 + \cdots$ converges. If moreover, each A_l is row-converging (resp. column-converging) for $l = 1, 2, \cdots$, then $A_1 + A_2 + \cdots$ is also row-converging (resp. column-converging).

(b) If A is row-converging (resp. column-converging), then AB (resp. BA) is defined for every B. If moreover, B is also row-converging (resp. column-converging), then AB is row-converging (resp. column-converging), too.

(c) If BC is defined and A is row-converging, then $A(BC), (AB)C$ are both

defined and they are equal. If BC is defined and A is column-converging, then $(BC)A$, $B(CA)$ are both defined and they are equal.

Proof. We only prove in the row-converging case, since the column-converging case follows similarly. In (a), let $A_l = (a_{i,j,l})_{i,j,l=1,2,\cdots}$. Note that $v(a_{i,j,l}) \geq n_l$ by the definition of n_l. The sum $\sum_{l=1}^{\infty} a_{i,j,l}$ converges since $\lim_{l\to\infty} v(a_{i,j,l}) = \infty$. To prove $A_1 + A_2 + \cdots$ is row-converging when $A_1, A_2, \cdots$ are row-converging, we fix an i. For every $N > 0$, there exists K_1 such that $n_l \geq N$ when $l > K_1$. There also exists K_2 such that $a_{i,j,l} \geq N$ when $l = 1, 2, \cdots, K_1$ and $j > K_2$. Therefore $v(\sum_{l=1}^{\infty} a_{i,j,l}) \geq N$ when $j > K_2$. This proves (a).

The only nontrivial part of (b) is to show AB is also row-converging when A, B are both row-converging. Let $A = (a_{i,j}), B = (b_{i,j})$. Fix an integer i. Since A is row-converging, for any N, there exists L_1 such that $v(a_{i,l}) \geq N$ when $l > L_1$. Since B is row-converging, there exists L_2 such that $v(b_{l,j}) \geq N$ when $l = 1, 2, \cdots, L_1$ and $j > L_2$. Therefore $v(\sum_l a_{i,l}b_{l,j}) \geq N$ when $j > L_2$.

The only nontrivial part of (c) is to show $(AB)C$ is defined. Let $C = (c_{i,j})$, respectively. Fix a pair of index i, j. Since A is row-converging, $\lim_{l\to\infty} v(a_{i,l}) = \infty$. Thus for any N, there exists M_1 such that $v(a_{i,l}) \geq N$ when $l > M_1$. Therefore for any r, $v(\sum_l a_{i,l}b_{l,r}) \geq \min\{N, v(a_{i,l}) + v(b_{l,r}) | l = 1, 2, \cdots, M_1\}$. Since BC is defined, there exists M_2 such that $v(b_{l,r}) + v(c_{r,j}) \geq N$ when $l = 1, 2, \cdots, M_1$ and $r \geq M_2$. As a result, $v((\sum_l a_{i,l}b_{l,r})c_{r,j}) \geq N$ when $r \geq M_2$. This proves $(AB)C$ is defined. □

Definition 12.1.3. Let Γ be an arbitrary ring, and A be an infinite dimensional

matrix over Γ. An infinite dimensional matrix B is said to be a *right (resp. left) inverse* of A, if $AB = I$ (resp. $BA = I$). If B is both a right inverse and a left inverse, then we simply say B is the *inverse* of A, denoted by A^{-1}.

Remark 12.1.4. A right or left inverse of an infinite dimensional matrix may not be unique. However, the inverse of an infinite dimensional matrix, if exists, must be unique.

Definition 12.1.5. Let $\mathfrak{R}$ be an $\mathfrak{a}$-adic ring. An infinite dimensional matrix $A = (a_{i,j})_{i,j=1,2,\cdots}$ is said to be *blockwise lower triangular (resp. blockwise upper triangular)*, if there exists $k_1 := 1 < k_2 < k_3 < \cdots$ such that $a_{i,j} = 0$ whenever there exists n such that $i < k_n \leq j$ (resp. $j < k_n \leq i$). A blockwise lower (resp. upper) triangular infinite dimensional matrix $A = (a_{i,j})_{i,j=1,2,\cdots}$ is said to be *regular*, if for all $n \geq 1$, the finite square matrix $(a_{i,j})_{k_n \leq i,j < k_{n+1}}$ is in $(\mathfrak{R}^{k_{n+1}-k_n})^{\times}$. In the special case when $k_i = i$, the corresponding matrices are called *lower (resp. upper) triangular matrices* and *regular lower (resp. upper) triangular matrices*.

Lemma 12.1.6. *The matrices here are all assumed to be infinite dimensional.*

(a) Let Γ be a ring. A regular blockwise lower (resp. upper) triangular matrix A over Γ has a unique right (resp. left) inverse, which is also a left (resp. inverse). The inverse A^{-1} is blockwise lower (resp. upper) triangular, and is the unique left (resp. right) inverse that is blockwise lower (resp. upper) triangular.

(b) Let $\mathfrak{R}$ be an $\mathfrak{a}$-adic ring, and A be a row-converging matrix (resp. column-converging) over $\mathfrak{R}$ with a row-converging (resp. column-converging) right (resp.

left) inverse. Let N be a row-converging (resp. column-converging) matrix with entries in $\mathfrak{a}$. Then $A+N$ is row-converging (resp. column-converging), and it has a unique right (resp. left) inverse, which is also a left (resp. right) inverse. The inverse is also row-converging (resp. column-converging), and is the unique left (resp. right) inverse that is row-converging (resp. column-converging).

Proof. We only prove the case when $k_n = n$ for $n = 1, 2, \cdots$ in the definition of blockwise lower or upper triangular matrices, i.e., the lower or upper triangular matrices in the usual sense. The proof to the general blockwise case is similar.

We only prove for the regular lower triangular case, since the regular upper triangular case follows similarly. Let us first look at (a). For every column vector $y = (y_1, y_2, \cdots)^t$, there exists a unique solution $x = (x_1, x_2, \cdots)^t$ to $Ax = y$ by setting $x_0 := \frac{y_1}{a_{1,1}}$, and $x_n := \frac{1}{a_{n,n}}(y_n - \sum_{i=1}^{n-1} a_{n,i}x_i)$. Take the column vector to be $(1, 0, 0, \cdots)$, $(0, 1, 0, \cdots)$, $\cdots$ in order, we deduce that A has a unique right inverse, which we denote by B. It is easy to see that for $y = (y_1, y_2, \cdots)^t$ whose i-th component is 1 and other components are 0, the solution $x = (x_1, x_2, \cdots)^t$ has 0 on the $1, 2, \cdots, i-1$ components. This proves B is also lower triangular. Since a lower-triangular matrix is row-converging, we have $A(BA) = (AB)A = A$ by (12.1.2). Again by the uniqueness of the solutions to $AX = A$, we deduce that B is also a left inverse. Hence B is the unique inverse, which will be denoted by A^{-1}. If C is another lower triangular left inverse, then $C = C(AB) = (CA)B = B$.

To prove (b), note that A^{-1} and N are both row-converging by the assumption,

hence $A^{-1}N$ is also row-converging. Thus $(A^{-1}N)^k$ is defined for any non-negative integer l. consider $X := I - A^{-1}N + (A^{-1}N)^2 - (A^{-1}N)^3 + \cdots$, which is convergent and row-converging by (12.1.2). It is easy to see that $X(I + A^{-1}N) = (I + A^{-1}N)X = I$, hence $X = (I + A^{-1}N)^{-1}$. Therefore $(A + N)^{-1} = (A(I + A^{-1}N))^{-1} = XA^{-1}$ exists, too. To see the uniqueness of the right inverse of $A+N$, it suffices to prove if $\mathbf{z} = (z_1, z_2, \cdots)^t$ is an infinite dimensional column vector over $\mathfrak{R}$ and $(A + N)\mathbf{z} = 0$, then $\mathbf{z} = 0$. Otherwise, let d be the first integer such that $v(z_d) = \min\{v(z_i)|i = 1, 2, \cdots\}$, then the valuation of the d-th row of $(A + N)\mathbf{z}$ should be equal to d, contradiction. The other statements in (b) can be proved in the same way as in the proof of (a). □

12.2 Infinite system of power series equations over an $\mathfrak{a}$-adic ring

Let $\mathfrak{R}$ be an $\mathfrak{a}$-adic ring, where $\mathfrak{a}$ is an ideal. For every $a \in \mathfrak{R}$, let $v(a)$ be the smallest non-negative integer d such that $a \in \mathfrak{a}^d \backslash \mathfrak{a}^{d+1}$. Let $\mathbb{N}^\infty$ be the set of $\{(i_1, i_2, \cdots)\}$ with all but finitely many $i_j = 0$. For $I = (i_1, i_2, \cdots) \in \mathbb{N}^\infty$, let $d(I) :=$ the number of $i_j > 0$, $\max I := \max\{i_k|k = 1, 2, \cdots\}$.

Definition 12.2.1. Define $\mathfrak{R}\langle\mathbf{X}\rangle$ to be the set of $\sum_I a_I x^I$ where $I \in \mathbb{N}^\infty$, $a_I \in \mathfrak{R}$ such that for fixed $d(I) = d$, $v(a_I) \to \infty$ as $\max I \to \infty$.

The following proposition is an easy exercise:

Proposition 12.2.2. (*a*) *Under the usual addition and multiplication,* $\mathfrak{R}\langle \mathbf{X}\rangle$ *is a commutative ring.*

(*b*) *For each* $f = \sum_I a_I x^I \in \mathfrak{R}\langle \mathbf{X}\rangle$ *and* $i = 1, 2, \cdots$, $\frac{\partial f}{\partial x_i} \in \mathfrak{R}\langle \mathbf{X}\rangle$, *too.*

(*c*) *Let* $\mathfrak{x}$ *be the ideal of* $\mathfrak{R}\langle \mathbf{X}\rangle$ *generated by* $x_1, x_2, \cdots$. *Then for every positive integer* r, $\mathfrak{x}^r$ *consists of* $\sum_I a_I x^I$ *in* $\mathfrak{R}\langle \mathbf{X}\rangle$ *such that* $a_I = 0$ *when* $d(I) < r$.

(*d*) $\mathfrak{R}\langle \mathbf{X}\rangle$ *is separated and complete with respect to the* $\mathfrak{x}$*-topology.*

Definition 12.2.3. For a sequence of (countably) infinitely many elements $\mathcal{P} = P_1, P_2, \cdots$ in $\mathfrak{R}\langle \mathbf{X}\rangle$, the *Jacobian* of $\mathcal{P}$ is defined as the infinite dimensional matrix $(\frac{\partial P_i}{\partial x_j})_{i,j=1,2,\cdots}$ over $\mathfrak{R}\langle \mathbf{X}\rangle$, denoted by $J(\mathcal{P})$. The evaluation of $J(\mathcal{P})$ at $x_1 = x_2 = \cdots = 0$ is denoted by $J_0(\mathcal{P})$.

