STRONG CM LIFTING PROBLEM II

TAISONG JING

VERSION: 01/09/2014

ABSTRACT. Let R_0 be a complete discrete valuation ring of mixed characteristic, $\mathcal{X}$ be a p-divisible group over R_0, and X be the closed fiber of $\mathcal{X}$. We say a subgroup G of X is potentially liftable, if after a finite base change G lifts to a finite locally free subgroup scheme of $\mathcal{X}_R$, where R/R_0 is a finite extension. In this article, we compute the complete list of potentially liftable subgroups in a first non-trivial example, where $\mathcal{X}$ is a CM p-divisible group with height 4 and dimension 2. As an application, we obtain a new type of counterexamples to the question of strong CM lifting.

1. INTRODUCTION

This is a continued work of [5] on strong CM lifting problem (sCML). The question (sCML) for abelian varieties asks whether every g-dimensional abelian variety over a finite field $\mathbb{F}_q$ with an action by the whole ring of integers in a CM field L of degree $2g$ admits an L-linear CM lifting to characteristic 0. This problem can be reduced to a question on lifting subgroups of CM p-divisible groups. Namely, if F is a p-adic local field and $\mathcal{X}$ is an $\mathcal{O}_F$-linear CM p-divisible group over a complete discrete valuation ring R of characteristic 0 with residue field $\overline{\mathbb{F}}_p$, which $\mathcal{O}_F$-stable subgroup of the closed fiber $\mathcal{X}_{\overline{\mathbb{F}}_p}$ is liftable into a finite locally free subgroup scheme of $\mathcal{X}$? In §6 of [5] we gave a condition on p-adic CM type of $\mathcal{X}$ such that every $\mathcal{O}_F$-stable subgroups of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ is liftable into a finite locally free subgroup scheme of the base change of $\mathcal{X}$ to a finite extension of R. In these examples, the p-adic CM type is induced from an unramified extension of $\mathbb{Q}_p$. As a corollary we proved that the answer to question (sCML) for abelian varieties is affirmative when every place v above p in the maximal totally real subfield L_0 is inert in L.

A complete answer to the question on lifting $\mathcal{O}_F$-stable subgroups of the closed fiber $\mathcal{X}_{\overline{\mathbb{F}}_p}$ to characteristic 0 requires us to consider all finite subgroups of the geometric generic fiber of $\mathcal{X}$, and compute the reduction 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 this article, we will study an example of $\mathcal{O}_F$-linear CM p-divisible group $\mathcal{X}$ 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. The answer is surprising to us: whether a finite subgroup of the geometric generic fiber of $\mathcal{X}$ 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 $\mathcal{X}_{\overline{\mathbb{F}}_p}[\pi_0^n]$, i.e., the kernel of multiplication on $\mathcal{X}_{\overline{\mathbb{F}}_p}$ 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 $\mathcal{X}_{\overline{\mathbb{F}}_p}[\pi_0^n]$ and $\mathcal{X}_{\overline{\mathbb{F}}_p}[\pi_0^{n+1}]$, and we have a description on its embedding in $\mathcal{X}_{\overline{\mathbb{F}}_p}[\pi_0^{n+1}]$; see (Theorem 2.3). This result indicates that the subgroups of the geometric generic fiber of $\mathcal{X}$ 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 conditions on Φ so far.

We use the theory of Kisin modules from integral p-adic Hodge theory as the main tool. A Kisin module is a $W(\kappa)[[u]]$-module satisfying certain additional conditions, where κ is a perfect field of characteristic p and $W(\kappa)$ is the ring of Witt vectors over κ. There is a p-divisible group or a finite locally free subgroup scheme in mixed characteristic associated 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 [2] (B.4.17) or [5] (3.2.2). The localized $W(\kappa)((u))$-module of the Kisin module carries the information on the generic fiber. In [5] (5.2.7), via the theory of Lubin-Tate formal group law we have computed elements in Kisin modules such that they correspond to the torsion points on the geometric generic fiber of the p-divisible group. Such elements generate the $W(\kappa)((u))$-module attached to a finite locally free subgroup scheme. After that, the computation of the closed fiber of a finite locally free subgroup scheme is reduced to a computation of the $W(\kappa)[[u]]$-module before inverting u; see (3.7.1) and (3.7.2). This computation is possible because of our knowledge on the torsion points, based on the explicit information on their coordinates given by the Lubin-Tate theory; see (3.6.2) and (3.6.3).

In the example of the $\mathcal{O}_F$-linear CM p-divisible group $\mathcal{X}$ 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 $\mathcal{X}$. This leads to a counterexample of (sCML). In §2 and §4 of [5], we studied the counterexamples of (sCML) coming from an extra symmetry on the Lie type of the closed fiber. That symmetry is caused by "small" residue fields of the reflex fields of the p-adic CM types in the sense of [5] (4.1). In the new counterexample in this article, however, 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 §4 of [5].

Besides that, we also study the F-linear CM lifting for $\mathcal{O}_F$-linear CM p-divisible groups over $\overline{\mathbb{F}}_p$, such that the p-adic CM type Φ of the lifting *cannot* be induced from an unramified extension of $\mathbb{Q}_p$. Let F_0 be the minimal subfield of F such that Φ is induced by a p-adic CM type for F_0. In the case when the ramification index of F_0 is small, we can prove a property similar to the one we proved in §6 of [5]: if $\mathcal{X}$ is an $\mathcal{O}_F$-linear CM p-divisible group with p-adic CM type Φ over a complete discrete valuation ring R of characteristic 0 with residue field $\overline{\mathbb{F}}_p$, then every $\mathcal{O}_F$-stable subgroup of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ lifts to a finite locally free subgroup scheme of the base change of $\mathcal{X}$ to a finite extension of R. This property on lifting $\mathcal{O}_F$-stable subgroups of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ is stronger than saying that every $\mathcal{O}_F$-linear CM p-divisible group isogeneous to $\mathcal{X}_{\overline{\mathbb{F}}_p}$ admits an F-linear CM lifting with p-adic CM type Φ; for the precise statement and an explanation on the property, see (3.1). As a corollary, we prove that the answer to question (sCML) is affirmative under the following broader condition 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 splits in L and the ramification index $e(v) < p - 1$; see (2.3.2). On the other hand, this strong lifting property on $\mathcal{O}_F$-stable subgroups of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ may fail to hold if the ramification index of F_0 is high; see Example (3.1.2). This observation indicates the subtlety in F-linear CM lifting with p-adic CM type Φ that cannot be induced from an unramified extension of $\mathbb{Q}_p$.

Acknowledgement. This work is part of the author's doctorial dissertation. Many thanks to C.-L. Chai for introducing the question to me and for many discussions and encouragement. I also thank F. Oort for his

questions and suggestions. I thank Institute of Mathematics, Academia Sinica for hospitality during the first half of 2013, where the main part of this work was done.

2. Reductions of finite locally free subgroup schemes

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.

Definition 2.1. Let R_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 R_0. A finite subgroup G of $\mathcal{X}_{\kappa_0}$ is said to be *potentially liftable*, if there exists a finite extension R over R_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, 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 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 [5] (Thm. 6.1), 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 (3.2), 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 (3.1).

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 (2.5.1 (b)), the computation is trivial simply because the closed fiber $\mathcal{X}_k$ "does not have many subgroups". In this section, we will compute a first non-trivial example.

2.2. **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 Dieudonne 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 Dieudonne 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 $[a_1c, b_1c^p] = [a_2, b_2]$ in $\mathbb{P}^1(k)$. Denote the equivalent classes on $\mathbb{P}^1(k)$ by $\mathfrak{Q}$. The set $\mathfrak{Q}$ 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 $\mathfrak{Q}$. 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 Dieudonne 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 $\delta_n(G) \in \mathfrak{Q}$ 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 2.3. *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 $\mathfrak{Q}$.

(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 (2.3) has the following consequences:

Corollary 2.4. *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 (2.3 (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 (2.3 (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 Dieudonne 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 2.4.1. As a corollary, the answer to question (sCML) relative to (F, F^{ur}) for p-divisible groups is negative; see [5] (3.1.8) for the precise statement of the question. 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 [5] (4.1). Thus we obtain a new counterexample to question (sCML) that does not fall in the framework in §4 of [5].

Corollary 2.5. *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 (2.4.1), [5] (4.1), and [5] (3.1.10). □

The most interesting phenomenon revealed by Theorem (2.3) 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 2.5.1. (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 $F_1 \subsetneq F$. 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 (2.3), we can say $d(\Phi) = 1$ in our example.

In the rest of the section we prove Theorem (2.3). 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 (2.6), we recall the comstructions from §5 of [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 Dieudonne 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 (2.6), we reduce the statements in Theorem (2.3) about the

closed fiber $\mathcal{G}_k$ to the existence of certain special elements in $\mathfrak{N}$; see (2.6)(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] (5.2). In (2.7) 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 (2.8), and then summarize a general linear algebra approach in (2.9). 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 (2.10). 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 (2.9); see the example (2.10.3) at the end of (2.10). In (2.11), we explain how the Serre dual of $\mathcal{X}_{O_{E_m}}$ comes to rescue for the problem. Finally in (2.12) 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 (2.3).

If $\mathfrak{M}$ is a Kisin module (or a finite Kisin module), and $x \in \mathfrak{M}^0 := W(k)((u)) \otimes_{W(k)[[u]]} \mathfrak{M}$, 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 $x_1 \equiv x_2 \mod \mathrm{ord}_u\, \geq D$.

2.6. **The Kisin modules attached to $\mathcal{X}$ and its base changes.** Now we prepare to prove Theorem (2.3). We first recall the constructions from §5 of [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 $E_m := B(k)(\pi_m)$. 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 §5 of [5] with (E_m, π_m), and let $\mathcal{X}_m$ be the associated p-divisible group over O_{E_m}. By [5] (5.2.7), $\mathcal{X}_m$ is the O_F-linear CM p-divisible group over 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 [5] (3.1.5) and (5.1.7), $\mathcal{X}_m$ is isomorphic to $\mathcal{X}_{O_{E_m}}$, and the isomorphism induces identity over the closed fiber. Thus to prove Theorem (2.3), 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] (5.1), the Kisin module $\mathfrak{M}_m = W(k)[[u]] \otimes_{\mathbb{Z}_p} O_F e$ with the natural O_F-action, and the (ϕ, 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 $W(k)[[u]] \otimes_{\mathbb{Z}_p} O_F e$ with $W(k) \otimes_{1,O_{F^{\mathrm{ur}}}} O_F[[u]]e_1 \oplus W(k) \otimes_{2,O_{F^{\mathrm{ur}}}} O_F[[u]]e_2 \cong W(k)[\pi][[u]]/(\pi^2 - \epsilon p)e_1 \oplus W(k)[\pi][[u]]/(\pi^2 - \epsilon^\sigma p)e_2$. Under such an identification, one can check that $a \cdot e_1 = ae_1$, $a \cdot e_2 = a^\sigma e_2$ for $a \in O_{F^{\mathrm{ur}}}$, and $\pi_0 \cdot e_i = \pi e_i$. The (ϕ, 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 Dieudonne module; by [2] (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" O_F-basis of $M(X_m)$ (see the beginning of the section for the definition of a "good" 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 (2.3(1)), it suffices to show:

(2.6.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 $x_s \in W(k)^\times$.

(2.6.b) When $t = 2n+1$ is odd, there exists $w \in \mathfrak{R}$ 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 (2.3(2)) it suffices to show:

(2.6.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 $\mathfrak{R}$ satisfying $w \equiv x_1\pi^{-(n+1)}e_1 + x_2\pi^{-(n+1)}e_2 \mod u$.