If $\mathcal{P}$ is a sequence of (countably) infinitely many elements $P_1, P_2, \cdots$ in $\mathfrak{R}\langle \mathbf{X}\rangle$ and $\mathbf{y} = (y_1, y_2, \cdots)^t$ is an infinite dimensional column vector over $\mathfrak{R}\langle \mathbf{X}\rangle$, we denote the infinite dimensional column vector $(P_1(\mathbf{y}), P_2(\mathbf{y}), \cdots)^t$ by $\mathcal{P}(\mathbf{y})$.

Proposition 12.2.4. *Suppose* $\mathcal{Q} = \{Q_1, Q_2, \cdots\}$ *is a sequence of (countably) infinitely many elements in* $\mathfrak{R}\langle \mathbf{X}\rangle$, *satisfying:*

(*1*) $\mathcal{Q}(\mathbf{0}) = \mathbf{0}$.

(*2*) $J := J(\mathcal{Q})$ *is row-converging with respect to the* $\mathfrak{x}$*-adic topology on* $\mathfrak{R}\langle \mathbf{X}\rangle$, *and there exists a row-converging right inverse* L *of* J.

(*3*) $J_0 := J_0(\mathcal{Q})$ *is row-converging with respect to the* $\mathfrak{a}$*-adic topology on* $\mathfrak{R}$, *and there exists a row-converging right inverse* L_0 *of* J_0.

(4) *Write* $Q_l = \sum_I Q_{l,I} x^I$, *then for a fixed* $l \in \{1, 2, \cdots\}$, $v(Q_{l,I}) \to \infty$ *as* $\max I \to \infty$.

Then there exists a unique solution $\mathbf{z} = (z_1, z_2, \cdots)^t$ *over* $\mathfrak{R}\langle \mathbf{X} \rangle$ *with* $z_i \in \mathfrak{x}$ *such that* $\mathcal{Q}(\mathbf{z}) = \mathbf{x} := (x_1, x_2, \cdots)^t$. *Moreover, we have* $\mathbf{z} \equiv L_0 \mathbf{x} \mod \mathfrak{x}^2$.

Proof. Define $\mathbf{z}(1) := L_0 \mathbf{x}$, which is an infinite dimensional vector in $\mathfrak{R}\langle \mathbf{X} \rangle$ due to the assumption that L_0 is row-converging. Then

$$\mathcal{Q}(\mathbf{z}(1)) = \mathcal{Q}(\mathbf{z}(1)) - \mathcal{Q}(0) \equiv J_0 \mathbf{z}(1) \equiv \mathbf{x} \mod \mathfrak{x}^2$$

Suppose now $n \geq 1$, we have constructed $\mathbf{z}(n)$ and shown $\mathcal{Q}(\mathbf{z}(n)) \equiv \mathbf{x} \mod \mathfrak{x}^{n+1}$. Define $\mathbf{z}(n+1) := \mathbf{z}(n) - L_0(\mathcal{Q}(\mathbf{z}(n)) - \mathbf{x})$, which is well defined since L_0 is row-converging. Then

$$\begin{aligned}
\mathcal{Q}(\mathbf{z}(n+1)) &= (\mathcal{Q}(\mathbf{z}(n+1)) - \mathcal{Q}(\mathbf{z}(n))) + \mathcal{Q}(\mathbf{z}(n)) \\
&\equiv J_0(\mathbf{z}(n+1) - \mathbf{z}(n)) + \mathcal{Q}(\mathbf{z}(n)) \mod \mathfrak{x}^{n+2} \\
&= -J_0 L_0(\mathcal{Q}(\mathbf{z}(n)) - \mathbf{x}) + \mathcal{Q}(\mathbf{z}(n)) \\
&= \mathbf{x}
\end{aligned}$$

The matrix products in the formulas above are well defined because J_0, L_0 are row-converging. Therefore the inductively defined $\mathbf{z}(n)$ converge to a solution $\mathbf{z} \in \mathfrak{R}[[x_1, x_2, \cdots]]$ to $\mathcal{P}(\mathbf{x}) = \mathbf{0}$, and $\mathbf{z} \equiv \mathbf{z}(1) = L_0 \mathbf{x} \mod \mathfrak{x}^2$.

Write $\mathbf{z} = (z_1, z_2, \cdots)^t$ with $z_i = \sum_K z_{i,K} x^K$. By the construction we know $z_{i,\emptyset} = 0$. To prove $\mathbf{z}$ is an infinite dimensional column vector over $\mathfrak{R}\langle \mathbf{X} \rangle$, it remains to prove for every fixed $i = 1, 2, \cdots$ and fixed $d(K) = d$, we have $v(z_{i,K}) \to \infty$ as

$\max K \to \infty$. Since $\mathbf{z}(n+1) - \mathbf{z}(n) \in \mathfrak{x}^{n+1}$, it suffices to prove for $j = 1, 2, \cdots, d$, we have $v(\mathbf{z}(j)_{i,K}) \to \infty$ as $\max K \to \infty$. We start with $j = 1$. By definition the components of $\mathbf{z}(1)_i$ are linear in $\mathbf{x}$, so it suffices to check in the $d = 1$ case, which follows directly from the assumption that L_0 is row-converging. Suppose now $2 \leq j \leq d$ and we have proved for $j - 1$. One can compute

$$\mathbf{z}(j)_{i,K} = \mathbf{z}(j-1)_{i,K} - \sum_{l=1}^{\infty} \sum_{I} L_{i,l} Q_{l,I} \mathbf{z}(j-1)_K^I$$

where $L_{i,l}$ is the (i,l)-th entry of L_0.

Now we fix an arbitrary $N > 0$. Since L is row-converging, there exists M_1 such that $v(L_{i,l}) \geq N$ when $l > M_1$. By the condition (4), there exists M_2 such that $v(Q_{l,I}) \geq N$ when $l = 1, 2, \cdots, M_1$ and $\max I > M_2$. Without loss of generality we assume $M_2 \geq i$. By the inductive hypothesis, there exists M_3 such that $v(\mathbf{z}(j-1)_{s,K}) \geq N$ for all $s = 1, 2, \cdots, M_2$ and $\max K > M_3$.

We now claim that $v(\mathbf{z}(j)_{i,K}) \geq N$ when $\max K > M_3$. By the choice of M_3, we have $v(\mathbf{z}(j-1)_{i,K}) \geq N$. By the choice of M_1 and M_2, it suffices to consider $l \leq M_1$ and $\max I \leq M_2$ in the sum $\sum_{l=1}^{\infty} L_{i,l} Q_{l,I} \mathbf{z}(j-1)_K^I$. By the definition of $\mathbf{z}(j-1)_K^I$, if $I = (i_1, i_2, \cdots, i_r)$, we can write $\mathbf{z}(j-1)_K^I = \sum \mathbf{z}(j-1)_{i_1,K_1} \mathbf{z}(j-1)_{i_2,K_2} \cdots \mathbf{z}(j-1)_{i_r,K_r}$, where the sum is over all the partitions $K = K_1 \coprod K_2 \coprod \cdots \coprod K_r$. Since $\max K > M_3$, there exists $s \in \{1, 2, \cdots, r\}$ such that $\max K_s > M_3$. Since $i_s \leq \max I \leq M_2$, by the choice of M_3 we have $v(\mathbf{z}(j-1)_{i_s,K_s}) \geq N$. This proves the claim as well as the fact that $\mathbf{z}$ is a column vector over $\mathfrak{R}\langle \mathbf{X} \rangle$.

For the uniqueness of $\mathbf{z}$ as a solution to $\mathcal{Q}(\mathbf{z}) = \mathbf{x}$, suppose $\mathbf{z} + \delta = (z_1 +$

$\delta_1, z_2 + \delta_2, \cdots)^t$ is another solution with $\delta_i \in \mathfrak{x}$ such that $\mathcal{Q}(\mathbf{z} + \delta) = \mathbf{x}$. Then $\mathcal{Q}(\mathbf{z} + \delta) - \mathcal{Q}(\mathbf{z}) = \mathbf{0}$. By the Taylor expansion of the left hand side based on $\delta_1, \delta_2, \cdots$, we derive a system of polynomial equations whose linear part in δ is $J := J(\mathcal{Q})$. Using the row-converging right inverse L (which is also a left inverse) evaluated at $\mathbf{z}$, we can put the system into the form of $\delta_i = g_i(\delta_1, \delta_2, \cdots)$ for $i = 1, 2, \cdots$ such that g_i's are formal power series over $\mathfrak{R}\langle\mathbf{X}\rangle$ with degree ≥ 2 in $\delta_1, \delta_2, \cdots$. For $y \in \mathfrak{R}\langle\mathbf{X}\rangle$, let $\mathrm{ord}_x(y)$ be the smallest integer d such that $y \in \mathfrak{x}^d$. If $\delta \neq \mathbf{0}$, let k be the integer such that $\mathrm{ord}_x(\delta_k) = \min\{\mathrm{ord}_x(\delta_i) | i = 1, 2, \cdots\}$. By our assumption $\mathrm{ord}_x(\delta_k) \geq 1$. However, $\mathrm{ord}_x(g_k(\delta_1, \delta_2, \cdots)) \geq 2\mathrm{ord}_x(\delta_k) > \mathrm{ord}_x(\delta_k)$, this is a contradiction to $\delta_k = g_k(\delta_1, \delta_2, \cdots)$. Therefore $\delta = \mathbf{0}$ and the uniqueness is proved. □

Corollary 12.2.5. *Suppose $\mathfrak{R}$ is an $\mathfrak{a}$-adic ring, where $\mathfrak{a}$ is an ideal. Let $P_i \in \mathfrak{R}\langle\mathbf{X}\rangle$ for $i = 1, 2, \cdots$. If $J(\mathcal{P})$ is row-converging over $\mathfrak{R}\langle\mathbf{X}\rangle$ with a row-converging inverse L, $J_0(\mathcal{P})$ is row-converging over $\mathfrak{R}$ with a row-converging right inverse L_0 of $J_0(\mathcal{P})$, then for every $\mathbf{c} = (c_1, c_2, \cdots)^t$ with $c_i \in \mathfrak{a}$, there exists a unique solution $\mathbf{z} := (z_1, z_2, \cdots)^t$ to the system of equations $\mathcal{P}(\mathbf{z}) = \mathbf{c}$. Moreover, we have $\mathbf{z} \equiv L_0\mathbf{c}$ mod $\mathfrak{a}^2$.*

Remark 12.2.6. In particular, if $J(\mathcal{P})$ and $J_0(\mathcal{P})$ can be written as the sum of a regular blockwise lower triangular matrix and a row-converging matrix with entries in $\mathfrak{a}$, then the conditions on the Jacobians and their inverses in (12.2.5) are satisfied by (12.1.6).