2.7. **The finite Kisin modules attached to finite locally free subgroup schemes.** To achieve the goals in 2.6, 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] (5.2.7), 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 $\mathfrak{R}_A^0 := W(k)((u))\{\eta \cdot v | \eta \in p^{-m}\mathcal{O}_F/\mathcal{O}_F\}$, and $\mathfrak{R}_A := \mathfrak{R}_A^0 \cap p^{-m}\mathfrak{M}_m/\mathfrak{M}_m$. 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 $\mathfrak{R}_A/(\mathfrak{R}_A \cap up^{-m}\mathfrak{M}/\mathfrak{M}) \cong (\mathfrak{R}_A + up^{-m}\mathfrak{M}_m/\mathfrak{M}_m)/(up^{-m}\mathfrak{M}_m/\mathfrak{M}_m)$ by $\mathfrak{R}_A \mod u$, then $\mathfrak{R}_A \mod u$ is the Dieudonne 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 $h^{(2m-1)}(u) \equiv \sum_{i=0}^{2m-1} \pi^i A_i(u) \mod p^m$, such that $A_i(u) \in W(\mathbb{F}_{p^2})((u))^\times$ and $\mathrm{ord}_u A_i = p^{2(2m-1-i)}$. Therefore

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

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:

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

Definition 2.7.1. Define

$$\begin{aligned} &\pi_1 := \pi && \pi_2 := \tau\pi = \lambda^{-1}\pi \\ &b_n := \textstyle\sum \lambda^{2i} A_{2i}(u)^\phi A_{n-2i}(u), && c_n := \textstyle\sum \lambda^{2i+1} A_{2i+1}(u)^\phi A_{n-2i-1}(u) \\ &y_j := b_j - c_j, && z_j := b_j + c_j \end{aligned}$$

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

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 2.7.2. 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 $v(\eta) = -2k$ (resp. $v(\eta) = -2k+1$). Define

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

Under such notations, one can check $\eta \cdot v = \sum_{s=1}^{2}\sum_{r=1}^{2m} \pi_s^{-r} v[\eta, r, s]e_s$; when $r > -v(\eta)$ 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 2.7.3. *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 $ord_u\, v[\eta, r, s] = p^{4m-2+v(\eta)+r}d$; in particular, it is independent of s and increasing in r.

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

(7) Let i, j be different integers between 0 and $2m-1$, and suppose $\gamma \in W(\mathbb{F}_{p^2})^\times$. Then $\gamma y_iy_j \pm \gamma^\sigma\lambda z_iz_j$, $\gamma z_iz_j \pm \gamma^\sigma\lambda y_iy_j$, and $\gamma y_iz_j \pm \gamma^\sigma\lambda z_iy_j$ 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 (2.7.4) 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 $y_iz_{i-2} - z_iy_{i-2} = (b_i - c_i)(b_{i-2} + c_{i-2}) - (b_i + c_i)(b_{i-2} - c_{i-2}) = 2b_ic_{i-2} - 2b_{i-2}c_i$, 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 2.7.4. *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 $ord_u\, x = ord_u\, y$.* □

2.8. **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 2.8.1. Let $m \ge 1$, $\eta \in p^{-1}\mathcal{O}_F/\mathcal{O}_F$, 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 $p^{4m-2+v(\eta)+j}d$. Let $w := u^{-p^{4m-2+v(\eta)+j}d}(\eta \cdot v)$, 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 (2.6.b) is achieved.

Example 2.8.2. Let $m \geq 2$, $\eta \in (p^{-2}O_F/O_F)\backslash(p^{-1}O_FO_F)$, $A = \langle\eta\rangle \cong \mathbb{Z}/p^2$. 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 $w_1^{(1)}$, $w_1^{(1)} - \pi_1^{-1}e_1$ is equal to $(v[p\eta,1,2]v[\eta,1,1] - v[\eta,1,2]v[p\eta,1,1])^{-1}\sum_{s=1}^{2}\sum_{r=2}^{4}(v[p\eta,1,2]v[\eta,r,s] - v[\eta,1,2]v[p\eta,r,s])e_s$. It suffices to:

(2.8.2.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);

(2.8.2.b) For $s = 1, 2$ and $r > 1$, show

$$\mathrm{ord}_u\,(v[p\eta,1,2]v[\eta,r,s] - v[\eta,1,2]v[p\eta,r,s]) > \mathrm{ord}_u\,(v[p\eta,1,2]v[\eta,1,1] - v[\eta,1,2]v[p\eta,1,1])$$

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 (2.7.3)(6) and Lemma 2.7.4, 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 $r \geq 2$, $\mathrm{ord}_u\, v[\eta, r, s] \geq dp^{4m-2+\nu(\eta)+r} \geq dp^{4m+\nu(\eta)}$, $\mathrm{ord}_u\, v[p\eta, r, s] \geq dp^{4m-2+\nu(p\eta)+r} \geq dp^{4m+2+\nu(\eta)}$. 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 (2.6.a) is achieved.

Example 2.8.3. Let $m \geq 3$, $\eta \in (p^{-3}O_FO_F)\backslash(p^{-2}O_FO_F)$, and $A = \langle\eta\rangle \cong \mathbb{Z}/p^3$. Take $A_1 := \langle p\eta\rangle \cong \mathbb{Z}/p^2$. By Example (2.8.2), 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, hence $u^{-dp^{4m+\nu(\eta)}}v[\eta, 2, s]$ 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 (2.6.b).

Example 2.8.4. Let $m \geq 1$, $\eta_1, \eta_2 \in p^{-1}O_F/O_F$, 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 $v[\eta_1,1,1]v[\eta_2,1,2] - v[\eta_2,1,1]v[\eta_1,1,2] = \epsilon^2(\alpha_1 y_1 + \beta_1 y_0)\alpha_2^\sigma \lambda z_0 - \epsilon^2(\alpha_1^\sigma y_1 + \beta_1^\sigma \lambda y_0)\alpha_2 y_0 = \epsilon^2(\alpha_1\alpha_2^\sigma \lambda y_1 z_0 - \alpha_1^\sigma \alpha_2 y_0 z_1)$ + Higher order terms. By Proposition 2.7.3 (7), we see the claim is true.

When $\nu(\eta_1) = \nu(\eta_2)$, $v[\eta_1,1,1]v[\eta_2,1,2] - v[\eta_2,1,1]v[\eta_1,1,2] = \epsilon^2(\alpha_1 y_{-\nu(\eta_1)-1} + \beta_1 y_{-\nu(\eta_1)-2})\alpha_2^\sigma z_{-\nu(\eta_2)-1} - \epsilon^2(\alpha_1^\sigma y_{-\nu(\eta_1)-1} + \beta_1^\sigma \lambda y_{-\nu(\eta_1)-2})\alpha_2 y_{-\nu(\eta_1)-1} = \epsilon^2(\alpha_1\alpha_2^\sigma - \alpha_1^\sigma\alpha_2)y_{-\nu(\eta_1)-1}z_{-\nu(\eta_1)-1}$ + Higher order terms. 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 $\mathrm{ord}_u\ (v[\eta_2,1,2]v[\eta_1,2,s] - v[\eta_1,1,2]v[\eta_2,2,s]) - \mathrm{ord}_u\ (v[\eta_1,1,1]v[\eta_2,1,2] - v[\eta_2,1,1]v[\eta_1,1,2]) \geq d(p^{4m+\nu(\eta_1)} + p^{4m-1+\nu(\eta_2)}) - d(p^{4m-1+\nu(\eta_1)} + p^{4m-1+\nu(\eta_2)}) = d(p^{4m+\nu(\eta_1)} - p^{4m-1+\nu(\eta_1)})$. 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 (2.6.a) is achieved.