Proof. Define $\phi : \mathfrak{R}\langle \mathbf{X} \rangle \to \mathfrak{R}$ by $\phi(x_i) := c_i$. It is an easy exercise to see that for $\sum_I a_I x^I$ in $\mathfrak{R}\langle \mathbf{X} \rangle$, its image $\sum_I a_I c^I$ under ϕ converges in $\mathfrak{R}$; hence ϕ is a well-defined homomorphism. Then the existence of $\mathbf{z}$ follows from (12.2.4) immediately. The uniqueness of $\mathbf{z}$ can be proved in the same way as we did in (12.2.4). □

Remark 12.2.7. Corollary (12.2.5) also covers the situation when there are only finitely many polynomials $P_1, P_2, \cdots, P_n$ in $x_1, x_2, \cdots, x_n$, such that the Jacobian's evaluation $J_0(\mathcal{P})$ at $\mathbf{0}$ is an invertible $n \times n$ matrix. One can realize this situation as a special case of (12.2.5) by introducing auxiliary indeterminates $x_{n+1}, x_{n+2}, \cdots$ and defining $P_i := x_i$ for $i = n+1, n+2, \cdots$. Then the conditions on the Jacobians are automatically satisfied. Consider the equations

$$P_1(\mathbf{x}) = c_1, P_2(\mathbf{x}) = c_2, \cdots, P_n(\mathbf{x}) = c_n, P_{n+1}(\mathbf{x}) = 0, P_{n+2}(\mathbf{x}) = 0, \cdots$$

we deduce that there exists a unique solution $\mathbf{z} := (z_1, z_2, \cdots, z_n)^t$ such that $P_i(\mathbf{z}) = c_i$. If we define L_0 to be the Jacobian of $P_1, P_2, \cdots, P_n$ evaluated at $x_1 = x_2 = \cdots = 0$, then we have $\mathbf{z} \equiv L_0 \mathbf{c} \mod \mathfrak{a}^2$.

Chapter 13

Algorithm

13.1 The deformation of p-divisible Groups

From now on let $k := \overline{\mathbb{F}}_p$. Let X be a connected p-divisible group over k with dimension m and codimension n. Denote the category of artinian local $W(k)$-algebras by $\mathrm{Art}_{W(k)}$.

Definition 13.1.1. The *deformation functor* $\mathrm{Def}(X/W(k))$ is a functor from $\mathrm{Art}_{W(k)}$ to the category of sets defined as follows: for every artinian local $W(k)$-algebra R, $\mathrm{Def}(X/W(k))(R)$ is the set of isomorphism classes of pairs $(\tilde{X}/R, \epsilon)$, where $\tilde{X}$ is a p-divisible group over R, and $\epsilon : \tilde{X}_k \to X$ is an isomorphism of p-divisible groups; $(\tilde{X}/R, \epsilon)$ and $(\mathcal{Y}'/R, \epsilon')$ are said to be *isomorphic*, if there exists an isomorphism $\alpha : \tilde{X} \xrightarrow{\cong} \tilde{X}'$ such that $\epsilon' \circ \alpha_k = \epsilon$.

Theorem 13.1.2 (Grothendieck-Messing)**.** *The functor* $\mathrm{Def}(X/W(k))$ *is repre-*

sentable by a smooth formal scheme Spf$\mathcal{R}$ over $W(k)$ of relative dimension mn.

There exists a p-divisible group $\mathcal{X}$ over $\operatorname{Spf}\mathcal{R}$ and an isomorphism $\epsilon_{\text{univ}} : \mathcal{X}_k \to X$, satisfying the following universal property: for every artinian local $W(k)$-algebra R, if $(\tilde{X}/R, \epsilon : \tilde{X}_k \xrightarrow{\cong} X)$ is a lifting of X, then there exists a unique map of $W(k)$-schemes: $s : \operatorname{Spec} R \to \operatorname{Spf}\mathcal{R}$, such that $(\tilde{X}, \epsilon)$ is the pull back of $(\mathcal{X}, \epsilon_{\text{univ}})$ via s. The p-divisible group $\mathcal{X}/\mathcal{R}$ is called the *universal lifting* of X.

The automorphism group $\operatorname{Aut}(X)$ of X has a natural action on $\operatorname{Def}(X/W(k))$ by relabelling:

Definition 13.1.3 (Relabelling action). Suppose $\rho \in \operatorname{Aut}(X)$, we define

$$R_\rho : \operatorname{Def}(X/W(k)) \to \operatorname{Def}(X/W(k))$$

as follows: for every artinian local $W(k)$-algebra R and an isomorphism class of lifting $[(\tilde{X}/R, \epsilon : \tilde{X}_k \xrightarrow{\cong} X)]$ of X, we define $R_\rho[(\tilde{X}/R, \epsilon)]$ to be $[(\tilde{X}/R, \rho \circ \epsilon)]$.

By the universality of $\mathcal{X}$, we can also define R_ρ as the unique map $\mathcal{R} \to \mathcal{R}$, such that there exists an isomorphism $\rho_{\text{univ}} : \mathcal{X} \to R_\rho^*\mathcal{X}$ making the following diagram commute:

$$\begin{array}{ccc} \mathcal{X}_k & \xrightarrow{\epsilon_{\text{univ}}} & X \\ \downarrow{\scriptstyle (\rho_{\text{univ}})_k} & & \downarrow{\scriptstyle \rho} \\ (R_\rho^*\mathcal{X})_k & \xrightarrow{\epsilon_{\text{univ}}} & X \end{array}$$

On the other hand, let F be an m-dimensional formal group law over k. If R is an artinian local $W(k)$-algebra and $\tilde{F}$ is a formal group law over R, we denote by $\tilde{F}_k$ the pushforward of $\tilde{F}$ under the natural residue homomorphism $R \to k$.

Definition 13.1.4. The *deformation functor* $\mathrm{Def}(F/W(k))$ is a functor from $\mathrm{Art}_{W(k)}$ to the category of sets defined as follows: for every artinian local $W(k)$-algebra R, $\mathrm{Def}(F/W(k))(R)$ is the set of isomorphism classes of pairs $(\tilde{F}/R, \epsilon)$, where $\tilde{F}$ is a formal group law over R, and $\epsilon : \tilde{F}_k \to F$ is an isomorphism of formal group laws; $(\tilde{F}/R, \epsilon)$ and $(\tilde{F}'/R, \epsilon')$ are said to be *isomorphic*, if there exists an isomorphism $\alpha : \tilde{F} \xrightarrow{\cong} \tilde{F}'$ such that $\epsilon' \circ \alpha_k = \epsilon$.

By (10.6.2), there exists an m-dimensional formal group law F over k such that the associated p-divisible group is isomorphic to X, and $\mathrm{Def}(F/W(k))$ is naturally isomorphic to $\mathrm{Def}(X/W(k))$. For every $\rho \in \mathrm{Aut}(F) \cong \mathrm{Aut}(X)$, the relabelling action R_ρ on $\mathrm{Def}(F/W(k))$ can be defined in the same way, and is compatible with the relabelling action on $\mathrm{Def}(X/W(k))$ under the isomorphism $\mathrm{Def}(F/W(k)) \xrightarrow{\cong} \mathrm{Def}(X/W(k))$.

The following alternative definition of $\mathrm{Def}(F/W(k))$ is often easier to use:

Definition 13.1.5 (An alternative definition of $\mathrm{Def}(F/W(k))$). A formal group law $\tilde{F}$ over R is said to be a *lifting* of F, if $\tilde{F}_k = F$. An isomorphism $\alpha : \tilde{F} \to \tilde{G}$ between formal group laws over R is said to be a $\star$-*isomorphism*, if $\alpha_k = \mathrm{Id}$. The *deformation functor* $\mathrm{Def}(F/W(k))$ is a functor from $\mathrm{Art}_{W(k)}$ to the category of sets that assigns each artinian local $W(k)$-algebra R the set of equivalent classes of liftings of F over R modulo $\star$-isomorphisms.

The two definitions of $\mathrm{Def}(F/W(k))$ in (13.1.4) and (13.1.5) are easily seen to be equivalent, since every isomorphism α between formal group laws $\tilde{F}_k$ and F over

k lifts to an m-tuple of formal power series $\tilde{\alpha}$ in m indeterminates with invertible Jacobian, hence $\alpha(\tilde{F}(\alpha^{-1}(X)+\alpha^{-1}(Y)))$ is a lifting of F.

By (10.3.10), we could choose F to be a p-typical formal group law. The following proposition says that it suffices to consider p-typical liftings of F in the definition of $\mathrm{Def}(F/W(k))$:

Proposition 13.1.6. *Suppose F is p-typical. Then for every artinian local $W(k)$-algebra R, $Def(F/W(k))(R)$ is equal to the set of p-typical formal group laws $\tilde{F}$ over R such that $\tilde{F}_k = F$, modulo $\star$-isomorphisms between p-typical formal group laws.*

Proof. It suffices to show that every lifting $\tilde{G}$ of F is $\star$-isomorphic to a p-typical lifting. Let $\mathfrak{m}$ be the maximal ideal of R. Let $\psi : \tilde{\mathcal{R}}^{\infty} \to R$ be the homomorphism such that $\psi_* H_U = \tilde{G}$. Define $\tilde{F} := (\psi \circ \kappa)_* F_V$. By (10.3.8), H_U and $\kappa_* F_V$ are strictly isomorphic via $\varsigma : H_U \xrightarrow{\cong} \kappa_* F_V$, and $\varsigma(X) \equiv X \mod \tilde{\mathfrak{a}}$, where $\tilde{\mathfrak{a}}$ is the ideal of $\tilde{\mathcal{R}}^{\infty}_{(p)}$ generated by $p, U(i,\mathbf{n})$ with $\mathbf{n}$ running over all multi-indices that are not of the form $p^s \mathbf{e}(j)$. Since F is p-typical, by (10.3.7) $\psi(\tilde{\mathfrak{a}}) \subset \mathfrak{m}$. As a result, $\psi_* \varsigma(X) \equiv X \mod \mathfrak{m}$ and hence is a strict $\star$-isomorphism between $\tilde{G}$ and $\tilde{F}$. □

Let $\mathcal{F}$ be a universal p-typical lifting of F over $\mathcal{R}$, i.e., for every artinian local $W(k)$-algebra R and a p-typical lifting $\tilde{F}$ of F over R, there exists a unique $W(k)$-homomorphism $s : \mathcal{R} \to R$ such that $s_* \mathcal{F} = \tilde{F}$. For $\rho \in \mathrm{Aut}(F)$, the relabelling action $R_\rho : \mathcal{R} \to \mathcal{R}$ is the unique $W(k)$-endomorphism such that there exists an isomorphism $\rho_{\mathrm{univ}} : \mathcal{F} \to (R_\rho)_* \mathcal{F}$ making the reduction of ρ_{univ} over k equal to $\rho : F \to F$.

A natural approach to compute R_ρ is to first find another p-typical lifting $\hat{\mathcal{F}}$ of F over $\mathcal{R}$ satisfying: (a) there exists an isomorphism $\alpha_\rho : \mathcal{F} \to \hat{\mathcal{F}}$ such that the reduction of α_ρ over k is equal to $\rho : F \to F$; (b) there exists a $W(k)$-endomorphism $\mathcal{R} \to \mathcal{R}$ such that the pushforward of $\mathcal{F}$ is $\star$-isomorphic to $\hat{\mathcal{F}}$. Then the $W(k)$-endomorphism in (b) is the desired relabelling action R_ρ.

A p-typical lifting $\hat{\mathcal{F}}$ that satisfies (a) can be constructed by (10.4.8) via Honda coordinates (see 10.4.7). The formal group laws over $\mathcal{R}$ that are isomorphic to $\hat{\mathcal{F}}$ can be parametrized by the countably infinitely many indeterminates $T_1, T_2, \cdots$ valued in $\mathcal{R}^{m\times m}$ and U valued in $(\mathcal{R}^{m\times m})^\times$ (see 11.6.3), and to make them $\star$-isomorphic to $\hat{\mathcal{F}}$ is equivalent to take the entries of $T_1, T_2, \cdots$ and $U - I$ in the maximal ideal $\mathfrak{m}_\mathcal{R}$ of $\mathcal{R}$. We need an appropriate choice of F and $\mathcal{F}$ at the beginning such that the p-typical coordinates of $\mathcal{F}$ are simple enough to compute the relabelling action R_ρ explicitly as in (b). In this process, we need the translation formulas developed in chapter 11 between the various coordinates of p-typical formal group laws over $\mathcal{R}$. These recursive formulas are *integral* so that the information after modulo p can be read off.

13.2 The choice of formal group law and its universal p-typical lifting

Let X be a connected p-divisible group over k with dimension m and codimension n. In this subsection we prove that we could choose F and a universal lifting of F over $\mathcal{R}$ with a simple p-typical coordinate. The main result of this subsection is as follows:

Theorem 13.2.1. (a) *There exists over k a p-typical formal group law F whose associated p-divisible group is isomorphic to X, and the p-typical coordinate $a_1, a_2, \cdots$ of F satisfy the following property: there exist a non-negative integer d_j for $j = 1, 2, \cdots, m$, such that $a_l(i,j) = 0$ for all $l \leq d_j - 1$ and $i = 1, 2, \cdots, m$, the matrix $W := (a_{d_j}(i,j))_{i,j=1,2,\cdots,m} \in (k^{m\times m})^\times$, and $d_1 + d_2 + \cdots + d_m = n + m$.*

(b) *Let $A_l(i,j)$ be the Teichmuller lift of $a_l(i,j)$ in $W(k)$ for $i, j = 1, 2, \cdots, m$ and $l = 1, 2, \cdots$, where $a_l(i,j)$ is the (i,j)-th entry in the l-th p-typical coordinate of F as in (a). Let $S_l(i,j)$ be an indeterminate for $i = 1, 2, \cdots, m$, $j = 1, 2, \cdots, m$, $l = 1, 2, \cdots, d_j - 1$. Let $\mathcal{F}$ be the p-typical formal group law over $W(k)[[S]] := W(k)[[S_l(i,j); j = 1, 2, \cdots, m, i = 1, 2, \cdots, d_j - 1]]$ with p-typical coordinate $W_l(i,j) := S_l(i,j)$ if $l \leq d_j - 1$, and $W_l(i,j) := A_l(i,j)$ otherwise. Then $\mathcal{F}$ is a lifting of F, and the corresponding homomorphism $\Psi : \mathcal{R} \to W(k)[[S]]$ is an isomorphism.*

The idea to prove (a) is to find a special V-basis of the Cartier module attached

to X (see 10.5 for the definition and basic properties of Cartier theory), such that under the correspondence between Cartier modules equipped with a V-basis and formal group laws (10.5.25), the p-typical coordinate has the desired forms in (a). To prove (b), we apply (11.6.3) to modify any first order deformation of the chosen formal group law in (a) into special forms. This allows us to construct the homomorphism Ψ in (13.2.1(b)); a computation of the Kodaira-Spencer map shows that Ψ is an isomorphism.

Proposition 13.2.2. *Let M be the $Cart_p(k)$-module of the formal group attached to X. Then there exists a set of V-basis $\{e_1, \cdots, e_m\}$ of M, such that for $j = 1, 2, \cdots, m$, there exist $x_j \in M$ and a non-negative integer d_j, satisfying $F(e_j) = V^{d_j} x_j$, and $\{x_1, x_2, \cdots, x_m\}$ is a set of V-basis of M. Moreover, $d_1 + d_2 + \cdots + d_m = n + m$.*

Proof. Let $\{e_{1,1}, e_{1,2}, \cdots, e_{1,m}\}$ be a V-basis of M. Since the topology on M induced by filtration $M \supset VM \supset V^2M \supset \cdots$ is separated and F is injective, there exists integers $d_{1,1}, d_{1,2}, \cdots$ and $x_{1,1}, x_{1,2}, \cdots, x_{1,m} \in M$ such that

$$Fe_{1,j} = V^{d_{1,j}} x_{1,j}, \overline{x}_{1,j} \neq 0 \in M/VM, \quad \text{for } j = 1, 2, \cdots, m$$

Without loss of generality, we may and do assume $d_{1,1} = \min\{d_{1,j} | j = 1, 2, \cdots, m\}$. For $j = 2, 3, \cdots, m$, if $\overline{x}_{1,j} = \lambda \overline{x}_{1,1} \in \text{span}_k \overline{x}_{1,1}$ for some $\lambda \in k$, then we can replace $e_{1,j}$ with $e'_{1,j} := e_{1,j} - V^{d_{1,j} - d_{1,1}} \langle \lambda^{\sigma^{-1-d_{1,1}}} \rangle e_{1,1}$. Thus $Fe'_{1,j} = V^{d_{1,j}}(x_{1,j} - \langle \lambda \rangle x_{1,1})$, which can be written as $V^{d'_{1,j}} x'_{1,j}$ for some $d'_{1,j} > d_{1,j}$ and $x'_{1,j} \in M$. If $\overline{x}'_{1,j}$ is still

in $\mathrm{span}_k \overline{x}_{1,1}$, repeat this procedure. The procedure must stop at some point, since otherwise we would get

$$F(e_{1,j} - \sum_{i=0}^{\infty} V^i \langle c_{i,j} \rangle e_{1,1}) = 0$$

where $c_{i,j} \in k$. By the injectivity of F, $e_{1,j} = \sum_{i=0}^{\infty} V^i \langle c_{i,j} \rangle e_{1,1}$, which contradicts the fact that $\{e_{1,1}, e_{1,2}, \cdots, e_{1,m}\}$ is a V-basis. Therefore we can modify the V-basis $\{e_{1,1}, e_{1,2}, \cdots, e_{1,m}\}$ into a new V-basis $\{e_{2,1}, e_{2,2}, \cdots, e_{2,m}\}$ such that $Fe_{2,j} = V^{d_{2,j}} x_{2,j}$, where $d_{2,1} = \min\{d_{2,j} | j = 1, 2, \cdots, m\}$ and $\overline{x}_{2,1}, \overline{x}_{2,j}$ are k-linearly independent in M/VM for $j = 2, 3, \cdots, m$.

In general, suppose we have obtained a V-basis $\{e_{r,1}, e_{r,2}, \cdots, e_{r,m}\}$ such that $Fe_{r,j} = V^{d_{r,j}} x_{r,j}$, where $d_{r,1} \leq d_{r,2} \leq \cdots \leq d_{r,r-1} \leq \min\{d_{r,j} | j = r, r+1, \cdots, m\}$ and $\overline{x}_{r,1}, \overline{x}_{r,2}, \cdots, \overline{x}_{r,r-1}, \overline{x}_{r,j}$ are k-linearly independent in M/VM for $j = r, r+1, \cdots, m$. Without loss of generality, we may and do assume $d_{r,r} = \min\{d_{r,j} | j = r, r+1, \cdots, m\}$. We can modify $e_{r,j}$ as above if $\overline{x}_{r,j}$ is not in $\mathrm{span}_k\{\overline{x}_{1,1}, \cdots, \overline{x}_{1,r-1}\}$. Thus we can modify $\{e_{r,1}, e_{r,2}, \cdots, e_{r,m}\}$ into a new V-basis $\{e_{r+1,1}, e_{r+1,2}, \cdots, e_{r+1,m}\}$ such that $Fe_{r+1,j} = V^{d_{r+1,j}} x_{r+1,j}$, where

$$d_{r+1,1} \leq d_{r+1,2} \leq \cdots \leq d_{r+1,r} \leq \min\{d_{r+1,j} | j = r+1, r+2, \cdots, m\}$$

and $\overline{x}_{r+1,1}, \overline{x}_{r+1,2}, \cdots, \overline{x}_{r+1,r}, \overline{x}_{r+1,j}$ are k-linearly independent in M/VM for $j = r+1, r+2, \cdots, m$. In particular, when we reach $r = m$, we can take $e_j := e_{m,j}$, $d_j := d_{m,j}$, and $x_j := x_{m,j}$ in the proposition.

It remains to prove $d_1 + d_2 + \cdots + d_m = n + m$. It suffices to notice that

$\{V^i x_j | j = 1, 2, \cdots, m, i = 1, 2, \cdots, d_j - 1\}$ is a k-basis of M/FM, whose dimension over k is equal to n. $\square$

The proof of (13.2.1):

We first prove (a). Let F be the formal group law associated to the $\mathrm{Cart}_p(k)$-module M equipped with the V-basis $\{e_1, \cdots, e_m\}$ as in (13.2.2). Assume $\overline{x}_j = \sum_{i=1}^{\infty} x_{i,j}\overline{e}_i$ in M/VM, where $a_{i,j} \in k$. Let $a_1, a_2, \cdots$ be the p-typical coordinate of F. By (10.5.25), $a_l(i,j) = 0$ if $l \leq d_j$, and $a_{d_j}(i,j) = x_{i,j}$. The matrix $W := (w_{d_j}(i,j))_{i,j=1,2,\cdots,m}$ is invertible because $\overline{x}_1, \cdots, \overline{x}_m$ are linearly independent over k. Thus (a) is proved.

To prove (b), note that the p-typical coordinate defined for $\mathcal{F}$ reduces to the p-typical coordinate of F over k, hence $\mathcal{F}$ is a lifting of F. Let $\Psi : \mathcal{R} \to W(k)[[S]]$ be the homomorphism that induces $\mathcal{F}$ from the universal lifting. Since $\mathcal{R}$ is smooth by (13.1.2), to prove Ψ is an isomorphism it suffices to check the Kodaira-Spencer map induced by Ψ between the tangent spaces is an isomorphism. By (13.1.2) and (13.2.2), the dimensions of the two tangent spaces are both equal to mn. Therefore it suffices to prove that for every lifting G of F over $k[\varepsilon]/(\varepsilon^2)$ with p-typical coordinates $v_1, v_2, \cdots$, there exists a lifting G' of F over $k[\varepsilon]/(\varepsilon^2)$ such that G' is $\star$-isomorphic to G, and the p-typical coordinate $v'_1, v'_2, \cdots$ of G' has the form $v'_l(i,j) \in \varepsilon k[\varepsilon]/(\varepsilon^2)$ when $l \leq d_j - 1$, and $v'_l(i,j) = a_l(i,j)$ when $l \geq d_j$.