2.9. **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 2.9.1. *Suppose $A \subset p^{-m}O_F/O_F$, $v_1, v_2, \cdots, v_{2n}$ 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 (2.9.1), 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 2.9.2. 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 $\sum_{j=1}^{k} \mathrm{ord}_u (C[\sigma(j), j]) \geq \sum_{j=1}^{k} \mathrm{ord}_u (C[\tau(j), j])$; 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 2.9.3. *Notations as in Definition (2.9.2). 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.

2.10. **The proof of Theorem (2.3) 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 $p^{-m}O_F/O_F$, then we have $r(A) \leq r(p^{-m}O_F/O_F) = 4$. 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 $p^{-1}O_F/O_F \subset A$, 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 2.3 in the case when $\mathcal{G} = \mathcal{G}_A$ such that $r(A) \leq 2$. Suppose $A = \langle \eta_1 \rangle \times \langle \eta_2 \rangle$, $\eta_i \in (p^{-m_i}O_F/O_F) \backslash (p^{-m_i+1}O_F/O_F)$ for $i = 1, 2$. Suppose $\#A = p^t$, then $m_1 + m_2 = t$. Without loss of generality we assume $v(\eta_1) \leq v(\eta_2)$. 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 $v(\eta_i) = -2m_i$ or $-2m_i + 1$. Define the following integer associated to A:

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

Proposition 2.10.1. *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 $w \equiv \pi_1^{-(n+1)}\alpha_1 e_1 + (-1)^c \pi_2^{-(n+1)} \alpha_1^{\sigma} \lambda^{2m_1 + v(\eta_1)} e_2$ mod $ord_u \geq d(p^{L(A)+1} - p^{L(A)})$, where $c = [\frac{-v(\eta_1)-n}{2}]$.

Before proving Proposition (2.10.1), we show that it implies Theorem (2.3)(1) in the case when $\mathcal{G} = \mathcal{G}_A$ such that $r(A) \leq 2$, and also implies Theorem (2.3)(2). It suffices to show the goals (2.6) (a), (b), and (c) are achieved. (2.10.1)(a) obviously implies (2.6)(a). Recall that $\pi_1 = \pi$, $\pi_2 = \lambda^{-1}\pi$, so the element w in (2.10.1)(b) can be written as $w \equiv \alpha_1 \pi^{-(n+1)} e_1 + (-1)^c \lambda^{2m_1 + v(\eta_1) + n + 1} \alpha_1^{\sigma} \pi^{-(n+1)} e_2$. Let $x_1 := \alpha_1$, $x_2 := (-1)^c \lambda^{2m_1 + v(\eta_1) + n + 1} \alpha_1^{\sigma}$. 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 (2.6) (b) is achieved. Concerning (2.6) (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 (2.10.1)(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 (2.3)(2) is proved once we prove Proposition (2.10.1).

The plan to prove Proposition 2.10.1 is as follows: we apply Lemma (2.9.1) 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) $v(p^j\eta_i) < v(p^{j'}\eta_{i'})$; or (b) $v(p^j\eta_i) = v(p^{j'}\eta_{i'})$ 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 2.9.1)

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

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 2.10.2. *Notations as above, then the $2n \times 2n$ matrices $C, C(1, r, s), C(2, r, s)$ 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 2.7.3 (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 2.8.2 and Example 2.8.4, it is straightforward to check that these blocks are all faithfully dominated by the diagonals. Therefore by Lemma 2.9.3 (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 2.7.4 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 2.10.1.

Proof of Proposition 2.10.1:

(a) In this case $m_1+m_2=2n$. Prove by induction on n. Suppose we have proved for all the subgroups $A\subset p^{-m}O_F/O_F$ 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 (2.10.2), we have shown $\det C\in W(k)((u))^\times$, so to apply Lemma (2.9.1) 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 (2.10.2) $\mathrm{ord}_u\,\det C$ 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 (2.10.2), 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 (2.7.3)(4). □

Therefore to complete the proof of Theorem 2.3(1), the remaining situation is when $r(A)=3$. In that case, we will meet difficulties if we still try to apply Lemma (2.9.1) directly, since the crucial proposition (2.10.2) may no longer hold. This phenomenon is reflected by the following example.

Example 2.10.3. 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 (2.9)

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

$$\det C\equiv -\lambda(\alpha-\alpha^\sigma)^2 y_1z_1(y_1^2z_0^2-z_1^2y_0^2)\mod \mathrm{ord}_u\ > d(2p^{4m-2}+4p^{4m-3})$$

However, $y_1^2z_0^2-z_1^2y_0^2=(b_1-c_1)^2b_0^2-(b_1+c_1)^2b_0^2=-4b_1c_1b_0^2$ has order equal to $d(3p^{4m-2}+p^{4m-4})$, hence $\mathrm{ord}_u\ (y_1z_1(y_1^2z_0^2-z_1^2y_0^2))=d(3p^{4m-2}+2p^{4m-3}+p^{4m-4})>d(2p^{4m-2}+4p^{4m-3})$. 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 [5] (3.1.3)), 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 2.10.3, 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 2.3 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 2.3 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.