By (11.6.3), it suffices to find $\delta \in k^{m\times m}\varepsilon$ and $t_1, t_2, \cdots$ in $(k^{m\times m})^\times$ such that $v'_n = \Theta_n(\delta, v_1, \cdots, v_n, t_1, \cdots, t_n)$ (see 11.6.4 for the definition of Θ_n) has the above desired

properties. Let us consider the entries $v'_l(i,j)$ with $l \geq d_j$ first. With $v_1, \cdots, v_l$ fixed, we can view the (i,j)-entry of $\Theta_l(\delta, v_1, \cdots, v_l, t_1, \cdots, t_l) - a_l$ as a polynomial $P_{i,j,l}$ in $\delta, t_1, t_2, \cdots, t_l$, with the constant term equal to $v_l(i,j) - a_l(i,j) \in \varepsilon k[\varepsilon]/(\varepsilon^2)$, since $v_l(i,j)$ reduces to $a_l(i,j)$ after modulo ε. Consider the infinite system of polynomial equations in the order of

$$P_{1,1,d_1}, P_{1,2,d_2}, \cdots, P_{1,m,d_m}, P_{2,1,d_1}, P_{2,2,d_2}, \cdots, P_{m,m,d_m}, P_{1,1,d_1+1}, P_{1,2,d_2+1}, \cdots$$

Put the indeterminates of these equations in the order:

$$\delta(1,1), \delta(1,2), \cdots, \delta(1,m), \delta(2,1), \cdots, \delta(m,m), t_1(1,1), t_1(1,2), \cdots, t_1(m,m),$$
$$t_2(1,1), \cdots$$

The Jacobian matrix J_0 of the system of equations (see 12.2.3 for the definition of Jacobian) is a blockwise lower triangular matrix (see 12.1.5 for definition) whose diagonal blocks are $(i,j = 1, 2, \cdots, m)$:

$$\underbrace{(v_{d_j}(i,j)), \cdots, (v_{d_j}(i,j))}_{m \text{ times}}, \underbrace{(v_{d_j}(i,j)^p), \cdots, (v_{d_j}(i,j)^p)}_{m \text{ times}}, \underbrace{(v_{d_j}(i,j)^{(p^2)}), \cdots, (v_{d_j}(i,j)^{(p^2)})}_{m \text{ times}}$$

and so on.

Since v_l reduces to w_l over k, the diagonal blocks are all invertible $m \times m$ matrices over k due to (a). Therefore J_0 is a regular lower triangular matrix. According to (12.2.5), the system of equations has a unique solution $(\delta, t_1, t_2, \cdots)$ whose entries are in $\varepsilon k[\varepsilon]/(\varepsilon^2)$.

Let $v'_n := \Theta_n(\delta, v_1, \cdots, v_n, t_1, \cdots, t_n)$ for all n. We have proved $v'_l(i,j) = a_l(i,j)$ when $l \geq d_j$. When $l \leq d_j - 1$, the constant term of the (i,j)-th entry of Θ_l

is equal to $v_l(i,j)$, which reduces to $w_l(i,j) = 0$ over k. Since we have known the entries of all the parameters $\delta, t_1, t_2, \cdots, t_n$ are in $\varepsilon k[\varepsilon]/(\varepsilon^2)$, we deduce that $v'_l(i,j) \in \varepsilon k[\varepsilon]/(\varepsilon^2)$ when $l \leq d_j - 1$. This verifies our claim that every lifting of F over $k[\varepsilon]/(\varepsilon^2)$ is $\star$-isomorphic to a lifting whose p-typical coordinate $v'_1, v'_2, \cdots$ satisfies the property that $v'_l(i,j) \in \varepsilon k[\varepsilon]/(\varepsilon^2)$ when $l \leq d_j - 1$, and $v'_l(i,j) = a_l(i,j)$ when $l \geq d_j$. This proves $\Psi : \mathcal{R} \to W(k)[[S]]$ is an isomorphism, and the theorem is proved.

13.3 The algorithm of computing the relabelling action

Thanks to (13.2.1), we may and do identify $\mathcal{R}$ and the universal lifting of F with $W(k)[[S]]$ and $\mathcal{F}$ from now on. Let $\mathfrak{R} := (p, S)$ be the ideal of $\mathcal{R}$. Define $\sigma : \mathcal{R} \to \mathcal{R}$ by $\sigma|_{W(k)}$ =the Frobenius automorphism, and $\sigma(S_l) = S_l^{(p)}$. This makes $(\mathcal{R}, \mathfrak{a}, \sigma)$ into a Honda ring. Let $W_1, W_2, \cdots$ be the p-typical coordinate of $\mathcal{F}$. By (13.2.1), $W_l^\sigma = W_l^{(p)}$ for all $l = 1, 2, \cdots$. According to (11.1.6), the Honda coordinate and the p-typical coordinate of $\mathcal{F}$ coincide with each other.

Define $\eta := p - W_1\partial - W_2\partial^2 - \cdots \in \mathcal{R}_\sigma[[\partial]]^{m\times m}$, then $\log \mathcal{F}(X) = (p\eta^{-1}) * X$ by the definition of Honda coordinate (see 10.4.5 and 10.4.7). Let $h : \mathcal{R} \to W(k)$ be the homomorphism that sends $S_l(i,j)$ to 0. If we equip $W(k)$ with the obvious structure of Honda ring $(W(k), (p), \sigma)$, h is a homomorphism between Honda rings.

The image of $W_l(i,j)$ under h is equal to $A_l(i,j)$. Let $A_l :=$ the $m \times m$ matrix $(A_l(i,j))_{1\leq i,j\leq m}$ over R, then $h_*(\eta) = p - A_1\partial - A_2\partial^2 - \cdots \in W(k)_\sigma[[\partial]]^{m\times m}$, which we will denote by η_A from now on. By (10.4.8), we have the following description of $\mathrm{End}(X) \cong \mathrm{End}(F)$ in terms of Honda's non-commutative formal power series:

$$\{\theta \in W(k)_\sigma[[\partial]]^{m\times m} | \eta_A\theta\eta_A^{-1} \in W(k)_\sigma[[\partial]]^{m\times m}\}/W(k)_\sigma[[\partial]]^{m\times m}\eta_A \quad \stackrel{\cong}{\to} \quad \mathrm{End}(F)$$

by sending $c + \eta_A$ to $\overline{(\log \mathcal{F})^{-1}(c * \log \mathcal{F}(X))}$.

For $\rho \in \mathrm{Aut}(X) = \mathrm{End}(X)^\times$, let $c = c(\rho)$ be a twisted formal power series in $W(k)_\sigma[[\partial]]^{m\times m}$ such that $\overline{(\log \mathcal{F})^{-1}(c * \log \mathcal{F}(X))} = \rho$. Write $c = \sum\limits_{n=0}^{\infty} c_n\partial^n$, where $c_n \in W(k)^{m\times m}$ for all n, and $c_0 \in (W(k)^{m\times m})^\times$. The algorithm of computing the relabelling action $R_\rho : \mathcal{R} \to \mathcal{R}$ is as follows:

Step 1. Construct a formal group law $\hat{\mathcal{F}}$ over $\mathcal{R}$ such that there exists a homomorphism from $\mathcal{F}$ to $\hat{\mathcal{F}}$ that induces ρ over k. The p-typical coordinate $\hat{W}_1, \hat{W}_2, \cdots$ of $\hat{\mathcal{F}}$ can be computed based on $c_0, c_1, \cdots$ and the p-typical coordinate $W_1, W_2, \cdots$ by an integral recursive formula (see 11.3.1):

$$\begin{aligned}\hat{W}_n \;=\; & c_0^{-1}W_n c_0^{\sigma^n} - \sum_{i=1}^{n-1} c_0 c_{n-i}\hat{W}_i^{(p^{n-i})} + pc_0^{-1}c_n + \\ & \tfrac{1}{p}\sum_{k=1}^{n-1}\sum_{l=1}^{n-k} c_0^{-1}W_k c_0^{\sigma^k}\hat{a}_{n-k-l}^{\sigma^k}((\hat{W}_l^{\sigma^k})^{(p^{n-k-l})} - (\hat{W}_l)^{(p^{n-l})})\end{aligned}$$

where $\hat{a}_n = \sum\limits_{i_1+i_2+\cdots+i_r=n} p^{-t}\hat{W}_{i_1}\hat{W}_{i_2}^{(p^{i_1})}\cdots\hat{W}_{i_r}^{(p^{i_1+\cdots+i_{r-1}})} \in p^{-n}\mathcal{R}^{m\times m}$ such that

$$\log_{\hat{F}}(X) = \sum_{n=0}^{\infty}\hat{a}_n X^{p^n}$$

Step 2. Compute the formal group law $\mathcal{F}'$ over $\mathcal{R}$ which is $\star$-isomorphic to $\hat{\mathcal{F}}$ over $\mathcal{R}$ such that $\mathcal{F}'$ could be realized as the pushforward of $\mathcal{F}$ under an appropriate

endomorphism of $\mathcal{R}$. If we denote the p-typical coordinate of $\mathcal{F}'$ by $W_1', W_2', \cdots$, then by our knowledge on the p-typical coordinate of $\mathcal{F}$ (see 13.2.1) the latter requirement is equivalent to saying for all $i = 1, 2, \cdots, m$, we have $W_l'(i,j) = W_l(i,j)$ if $l \geq d_j$, and $W_l'(i,j) \equiv W_l'(i,j) \mod \mathfrak{m}_{\mathcal{R}}$ if $l \leq d_j - 1$. By (11.6.3), the p-typical coordinates of the $\star$-isomorphic p-typical formal group laws $\mathcal{F}'$ and $\hat{\mathcal{F}}$ are connected via a system of infinitely many polynomial equations in the parameters $D, T_1, T_2, \cdots$ and $W_l'(i,j)$ with $i, j = 1, 2, \cdots, m$, $l = 1, 2, \cdots, d_j - 1$:

$$\hat{W}_l(i,j) = \Theta_{l,i,j}(D, W_1', \cdots, W_l', T_1, \cdots, T_l), i, j = 1, 2, \cdots, m, l = 1, 2, \cdots \quad (13.3.a)$$

Proposition 13.3.1. *(a) For $i, j = 1, 2, \cdots, m$ and $l = 1, 2, \cdots, d_j - 1$, there exists a unique formal power series $P_{l,i,j}(D, T_1, T_2, \cdots, T_l)$ in $D, T_1, T_2, \cdots, T_l$, such that $\hat{W}_l(i,j) = \Theta_{l,i,j}(D, A_1 + P_1, \cdots, A_l + P_l, T_1, \cdots, T_l)$, where $P_l = (P_{l,i,j})_{i,j=1,2,\cdots,m}$, and $P_{l,i,j} := 0$ if $l \geq d_j$.*

(b) Let $\tilde{\Theta}_{l,i,j}(D, T_1, \cdots, T_l) := \Theta_{l,i,j}(D, A_1 + P_1, \cdots, A_l + P_l, T_1, \cdots, T_l)$, then the system of equations

$$\hat{W}_l(i,j) = \tilde{\Theta}_{l,i,j}(D, T_1, \cdots, T_l), i, j = 1, 2, \cdots, m, l = d_j, d_j + 1, \cdots$$

has a unique solution $(D, T_1, T_2, \cdots) = (\delta, t_1, t_2, \cdots)$ in $\mathfrak{m}_{\mathcal{R}}^{m \times m}$.