2.11. **The Serre dual.** Recall from (2.6) 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 $\phi_m(e_1)=\tau_2(\overline{h_{2m}}(u))e_2,\phi_m(e_2)=\tau_1(\overline{h_{2m}}(u))e_1$, 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 $B(k)[\pi]/(\pi^2-\epsilon p)[[u]]$ (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 $h_{2m}(u)=g_1(u)+\pi_0g_2(u)$. Then in matrix form we can write

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

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 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 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 O_F-structures, i.e., $\langle x \cdot v, w\rangle = \langle v, x \cdot w\rangle$ for $x \in O_F$, $v \in \mathfrak{M}_m$, 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 (2.10.3) 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 2.11.1. *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 Dieudonne module attached to $X = (\mathcal{X}_m)_k$. The Dieudonne module attached to $\mathcal{G}_k$ is $\pi^{-l}M_m/M_m$, so the Dieudonne 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 (2.11.1) has the following immediate corollary:

Corollary 2.11.2. *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 $\eta \cdot \hat{v}$, $\eta \in p^{-m}O_F/O_F$. For any subgroup A of $p^{-m}O_F/O_F$, 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 $p^{-m}O_F/O_F$. Now supppose $n \leq m$, A is a subgroup of $p^{-n}O_F/O_F$, 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 2.11.3. 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 $n \le m$ 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 2.11.4. 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 2.11.5. *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 $0 \le n_i \le n$, 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 2.3 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 $i \ge j$. In fact, by Proposition 2.11.5 we know $A^{\perp;i} \cong \mathbb{Z}/p^i \times \mathbb{Z}/p^{i-j}$ has p-rank at most 2, hence Theorem (2.3) for $\mathcal{G}_A$ follows from Proposition (2.10.1) and Corollary (2.11.2). Explore this idea further we will be able to prove Theorem 2.3 for $\mathcal{G}_A$ in the general case when the p-rank of A is equal to 3 in the next subsection.

2.12. **The proof of Theorem (2.3) 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 $m_1 \ge m_2 \ge m_3 \ge 1$. 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 $v(\eta_i) = -2m_i$ 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 $\mathcal{X}[\pi] \not\subseteq \mathcal{G}$, 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 2.12.1. Assumptions on A are as above. Define $L(A) := 4m-2+v(\eta_1)+\lceil\frac{t+1}{2}\rceil$, and $D(A) := \begin{cases} d(p^{L(A)}-p^{L(A)-1}) & \text{if } v(\eta_1) = -2m_1+1 \text{ and } m_1 = m_2+m_3 \\ d(p^{L(A)+1}-p^{L(A)}) & \text{otherwise} \end{cases}$.

Proposition 2.12.2. *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 $ord_u\,(w_s^{(r)} - \pi_s^{-r}e_i) \ge D(A)$.

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

Before we prove Proposition 2.12.2, we first explain how to deduce Theorem 2.3(1) from it under the assumption on A as in the beginning of the subsection. It suffices to prove (2.6)(a) and (b). When $m_1 \geq m_2 + m_3$, they follow immediately from Proposition 2.12.2; see the argument after Proposition (2.10.1). 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 2.11.5. But now $m_1 - m_2 < m_3$, hence (2.6)(a) and (b) follows from induction hypothesis and Corollary (2.11.2), and Theorem 2.3 is proved.

In the rest of this subsection we prove Proposition 2.12.2. 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 2.10.1 (b) and is left as an exercise.

Now we look at Proposition 2.12.2 (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 $d(p^{4m-2+v(\eta_1)+n} + p^{4m+v(\eta_1)+n})$. Since $\mathrm{ord}_u\, v[p\eta_1, n, 2] \geq \mathrm{ord}_u\, v[\eta_1, n, 2] \geq dp^{4m-2+v(\eta_1)+n}$, and $-(d(p^{4m-2+v(\eta_1)+n} + p^{4m+v(\eta_1)+n})) + dp^{4m-2+v(\eta_1)+n} + D(A') \geq D(A)$, 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 2.12.2 (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 $v(\eta_1) = -2m_1$ and $v(\eta_1) = -2m_1 + 1$. We first assume $v(\eta_1) = -2m_1$.

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 2.11.5 (1), $A_1^{\perp;m_2} = \langle \widehat{\eta_1}\rangle \times \langle \widehat{\eta_2}\rangle$, with $\widehat{\eta_1} \in (p^{-m_2}O_F/O_F)\backslash(p^{-(m_2-1)}O_F/O_F)$ and $\widehat{\eta_2} \in (p^{-(m_2-1)}O_F/O_F)\backslash(p^{-(m_2-2)}O_F/O_F)$. Moreover, by Proposition 2.11.5 (2) we know $R_{2m_2}(A_1^{\perp;m_2}) = 2 - R_1(A_1) = 1$, so $v(\widehat{\eta_1}) = -2m_2$. 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 2.10.1, 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 $c_1 = [\frac{-v(\widehat{\eta_1})-(m_2-1)}{2}]$. By Lemma 2.11.1 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 2.10.1 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 $c_2 = [\frac{-v(\eta_1)-m_2}{2}]$. 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 that 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 $\mathfrak{R}_A$ 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 2.12.2 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 2.11.5 (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 $\widehat{\eta_i} \in (p^{-m_i'}O_F/O_F)\backslash(p^{-(m_i'-1)}O_F/O_F)$, then $m_1' = m_2 + m_3 - 2$, $m_2' = m_2 - 2$, $m_3' = m_3 - 2$. By Proposition 2.11.5 (b) we know $v(\widehat{\eta_1}) = -2(m_2+m_3-2) = -2(n-2)$. By the induction hypothesis, we know $\widehat{\mathfrak{R}_{A_1^{\perp;(m_1-2)}}}$ 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 $w_s^{(r)} \in \mathfrak{R}_{A_1}$ 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 $\widehat{w_k^{(l)}} \in \widehat{\mathfrak{R}_{A_2}}$ 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

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

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

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

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 $\begin{pmatrix} \lambda v[\widehat{\eta_1}, n-3, 1] & v[\widehat{\eta_1}, n-3, 2] \\ \lambda v[p\widehat{\eta_1}, n-3, 1] & v[p\widehat{\eta_1}, n-3, 2] \end{pmatrix}$ by T, 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 $\mathfrak{R}_{A_1}$:

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

If we follow the linear algebra approach in 2.9 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:

$$C \equiv \begin{pmatrix} v[\eta_1,n,1] & v[p\eta_1,n,1] & h_{1,n,n-1,1} & h_{1,n,n-1,2} & 0 & \cdots & 0 \\ v[\eta_1,n,2] & v[p\eta_1,n,2] & h_{2,n,n-1,1} & h_{2,n,n-1,2} & 0 & \cdots & 0 \\ v[\eta_1,n-1,1] & v[p\eta_1,n-1,1] & 1 & & & & \\ v[\eta_1,n-1,2] & v[p\eta_1,n-1,2] & & 1 & & & \\ \vdots & \vdots & & & 1 & & \\ & & & & & \ddots & \\ v[\eta_1,1,1] & v[p\eta_1,1,1] & & & & & \\ v[\eta_1,1,2] & v[p\eta_1,1,2] & & & & & 1 \end{pmatrix}$$
$$\bmod \mathrm{ord}_u \geq d(p^{4m+1-n} - p^{4m-1-n})$$

By Lemma (2.9.1), it suffices to show $\det C$ is a unit in $W(k)((u))$, and $\mathrm{ord}_u\ (\det C)^{-1}C_{k,l}v_{l,r,s} \geq D(A) = d(p^{4m-1-n} - p^{4m-2-n})$ 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:

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

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 2.7.3, 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 (2.9.1). That lower bound is exactly equal to $D(A)$, thus Proposition 2.12.2 is proved in the case when $v(\eta_1) = -2m_1$.

Finally we are left with the case when $v(\eta_1) = -2m_1 + 1$. 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 $v(\eta_i) = -2m_i$ for $i = 2, 3$. Pick $\eta_i^* \in p^{-m}O_F/O_F$ 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 2.11.5 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 $\widehat{w_s^{*(r)}} \in \mathfrak{N}_{\widehat{(A^*)^{\perp;m_1}}}$ 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 2.10.1 also implies the existence of such $\widehat{w_i^{*(r)}}$. Then by Lemma 2.11.1 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 2.12.2 is completed.

2.13. **A final remark.** Let R runs over the finite extensions of R_0, it is unexpected from Theorem (2.3) 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 (2.3)(1)(b) for all odd positive integers t, then there is in fact a simple proof to deduce Theorem (2.3)(1)(a) for all even positive integers t.

Since the reflex field of the p-adic CM type (F, Φ) is equal to $F = B(\mathbb{F}_{p^2})[\pi_0]/(\pi_0^2 - \epsilon p)$ 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 [2](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 Dieudonne 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 Dieudonne 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 Dieudonne module M' is $\mathcal{O}_F$-stable if and only if $a(M') = 2$. In fact, to make $Fx \in M'$ we must have $x \equiv \pi^{-1}(x_1 e_1 + x_2 e_2) \mod M$ 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 $\epsilon^{-1}(x_1 x_2)^\sigma(1 - \lambda^{-\sigma-1}) = 2\epsilon^{-1}(x_1 x_2)^\sigma$, 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 Dieudonne 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 $G/G_2 = (Y/G_2)[\pi]$, $G = Y[\pi^n]$.

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

3.1. **Examples of 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 $\mathcal{O}_{F'\cdot B(k)}$ with p-adic CM type Φ. In [5] 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 $1 \le a \le n-1$. In these examples, the reflex field $F' = F^{\mathrm{ur}}$. It was proved in [5] (Thm. 6.1) 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 §2 and §4 of [5]. 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 3.1.1. 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] (5.1), 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 [2] (B.4), the Dieudonne 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] (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 [2] (B.4), it is clear that the Dieudonne 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 3.1.2. Let $F = B(\mathbb{F}_{p^3})[\pi]/(\pi^e + p)$, where $e \ge 2$ 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] (5.1), 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 [2] (B.4), the Dieudonne 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] (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 $\eta \in p^{-1}O_F/O_F$.

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 $g_i(u) \in O_{F^{\mathrm{ur}}}[u]$, such that $h^{(e-1)}(u) \equiv \sum_{i=1}^{e-1} \pi^i g_i(u) \mod p$, $g_i(u) \in O_{F^{\mathrm{ur}}}((u))^{\times}$, and $\mathrm{ord}_u\, g_i(u) = p^{3e-3-3i}$. When $\eta = \pi^{-j}$ with $1 \le j \le e$, 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 Dieudonne 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 O_F-stable subgroup of $\mathcal{X}$. We denote this subgroup of order p by G_2. Because for every $\eta \in p^{-1}O_F/O_F$, there exists some $1 \le j \le e$ such that η differs from π^{-j} by a unit in 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 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 $u^{-ep^{3e-3}-p^2}(p^{-1}v) \equiv c'\pi^{-1}e_2$, where $c, c' \in W(k)^{\times}$. Thus G_2 and G_3 are both potentially liftable.

The p-adic CM type in Example (3.1.2) can be viewed as a generalization of the p-adic CM type we considered in §6 of [5]. 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 [5] (Thm. 6.1).

3.2. **Positive results on question (sCML).** Let F be a p-adic local field, π be a uniformizer in 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 3.3. *Let a be an integer such that $0 \le a \le n-1$, and t be an integer such that $0 \le t \le e_0 - 1$. 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 O_F-linear CM p-divisible group over R_0 with p-adic CM type Φ. Then for every 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 3.3.1. It suffices to prove Theorem (3.3) in the case when $t \ge 1$ and $F = F_0$. In fact, if $t = 0$ then we are reduced to [5] Thm. (6.1). We may assume $F = F_0$ because $\mathcal{X}$ is 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 (6.6) in [5].

Theorem (3.3) has the following consequences:

Corollary 3.4. *Notations as in (3.3). 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 (3.3), 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. □

Remark 3.4.1. In the context of question (LTI) for p-divisible groups (cf. [5](3.1.11)), Corollary (3.4) implies $\mathrm{LTI}(F, \Phi) = \{\text{the set of Lie types of dimension } ae + td_0\}$.

Corollary 3.5. *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 [5] (6.3(a)) by [5] (3.1.10), 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; cf. [5] (3.1.8). 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 $0 \le a \le n(K_0) - 1$ and $0 \le t \le e(K_0) - 1$. The dimension of the Serre dual $Y_2^\vee$ is also equal to $ae(K_0) + t$. Therefore by Corollary (3.4), 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). □

Now we prove Theorem (3.3) under the assumption that $t \ge 1$ 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 $\mathrm{Frac}\, R_1$. Let us recall from §5 of [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] (5.2.7) 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] (5.2.7), 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 $1 \le i \le a$, $\phi_{\mathfrak{M}}(e_{a+1}) = \overline{f(u)}e_{a+2}$, and $\phi_{\mathfrak{M}}(e_i) = E(u)e_{i+1}$ if $a+2 \le i \le n$.

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 Dieudonne module of the closed fiber of $\mathcal{G}_A$.