(c) Let $W_l' := P_l(\delta, t_1, \cdots, t_l)$, then $W_l' \equiv \hat{W}_l \equiv W_l \mod \mathfrak{m}_{\mathcal{R}}$ for all $l = 1, 2, \cdots$. In particular, the p-typical formal group law $\mathcal{F}'$ with p-typical coordinate $W_1', W_2', \cdots$ is $\star$-isomorphic to $\hat{\mathcal{F}}$.

Corollary 13.3.2. *The relabelling action $R_\rho : \mathcal{R} = W(k)[[S]] \to \mathcal{R} = W(k)[[S]]$ is*

the $W(k)$-endomorphism that sends $S_l(i,j)$ to $P_{l,i,j}(\delta, t_1, t_2, \cdots)$.

Proof of 13.3.1:

We first prove (a). By the definition of $\Theta_{l,i,j}$, if we evaluate $W'_s = A_s$, then $\Theta_{l,i,j}(D, A_1, \cdots, A_l, T_1, \cdots, T_l) \equiv A_l(i,j) \mod (p, D, T)$, where (D, T) is the ideal generated by the $D(i,j)$ and $T_l(i,j)$'s. On the other hand, since $\hat{\mathcal{F}}$ reduces to F over k, we have $\hat{W}_l(i,j) \equiv W_l(i,j) \equiv A_l(i,j) \mod \mathfrak{m}_{\mathcal{R}}$. Therefore if we write the equation as

$$\begin{aligned} & \Theta_{l,i,j}(D, A_1 + P_1, \cdots, A_l + P_l, T_1, \cdots, T_l) - \Theta_{l,i,j}(D, A_1, \cdots, A_l, T_1, \cdots, T_l) \\ = \;& \hat{W}_l(i,j) - \Theta_{l,i,j}(D, A_1, \cdots, A_l, T_1, \cdots, T_l) \end{aligned}$$

the right hand side is in $\mathfrak{m}_{\mathcal{R}}$. View this as a system Θ of mn polynomial equations in $P_l(i,j)$ with $i, j = 1, 2, \cdots, m$ and $l = 1, 2, \cdots, d_j - 1$, its Jacobian $J(\Theta)$'s evaluation at $P_1 = P_2 = \cdots = 0$ is congruent to the identity matrix modulo (p, D, T) (see 11.6.5). Now (a) follows from (12.2.7).

To prove (b), put the equations in the order of

$$\tilde{\Theta}_{d_1,1,1} - W_{d_1}(1,1) = \hat{W}_{d_1}(1,1) - W_{d_1}(1,1)$$

$$\tilde{\Theta}_{d_2,1,2} - W_{d_2}(1,2) = \hat{W}_{d_2}(1,2) - W_{d_2}(1,2)$$

$$\vdots$$

$$\tilde{\Theta}_{d_m,1,m} - W_{d_m}(1,m) = \hat{W}_{d_m}(1,m) - W_{d_m}(1,m)$$

$$\tilde{\Theta}_{d_1,2,1} - W_{d_1}(2,1) = \hat{W}_{d_1}(2,1) - W_{d_1}(2,1)$$

$$\vdots$$

$$\tilde{\Theta}_{d_m,m,m} - W_{d_m}(m,m) = \hat{W}_{d_m}(m,m) - W_{d_m}(m,m)$$

$$\tilde{\Theta}_{d_1+1,1,1} - W_{d_1+1}(1,1) = \hat{W}_{d_1+1}(1,1) - W_{d_1+1}(1,1)$$

$$\tilde{\Theta}_{d_2+1,1,2} - W_{d_2+1}(1,2) = \hat{W}_{d_2+1}(1,2) - W_{d_2+1}(1,2)$$

$$\vdots$$

The left hand sides are all polynomials in finitely many indeterminates among $D(i,j), T_l(i,j)$ and do not have constant terms since $W'_l(i,j) = W_l(i,j)$ when $l \geq d_j$. The right hand sides are all in $\mathfrak{m}_{\mathcal{R}}$. Denote by Ω the $m^2 \times m^2$ block matrix whose diagonal $m \times m$ blocks are $(W_{d_j}(i,j))_{1\leq i,j\leq m}$ and zero elsewhere. For every positive integer d, denote by $\Omega[-d]$ the $m^2 \times m^2$ block matrix whose diagonal $m \times m$ blocks are $(S_{d_j-d}(i,j))_{1\leq i,j\leq m}$ and zero elsewhere. If $d > d_j$, we treat $S_{d_j-d}(i,j) = 0$. Let $J_0(\tilde{\Theta})$ be the Jacobian $J(\tilde{\Theta})$'s evaluation at $\mathbf{0}$, then $J_0(\tilde{\Theta}) = J_1 + N_1$, where J_1 a blockwise lower triangular matrix with diagonal blocks equal to $\Omega, \Omega^{(p)}, \Omega^{(p^2)}, \cdots,$

and N_1 is a blockwise upper triangular matrix in the form

$$\begin{pmatrix} 0 & \Omega[-1]^{(p)} & \Omega[-2]^{(p^2)} & \Omega[-3]^{(p^3)} & \ddots \\ & 0 & \Omega[-1]^{(p^2)} & \Omega[-2]^{(p^3)} & \ddots \\ & & 0 & \Omega[-1]^{(p^3)} & \ddots \\ & & & 0 & \ddots \\ & & & & \ddots \end{pmatrix}$$

By (13.2.1) J_1 is regular. Since $\Omega[-d] = 0$ if $d > \max\{d_j | j = 1, 2, \cdots, m\}$, N_1 is row-converging. Therefore by (12.1.6) the Jacobian $J(\tilde{\Theta})$'s evaluation at $\mathbf{0}$ is row-converging with a row-converging right inverse. Note that each equation only involves finitely many indeterminates, hence the Jacobian $J(\tilde{\Theta})$ is equal to $J_0(\tilde{\Theta}) + N_0$, where N_0's entries are in $\mathfrak{x} \subset \mathcal{R}\langle \mathbf{X} \rangle$ and each row of N_0 only contains finitely many nonzero entries. By (12.2.5) and (12.2.6), (b) is proved.

To prove (c), it suffices to notice that $P_{l,i,j}$'s evaluation at $D = T_1 = T_2 = \cdots = 0$ is equal to $\hat{W}_l(i, j)$. Therefore $W'_l(i, j) \equiv \hat{W}_l(i, j) \mod \mathfrak{m}_{\mathcal{R}}$ when $l \leq d_j - 1$, while $\hat{W}_l \equiv W_l \mod \mathfrak{m}_{\mathcal{R}}$ follows from the construction of $\hat{\mathcal{F}}$. When $l \geq d_j$, $W'_l(i, j)$ was set to be equal to $W_l(i, j)$. This concludes the proof.

13.4 Asymptotic expansions of the relabelling action over the characteristic p fiber

We are interested in the endomorphism $\overline{R}_\rho$ of $\mathcal{R}/p\mathcal{R}$ induced by the relabelling action R_ρ. For the simplicity of notations, we use capital letter to implicate the p-typical coordinate of a p-typical formal group law over $\mathcal{R}$, and the regular letter to stand for its reduction modulo p. Since $\mathcal{R} \cong W(k)[[S]] := W(k)[[S_l(i,j); i,j = 1,2,\cdots,m, l = 1,2,\cdots,d_j-1]]$ by (13.2.1), we are reduced to computing $R_\rho(S_l(i,j))$ mod p in $k[[S]]$. In terms of the notations in (13.3), we want to compute $w'_l - w_l (= W'_l - W_l \mod p)$.

Definition 13.4.1. For $x \in k[[S]]$ (resp. $W(k)[[S]]$), let $\mathrm{ord}_u(x)$ be the largest integer d such that $x \in \mathfrak{m}^d$ (resp. $\mathfrak{m}_{\mathcal{R}}^d$). For $x = (x_{i,j}) \in k[[S]]^{m\times m}$ (resp. $W(k)[[S]]^{m\times m}$), let $\mathrm{ord}_u(x) := \min\{\mathrm{ord}_u(x_{i,j}) | 1 \le i,j \le m\}$.

There exist natural filtrations for $\rho \in \mathrm{Aut}(X)$ and $R_\rho \in \mathrm{Aut}(\mathcal{R}/p\mathcal{R})$ as analogies of ramification groups:

$$\mathrm{Aut}(X) \supset 1 + p\mathrm{End}(X) \supset 1 + p^2\mathrm{End}(X) \supset \cdots$$

and

$$\mathrm{Aut}(\mathcal{R}/p\mathcal{R}) \supset \mathrm{Fil}^2(\mathrm{Aut}(\mathcal{R}/p\mathcal{R})) \supset \mathrm{Fil}^3(\mathrm{Aut}(\mathcal{R}/p\mathcal{R})) \supset \cdots$$

where $\mathrm{Fil}^r(\mathrm{Aut}(\mathcal{R}/p\mathcal{R}))$ is defined to be

$$\{\varphi \in \mathrm{Aut}(k[[S]]) | \varphi(S_l(i,j)) \equiv S_l(i,j) \mathrm{mod} \mathrm{ord}_u \ge r, i,j = 1,\cdots,m, l = 1,2,\cdots\}$$

Note that $\mathrm{Fil}^r(\mathrm{Aut}(\mathcal{R}/p\mathcal{R}))$ does not depend on the choice of the coordinates $S_l(i,j)$. In fact, if $f : k[[S]] \to k[[S]]$ is an isomorphism and $\varphi(S) \equiv S \mod \mathrm{ord}_u \geq r$, then we also have $f^{-1} \circ \varphi \circ f(S) = f^{-1}(f(S) + \mathrm{ord}_u \geq r) \equiv S \mod \mathrm{ord}_u \geq r$ by Taylor expansion.

We would like to study the asymptotic behaviour of $\overline{R}_\rho$ as $\rho \to 1$, with respect to these two filtrations. Moreover, for fixed $\rho \in \mathrm{Aut}(X)$ and order N, we describe the process of computing $\overline{R}_\rho(S_l(i,j)) \mod \mathrm{ord}_u \geq N$.