3.6. **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] (5.3). We take a valuation v on $B(k)[\pi_0]/(\pi_0^{e_0}+p)$ such that $v(\pi_0) = 1$. 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. We include a technical lemma from [5] as the reference of the future computations:

Lemma 3.6.1. *Let F be a p-adic local field, and π be a uniformizer in $\mathcal{O}_F$. Suppose $f(x) = x^r f_0(x)$, where r is an integer and $f_0(x)$ is a monic polynomial with nonzero constant term. Let $d = r + \deg f_0$. Suppose the slopes of Newton polygon $NP(f)$ are $\lambda_1 > \lambda_2 > \cdots > \lambda_r$, with heights $\alpha_1, \alpha_2, \cdots, \alpha_r$, respectively. Let $s = \sum_{j=1}^{r} \alpha_j$. Then there exist $g_i(u) \in \mathcal{O}_{F^{ur}}[u]$ for $i = 1, 2, \cdots, s-1$ and $g_s(u) \in \mathcal{O}_F[u]$ such that:*

(a) $f(u) = \sum_{i=0}^{s} \pi^i g_i(u)$;

(b) $g_i(u) \in \mathcal{O}_{F^{ur}}((u))^\times$ for $i = 1, 2, \cdots, s-1$, and $g_s(u) \in \mathcal{O}_F((u))^\times$;

(c) we have the following estimates on their orders:

$$ord_u\ g_i \geq d + \sum_{j=1}^{k-1} \lambda_j^{-1}\alpha_j + \lambda_k^{-1}(i - \sum_{j=1}^{k-1}\alpha_j), \quad \text{if } \sum_{j=1}^{k-1}\alpha_j < i < \sum_{j=1}^{k}\alpha_j, k = 1, 2, \cdots, r$$
$$ord_u\ g_i = d + \sum_{j=1}^{k} \lambda_j^{-1}\alpha_j, \qquad \text{if } i = \sum_{j=1}^{k}\alpha_j, k = 0, 1, 2, \cdots, r$$

See [5](5.3) for its proof. The following proposition is a straightforward application of Lemma (3.6.1).

Proposition 3.6.2. *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 height* e_0.

(b) The vertices of NP($E_0(u)$*) are* $(de_0, 0)$, $(de_0p^{-n}, e_0), \cdots, (de_0p^{-N(ne_0-1)}, e_0(Ne_0 - \frac{N}{n}))$, *and the slopes of NP(*$E_0(u)$*) are* $-\frac{1}{d(1-p^{-n})} > -\frac{1}{d(p^{-n}-p^{-2n})} > \cdots > -\frac{1}{d(p^{-N(ne_0-1)+n}-p^{-N(ne_0-1)})}$, *each with height* e_0.

(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 height* e_0.

(d) The vertices of NP($f_0(u)$*) are* $(dt, 0)$, (dtp^{-n}, t), $(dtp^{-2n}, 2t)$, $\cdots$, $(dtp^{-N(ne_0-1)}, t(Ne_0 - \frac{N}{n}))$, *and the slopes of NP(*$f_0(u)$*) are* $-\frac{1}{d(1-p^{-n})} > -\frac{1}{d(p^{-n}-p^{-2n})} > \cdots > -\frac{1}{d(p^{-N(ne_0-1)+n}-p^{-N(ne_0-1)})}$, *each with height* t.

Apply Lemma (3.6.1), 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 3.6.3. *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* $g_k(u) \in O_{F^{ur}}[u]$ *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*

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

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

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

3.7. **The proof of Theorem (3.3).** The Dieudonne 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

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

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

If G is an O_F-stable subgroup of $\mathcal{X}_k$, then the Dieudonne 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

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

Such a vector $\underline{d} = (d_i)_i \in \mathbb{N}^n$ is called $\xi(\Phi)$-*admissible* in the sense of [5] (6.5). 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 Dieudonne module $\bigoplus_{i=1}^{n} \pi_0^{-d_i} M_i/M_i$, and let $G(\underline{d})$ be the associated 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 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 O_F-linear CM p-divisible group, and we can write down its Lie type directly from $\underline{d}$; see [5] (6.5.2). We will first prove for every $\xi(\Phi)$-admissible and reduced vector $\underline{d} \in \mathbb{N}^n$, there exists a subgroup $A \subset p^{-n}O_F/O_F$ such that $\mathfrak{N}_A \mod u = N(\underline{d})$.

Define $q_i := \begin{cases} \min\{(i-1)e_0, (n-a)e_0 - t\} & \text{if } i \le a+1 \\ \min\{ae_0 + t, (n-a)e_0 - t\} & \text{if } i = a+2 \\ \min\{(n+1-i)e_0, ae_0 + t\} & \text{if } i \ge a+3 \end{cases}$ 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 $1 \le r \le q_i$.

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 $0 \le l \le n-1$, the submatrix $[\zeta_i^{\sigma^j}]_{0 \le i,j \le l}$ is non-degenerating; cf. [5] (6.6). Take $\underline{\lambda_l} = (\lambda_{l,0}, \lambda_{l,1}, \cdots, \lambda_{l,l})$ in $(W(k))^{l+1}$ such that $(\lambda_{l,0}, \lambda_{l,1}, \cdots, \lambda_{l,l}) \cdot [\zeta_i^{\sigma^j}]_{0 \le i,j \le l} = (0, 0, \cdots, 0, 1)$.

Definition 3.7.1. Suppose (s, r) is a pair of integers such that $1 \le s \le n, 1 \le r \le q_s$. Write $r = i_r e_0 - j_r$, where $0 \le j_r \le e_0 - 1$. Define $A_s^{(r)} :=$

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

as subgroups of $p^{-n}O_F/O_F$.

Define integers

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

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

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 3.7.2. *For each pair of (s,r) that satisfies the condition in (3.7.1). Write $r = i_r e_0 - j_r$, where $0 \le j_r \le e_0 - 1$. Then there exists $w_s^{(r)} \in \mathfrak{N}_{A_s^{(r)}}$ such that $w_s^{(r)} \equiv p^{-i_r}\pi_0^{j_r} e_s \mod ord_u \ge D(s,r)$.*

Proof. When $a+2 \le s \le n$ we prove by an increasing induction on r. When $1 \le s \le a+1$ 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 $a+2 \le s \le n$ and $e_0 - t \le j_r \le e_0 - 1$. 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 $a+3-i_r \le i \le s-1$. Now we examine the coefficients for e_i with $i \le a+2-i_r$ or $i \ge s$.