Theorem 13.4.2. *If $M \geq \max\{d_j | j = 1, 2, \cdots, m\} - 1$ and $\rho \in 1 + p^M \mathrm{End}(X)$, then $R_\rho \in \mathrm{Fil}^{p^M} \mathrm{Aut}(X)$.*

Theorem 13.4.3. *Let M, N be given integers. There exists an integer $K = K(M,N)$ that only depends on M, N, and a polynomial $S_{l,i,j}(x_1, x_2, \cdots, x_K)$ (here x_s is short for m^2 indeterminates $x_s(1,1)$, $x_s(1,2), \cdots, x_s(m,m)$) with degree $\leq Np^{-M}$ over $k[[S]]$ that only depends on M, N and X, such that*

$$\overline{R}_\rho(S_l(i,j)) - S_l(i,j) \equiv \mathcal{S}_{l,i,j}(\hat{w}_{M+1} - w_{M+1}, \hat{w}_{M+2} - w_{M+2}, \cdots, \hat{w}_{M+K} - w_{M+K}) \mod ord_u \geq N$$

Before proving the theorems, we first make some notations.

- Let $c = c_0 + c_1\partial + c_2\partial^2 + \cdots$ be a twisted formal power series in $\mathcal{R}_\sigma[[\partial]]^{m \times m}$ that corresponds to $\rho \in \mathrm{Aut}(X)$.

- Let $\mathcal{I} := \mathrm{Map}(\{(l,i,j) | 1 \leq i,j \leq m, 1 \leq l \leq d_j - 1\}, \mathbb{N})$. If $I \in \mathcal{I}$, let S^I be short for $\prod S_l(i,j)^{I(l,i,j)}$.

- Write $\hat{W}_n(i,j) - W_n(i,j)$ in $\mathcal{R} \cong W(k)[[S]]$ as $\sum_{I\in\mathcal{I}} a_I S^I$ where $a_I \in W(k)$, define $\Delta(n,r;i,j) := \sum_{I:\mathrm{ord}_p(a_I)=r} a_I S^I$, and $\Sigma(n,r;i,j) := \sum_{l=0}^{r} \Delta(n,l)$. Define $\Delta(n,r) := (\Delta(n,r;i,j))_{1\le i,j\le m}$, and $\Sigma(n,r) := (\Sigma(n,r;i,j))_{1\le i,j\le m}$.

By these definitions we know that $\Sigma(n,r) = \Sigma(n,r-1) + \Delta(n,r)$, $\hat{W}_n - W_n = \sum_{r=0}^{\infty} \Delta(n,r)$, and $p^r | \Delta(n,r)$.

Proposition 13.4.4. *Suppose $c_0 = 1 + p^M\gamma_0$, $c_i = p^M\gamma_i$ for $i = 1, 2, \cdots$. If $r \le M-1$, then*

$$\begin{aligned}\Sigma(n,r) \equiv\ & \tfrac{1}{p}\sum_{i=1}^{n-1}\sum_{l=1}^{n-i}\sum_{s=1}^{p^{n-i-l}} W_i a_{n-i-l}^{\sigma^i}\tbinom{p^{n-i-l}}{s}(W_l^{(p^{n-l}-p^i s)} * (\Sigma(l,r)^{\sigma^i})^{(s)} - \\ & \tfrac{1}{p}\sum_{i=1}^{n-1}\sum_{l=1}^{n-i}\sum_{s=1}^{p^{n-l}} W_i a_{n-i-l}^{\sigma^i}\tbinom{p^{n-l}}{s}(W_l^{(p^{n-l}-s)} * \Sigma(l,r)^{(s)}) \\ & + \sum_{i=1}^{n-1}\sum_{l=1}^{n-i}\sum_{s=0}^{p^{n-i-l}-1} \tfrac{1}{p}\tbinom{p^{n-i-l}-1}{s} W_i W_1^{(p^i)} W_1^{(p^{i+1})}\cdots W_1^{(p^{n-l-1})} \\ & (W_l^{(p^i s)} * (\Sigma(l,r)^{\sigma^i})^{(p^{n-i-l}-s-1)} * \Delta(l,r+1)^{\sigma^i}) \mod p^{r+1}\end{aligned}$$

Proof. Recall from (see 11.3.1) that

$$\begin{aligned}\hat{W}_n =\ & c_0^{-1} W_n c_0^{\sigma^n} - \sum_{i=1}^{n-1} c_0 c_{n-i} \hat{W}_i^{(p^{n-i})} + p c_0^{-1} c_n + \\ & \tfrac{1}{p}\sum_{i=1}^{n-1}\sum_{l=1}^{n-i} c_0^{-1} W_i c_0^{\sigma^k} \hat{a}_{n-i-l}^{\sigma^i}((\hat{W}_l^{\sigma^i})^{(p^{n-i-l})} - (\hat{W}_l)^{(p^{n-l})})\end{aligned}$$

By (11.2.2), $c_0^{\sigma^i}\hat{a}_{n-i-l}^{\sigma^i} = \sum_{j=0}^{n-i-l} a_j^{\sigma^i} c_{n-i-l-j}^{\sigma^{i+j}} \equiv a_{n-i-l} \mod p^{M-(n-i-l)}\mathcal{R}$. By (11.1.2), $p^{n-i-l+1} | ((\hat{W}_l^{\sigma^i})^{(p^{n-i-l})} - (\hat{W}_l)^{(p^{n-l})})$. Since $r+1 \le M$, if we are only interested in $\hat{W}_n$ modulo p^{r+1}, we could replace $c_0^{\sigma^k}\hat{a}_{n-i-l}^{\sigma^i}$ with $a_j^{\sigma^i}$ in the formula. Based on similar reasons, we can simplify other terms in the formula into the following after modulo p^{r+1}:

$$\Sigma(n,r) \equiv \frac{1}{p}\sum_{i=1}^{n-1}\sum_{l=1}^{n-i} W_i a_{n-i-l}^{\sigma^i}((\hat{W}_l^{\sigma^i})^{(p^{n-i-l})} - (\hat{W}_l)^{(p^{n-l})}) \mod p^{r+1}$$

By (11.1.5), the right hand side modulo p^{r+1} is further congruent to

$$\begin{aligned}
&\tfrac{1}{p}\sum_{i=1}^{n-1}\sum_{l=1}^{n-i} W_i a_{n-i-l}^{\sigma^i}((W_l^{(p^i)}+\Sigma(l,r+1)^{\sigma^i})^{(p^{n-i-l})}-(W_l+\Sigma(l,r))^{(p^{n-l})})\\
\equiv\ &\tfrac{1}{p}\sum_{i=1}^{n-1}\sum_{l=1}^{n-i} W_i a_{n-i-l}^{\sigma^i}((W_l^{(p^i)}+\Sigma(l,r)^{\sigma^i})^{(p^{n-i-l})}-(W_l+\Sigma(l,r))^{(p^{n-l})})+\\
&\sum_{i=1}^{n-1}\sum_{l=1}^{n-i}\tfrac{1}{p^{n-i-l+1}} W_i W_1^{(p^i)} W_1^{(p^{i+1})}\cdots W_1^{(p^{n-l-1})}((W_l^{(p^i)}+\Sigma(l,r+1)^{\sigma^i})^{(p^{n-i-l})}\\
&-(W_l^{(p^i)}+\Sigma(l,r)^{\sigma^i})^{(p^{n-i-l})})
\end{aligned}$$

Note that

$$\begin{aligned}
&(W_l^{(p^i)}+\Sigma(l,r+1)^{\sigma^i})^{(p^{n-i-l})}-(W_l^{(p^i)}+\Sigma(l,r)^{\sigma^i})^{(p^{n-i-l})}\\
=\ &\sum_{s=0}^{p^{n-i-l}-1}\tbinom{p^{n-i-l}}{s} W_l^{(p^i s)} * ((\Sigma(l,r+1)^{\sigma^i})^{(p^{n-i-l}-s)}-(\Sigma(l,r)^{\sigma^i})^{(p^{n-i-l}-s)})\\
=\ &\sum_{s=0}^{p^{n-i-l}-1} W_l^{(p^i s)} * (\sum_{j=1}^{p^{n-i-l}-s}\tbinom{p^{n-i-l}}{s}\tbinom{p^{n-i-l}-s}{j}(\Sigma(l,r)^{\sigma^i})^{(p^{n-i-l}-s-j)}\\
&*(\Delta(l,r+1)^{\sigma^i})^{(j)})
\end{aligned}$$

In the last line, if we assume $p^\alpha || j$, then $\binom{p^{n-i-l}}{s}\binom{p^{n-i-l}-s}{j} = \binom{p^{n-i-l}}{j}\binom{p^{n-i-l}-j}{s}$ is divisible by $n-i-l-\alpha$ by (11.1.4). Thus the last line is divisible by $p^{j(r+1)+n-i-l-\alpha}$. Since $j(r+1)+n-i-l-\alpha \geq (r+1)+(n-i-l+j-\alpha-1) \geq (r+1)+(n-i-l+p^\alpha-\alpha-1)$, it would have no contribution to $\Sigma(n,r) \mod p^{r+1}$ unless $j = p^\alpha = \alpha+1$, which forces $j=1$ (here we have used the assumption that $p>2$). This proves

$$\begin{aligned}
&\tfrac{1}{p}\sum_{i=1}^{n-1}\sum_{l=1}^{n-i} W_i a_{n-i-l}^{\sigma^i}((W_l^{(p^i)}+\Sigma(l,r+1)^{\sigma^i})^{(p^{n-i-l})}-(W_l+\Sigma(l,r))^{(p^{n-l})})\\
\equiv\ &\tfrac{1}{p}\sum_{i=1}^{n-1}\sum_{l=1}^{n-i}\sum_{s=1}^{p^{n-i-l}} W_i a_{n-i-l}^{\sigma^i}\tbinom{p^{n-i-l}}{s}(W_l^{(p^{n-l}-p^i s)} * (\Sigma(l,r)^{\sigma^i})^{(s)})-\\
&\tfrac{1}{p}\sum_{i=1}^{n-1}\sum_{l=1}^{n-i}\sum_{s=1}^{p^{n-l}} W_i a_{n-i-l}^{\sigma^i}\tbinom{p^{n-l}}{s}(W_l^{(p^{n-l}-s)} * \Sigma(l,r)^{(s)})+\\
&\sum_{i=1}^{n-1}\sum_{l=1}^{n-i}\sum_{s=0}^{p^{n-i-l}-1}\tfrac{1}{p}\tbinom{p^{n-i-l}-1}{s} W_i W_1^{(p^i)} W_1^{(p^{i+1})}\cdots W_1^{(p^{n-l-1})}\\
&(W_l^{(p^i s)} * (\Sigma(l,r)^{\sigma^i})^{(p^{n-i-l}-s-1)} * \Delta(l,r+1)^{\sigma^i}) \mod p^{r+1}
\end{aligned}$$

This concludes the proof. □

Corollary 13.4.5. *Suppose* $c_0 = 1 + p^M\gamma_0$, $c_i = p^M\gamma_i$ *for* $i = 1, 2, \cdots$.