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

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

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 $n-s+1 \ge i_r$ because $r \le q_s$, $a+1-i \ge i_r$ because of the assumption on the range of i. Therefore apply Lemma 3.6.3, 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

$$\mathrm{ord}_u\, g_k \ge d[p^{\max\{s-1,n-a-1+i\}} - e_0(p^{\min\{s-2,n-a-2+i\}} + \cdots + p^{s-a-1}) + p^{n-a-2+i}t - p^{s-a-2}t] \ge D(s,r)$$

When $i = a+2-i_r$, the coefficient of e_i is the product of a scalar in $W(k)$ with

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

This time $n - i_r \ge s-1 > s-2$, and $i_r e_0 - j_r - 1 \le (i_r - 1)e_0 + t - 1$ (*Note that here we use the condition that $j_r \ge e_0 - t$*). Hence by Lemma 3.6.3 (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 $\mathrm{ord}_u\, g_k \ge d((t - (e_0 - j_r) + 1)p^{n-i_r} - e_0(p^{s-2} + \cdots + p^{s-a-1}) - tp^{s-a-2}) \ge d(p^{s-1} - e_0(p^{s-2} + \cdots + p^{s-a-1}) - (i_r e_0 - j_r)p^{s-a-2}) = D(s,r)$

When $i \ge s + i_r + 1$, 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 $i_r \le a$, then $\min\{i-s, a\} \ge i_r$. Hence by Lemma 3.6.3 (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 $\mathrm{ord}_u\, g_k \ge d[p^{\max\{s-1,n-a-1+i\}} - e_0(p^{\min\{s-2,n-a-2+i\}} + \cdots + p^{s-a-1}) + p^{i-a-2}t - p^{s-a-2}t] \ge D(s,r)$. If $i_r = a+1$, then $i \ge s + i_r + 1$ implies $i - a - 2 \ge s$;

at the same time, $i_re_0 - j_r - 1 \leq (i_r-1)e_0 + t - 1$ (*Note that here we use the condition that* $j_r \leq e_0 - t$). Hence by Lemma 3.6.3(b), modulo 1 we can write this coefficient as $p^{-i_r}\pi_0^{j_r}(g_1+\pi_0 g_1+\pi_0^2 g_2+\cdots+\pi_0^{i_re_0-j_r-1}g_{i_re_0-j_r-1})$, with $\mathrm{ord}_u\, g_k \geq d((t-(e_0-j_r)+1)p^{i-a-2}-e_0(p^{s-2}+\cdots+p^{s-a-1})-tp^{s-a-2}] \geq d[p^s-e_0(p^{s-2}+\cdots+p^{s-a-1})-tp^{s-a-2}) \geq D(s,r)$, too.

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 3.6.3 (a), modulo 1 we can write it as $p^{-i_r}\pi_0^{j_r}(g_1+\pi_0 g_1+\pi_0^2 g_2+\cdots+\pi_0^{i_re_0-j_r-1}g_{i_re_0-j_r-1})$ 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 $i_re_0 - j_r - 1 \leq ae+t-1$ (*Note that here we use the condition that* $j_r \leq e_0 - t$), hence apply Lemma 3.6.3 (c) we can write it as $p^{-i_r}\pi_0^{j_r}(g_1+\pi_0 g_1+\pi_0^2 g_2+\cdots+\pi_0^{i_re_0-j_r-1}g_{i_re_0-j_r-1})$ 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 3.6.2(d) and Lemma (3.6.1), we can write it as $p^{-i_r}\pi_0^{j_r}(g_0+\pi_0 g_1+\pi_0^2 g_2+\cdots+\pi_0^{i_re_0-j_r-1}g_{i_re_0-j_r-1})$ 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

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

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 $1 \leq j \leq i_re_0-j_1-1$, $\mathrm{ord}_u\, h_{i,j} \geq -jp^{s-a-2}d$.

For each j satisfying $0 \leq j \leq i_re_0-j_r$, there exists a unique pair of (i_r', j_r') with $0 \leq j_r' \leq e_0-1$ such that $i_r'e_0-j_r' = i_re_0-j_r-j = r-j$. 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 $\mathfrak{R}_{A_i^{(r-j)}}$. 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:

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

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

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

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 $1 \leq j \leq i_re_0 - j_1 - 1$, $\mathrm{ord}_u\, h_{i,j} \geq -jp^{s-a-2}d$.

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 $A(\underline{d}) \subset p^{-n}O_F/O_F$ 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 3.7.3. 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 $A(\underline{d}) := \prod_{l=0}^{e_0-1}\prod_{j=0}^{d_l'}\langle p^{-m_{j,l}}\pi_0^l\zeta_j\rangle \subset p^{-h(\underline{d})}O_F/O_F$.

Proposition 3.7.4. *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 3.7.2, 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 $A(\underline{d})$. □

By a combination of Proposition (3.7.2) and (3.7.4), we deduce that $\mathfrak{N}_{A(\underline{d})} \mod u = N(\underline{d})$. 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 (3.3).

Remark 3.7.5. 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 (3.7.3). Therefore in Theorem (3.3), for each 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 (3.4), we can also have control on the endomorphism ring of the CM lifting and the ramification of the base ring of the CM lifting.

References

[1] C. Breuil: Une application de corps des norm, Compositio Math. 117 (1999), 189-203.

[2] C. Chai, B. Conrad, F. Oort: Complex multiplication and lifting problems.

[3] J.M.Fontaine, Representations p-adiques des corps locaux. I, in The Grothendieck Festschrift, vol. 2, Progr. Math. 87, Birkhauser, Boston, 1990, pp. 24909

[4] M. Hazewinkel, Formal groups and applications, Academic Press, 1978

[5] T. Jing, Strong CM Lifting Problem I

[6] M. Kisin: Modularity of 2-adic Barsotti-Tate representations, Invent. Math. 2009

[7] M. Kisin: Moduli of finite flat group schemes, and modularity, Ann. Math. 2009

[8] T. Liu, Torsion p-adic Galois Representation and a Conjecture of Fontaine, Ann. Scient. de l'E.N.S., Vol. 40, Issue 4, July-August 2007, pp. 633-674

[9] J.P. Wintenberger, Le corps des normes de certaines extensions infinies de corps locaux; applications, Ann. Scient. de l'E.n.S. 16, 1983, 59-89.