(*a*) *If* $n \leq M$, *then* $\hat{W}_n \equiv W_n \mod p^{M+1-n}$.

(*b*) $\hat{W}_{M+1} - W_{M+1} \equiv W_1 W_1^{(p)} \cdots W_1^{(p^{M-1})} \Delta(1, M)^{\sigma^M}$.

Proof. We claim that $\Sigma(n, r) = 0$ for $n + r \leq M$, and $\Delta(n, M + 1 - n) = W_1\Delta(n - 1, M + 2 - n)^\sigma$ for $2 \leq n \leq M + 1$. Prove the first claim by induction on n. When $n = 1$, $\hat{W}_1 = c_0^{-1} W_1 c_0^\sigma \equiv W_1 \mod p^M$, hence $\Sigma(1, r) = 0$ for $r \leq M - 1$. The induction step follows immediately from the formula in (13.4.4). As for the second claim, note that in the formula in (13.4.4), if $r = M + 1 - n$, then every $\Sigma(n', r')$ or $\Delta(n', r')$ that shows up in the formula satisfies $n' + r' \leq M + 1$, and the equality holds only in the term $W_1\Delta(n - 1, M + 2 - n)^\sigma$. This proves our claim, and the corollary follows immediately from the claim. □

Proof of 13.4.2:

We prove by induction on n and (decreasing) induction in r that $\mathrm{ord}_u\Delta(n, r) \geq p^{M-r}$ for $r = 0, 1, \cdots, M$ and $n = 1, 2, \cdots$. When $r = M$, it follows from the fact that $\hat{W}_n \equiv W_n \mod \mathfrak{m}_\mathcal{R}$. Suppose now $0 \leq r \leq M - 1$, $n \geq 1$ and we have proved for $r + 1$ and smaller n. In the formula in (13.4.4), each term either has a factor of $\Sigma(n', r)$ with $n' < n$, or has a factor of $\Delta(n', r + 1)^{\sigma^i}$ with $n' < n$ and $i \geq 1$. By the induction hypothesis, their orders are both at least p^{M-r}. This proves $\mathrm{ord}_u\Delta(n, r) \geq p^{M-r}$ for $r = 0, 1, \cdots, M$ and $n = 1, 2, \cdots$. In particular, since $\hat{W}_n - W_n \equiv \Delta(n, 0) \mod p$, we deduce that $\mathrm{ord}_u(\hat{w}_n - w_n) \geq p^M$.

Follow the notations in (13.3.1), apply (12.2.5) we have $\mathrm{ord}_u(\delta) \geq p^M$ and

$\mathrm{ord}_u(t_i) \geq p^M$ for $i = 1, 2, \cdots$. When $l \leq d_j - 1$,

$$W_l'(i,j) = W_l(i,j) + P_{l,i,j}(\delta, t_1, t_2, \cdots, t_l)$$

and $P_{l,i,j}(0, 0, \cdots, 0) = \hat{W}_l(i,j) - W_l(i,j)$. The condition that $M \geq \max\{d_j | j = 1, 2, \cdots, m\} - 1$ implies $\hat{W}_l(i,j) \equiv W_l(i,j) \mod p$ by (13.4.5). This proves

$$\mathrm{ord}_u(w_l'(i,j) - w_l(i,j)) \geq p^M$$

when $l \leq d_j - 1$. When $l \geq d_j$, $w_l'(i,j) = w_l(i,j)$. This concludes the proof of (13.4.2).

Proof of 13.4.3:

By (13.3.1),there exist $\Delta, T_1, T_2, \cdots \in W(k)[[S]]\langle \mathbf{X} \rangle$, and formal power series $P_{l,i,j}$ over $W(k)[[S]]$ for each $l \leq d_j - 1$ such that $R_\rho(S_l(i,j)) - S_l(i,j) = W_l'(i,j) - W_l(i,j)$ is equal to $P_{l,i,j}(\delta, t_1, t_2, \cdots, t_l)$, where $\delta = \Delta(\hat{W}_l(i,j) - W_l(i,j); i, j = 1, 2, \cdots, m, l \geq d_j)$, $t_n = T_n(\hat{W}_l(i,j) - W_l(i,j); i, j = 1, 2, \cdots, m, l \geq d_j)$ are solutions to infinitely many polynomial equations as in (13.3.1 (b)). Replace $\delta, t_1, t_2, \cdots$ with $\Delta, T_1, T_2, \cdots$ in $P_{l,i,j}$, we write

$$R_\rho(S_l(i,j)) - S_l(i,j) := Q_{l,i,j}(\hat{W}_l(i,j) - W_l(i,j); i, j = 1, 2, \cdots, m, l \geq d_j)$$

as formal power series in $\hat{W}_l(i,j) - W_l(i,j)$. Note that $\Delta, T_1, T_2, \cdots$ do not depend on ρ. Since $M \geq \max\{d_j | j = 1, 2, \cdots, m\} - 1$, by (13.4.5) $\hat{W}_l(i,j) \equiv W_l(i,j)$ for $l \leq d_j - 1$. Therefore after modulo p, $\overline{P}_{l,i,j}$ does not depend on ρ, either. As a result, $\overline{R}_\rho(S_l(i,j)) = \overline{Q}_{l,i,j}(\hat{w}_l(i,j) - w_l(i,j); i, j = 1, 2, \cdots, m, l \geq d_j)$ only depends on X.

Let $\mathcal{I}' := \{(i,j,l)|i,j = 1,2,\cdots,m, l \geq d_j\}$. Write $\overline{Q}_l(i,j)(X_l(i,j);(i,j,l) \in \mathcal{I}')$ in the form of $\sum_J a_J X^J$, where $a_J \in k[[S]]$ and J runs over all the maps from $\mathcal{I}'$ to $\mathbb{N}$ sending all but finitely many triples (i,j,l) to zero. Let $d(J)$ be the number of triples (i,j,l) whose images under J are non-zero. By (13.4.2), $\mathrm{ord}_u(\hat{w}_l(i,j) - w_l(i,j)) \geq p^M$. Therefore when $d(J) \geq Np^{-M}$, $\mathrm{ord}_u(a_J X^I) \geq N$ when we evaluate at $X_l(i,j) = \hat{w}_l(i,j) - w_l(i,j)$. Since $\overline{Q}_{l,i,j} \in k[[S]]\langle \mathbf{X} \rangle$, there are only finitely many J satisfying $d(J) \leq Np^{-M}$ and $\mathrm{ord}_u a_J \leq N$. Let $\mathcal{J}$ be the set of J that satisfies $d(J) \leq Np^{-M}$ and $\mathrm{ord}_u a_J \leq N$. Define $\mathcal{S}_{l,i,j}(X_l(i,j);(i,j,l) \in \mathcal{I}') := \sum_{J \in \mathcal{J}} a_J X^J$, then $\overline{R}_\rho(S_l(i,j)) - S_l(i,j) \equiv \mathcal{S}_{l,i,j}(\hat{w}_l(i,j) - w_l(i,j);(i,j,l) \in \mathcal{I}') \mod \mathrm{ord}_u \geq N$. By (13.4.5) $\hat{w}_l(i,j) - w_l(i,j) = 0$ if $l \leq M$. Therefore $\mathcal{S}_{l,i,j}$ is in fact a polynomial of $\hat{w}_{M+1} - w_{M+1}, \hat{w}_{M+2} - w_{M+2}, \cdots, \hat{w}_{M+K} - w_{M+K}$ with degree $\leq Np^{-M}$. The proof is now completed.

Bibliography

[1] C-L. Chai, B. Conrad & F. Oort, *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs, volume 195, American Mathematical Society, 2013.

[2] C.-L. Chai, *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli*, Inventiones mathematicae 121.1 (1995): 439-479.

[3] C.-L. Chai, *The group action on the closed fiber of the Lubin-Tate moduli space*, vol. 82, no. 3. Duke Mathematical Journal (C), 1996.

[4] E. Devinatz, *Morava's change of rings theorem*, in: The Cech centennial (Boston, MA, 1993), Contemp. Math. 181, Amer. Math. Soc. (1995): 83-118.

[5] G. Faltings & C-L. Chai, *Degeneration of abelian varieties*. Ergebnisse der Mathematik 22, Springer-Verlag, New York, 1990.

[6] O. Goldman, *Determinants in projective modules*, Nagoya Mathematical Journal 18 (1961): 27-36.

[7] M. Hopkins and B. Gross, *Equivariant vector bundles on the Lubin-Tate moduli space*, Contemporary Mathematics 158 (1994): 23-88.

[8] M. Hazewinkel, *Formal groups and applications*, Academic Press, 1978.

[9] A. J. de Jong, *Crystalline Dieudonné module theory via formal and rigid geometry*. Publ. Math. IHES 82 (1995): 5-96.

[10] N. Katz, *Serre-Tate local moduli*, Lect. Notes Math. 868, Springer-Verlag (1981): 138-202.

[11] M. Kisin, *Modularity of 2-adic Barsotti-Tate representations*, Invent. Math. (2009): 587-634.

[12] M. Kisin, Moduli of finite flat group schemes, and modularity, Ann. of Math.(2) 170, no. 3 (2009): 1085-1180.

[13] T. Liu, *Torsion p-adic Galois Representation and a Conjecture of Fontaine*, Ann. Scient. de l'E.N.S., vol. 40, no. 4 (2007): 633-674.

[14] J. Lubin and J. Tate, *Formal moduli for one-parameter formal Lie groups*, Bulletin de la Socit Mathmatique de France 94 (1966): 49-59.

[15] J. Lurie, *Chromatic homotopy theory*, Lecture notes online.

[16] J. Morava, *Noetherian localisations of categories of cobordism comodules*, Ann. of Math. 121 (1985): 1-39.

[17] W. Messing, *The crystals associated to Barsotti-Tate groups*, Springer Berlin Heidelberg, 1972.

[18] F. Oort, *CM-liftings of abelian varieties*, Journ. Alg. Geom. 1 (1992): 131-146.

[19] D. Quillen, *On the formal group laws of oriented and unoriented cobordism theory*, Bull. Amer. Math. Soc. 75 (1969): 1293-1298.

[20] J. P. Serre & J. Tate, *Good reduction of abelian varieties*, Ann. Math. 88(1965): 492-517.

[21] S. Shatz, *Group schemes, formal groups, and p-divisible groups*. In Arithmetic geometry(G. Cornell & J. Silverman, ed.), Springer-Verlag, New York, 1986.

[22] G. Shimura & Y. Taniyama, *Complex Multiplication of Abelian Varieties and Its Application to Number Theory*, Math. Soc. Japan, 1961.

[23] J. Tate, *p-divisible groups*. In Proc. conference on local fields (T.Springer ed.), Springer-Verlag (1967): 158-183.

[24] T. Zink, *Cartiertheorie kommutativer formaler Gruppen*, Teubner-Texte zur Mathematik 68.