STRONG CM LIFTING PROBLEM I

TAISONG JING
VERSION: 01/09/2014

ABSTRACT. It is known that an abelian variety over a finite field may not admit a lifting to an abelian variety with complex multiplication in characteristic 0. In this article we study the question of strong CM lifting (sCML): can we kill the obstructions to a CM lifting by requiring the whole ring of integers in the CM field act on the abelian variety? We give counterexamples to question (sCML), and prove the answer to question (sCML) is affirmative under the following assumptions on the CM field L: for every place v above p in the maximal totally real subfield L_0, either v is inert in L, or v is split in L with absolute ramification index $e(v) < p - 1$.

1. INTRODUCTION

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

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

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

History. If we drop the assumption that O_L acts on A and only require $\mathrm{End}^0(A)$ contains L, the resulted CM lifting question, denoted by (CML) in [1], was first addressed by F. Oort in [9] (Thm. B). A sharper version proved in [1] (3.5.6) said that if $g \geq 2$, in any isogeny class of abelian varieties over k with p-rank at most $g-2$, there exists an abelian variety that does not admit a CM lifting to characteristic 0. Moreover, there are effective controls on the finite fields over which such examples can be constructed. Therefore (CML) does not hold in general.

The question (sCML) can be considered as a first step in studying which abelian variety over $\mathbb{F}_q$ admits a CM lifting. For an abelian variety A in characteristic 0 with complex multiplication by L, the isomorphism class of the representation of L on $\mathrm{Lie}(A)$ is called the CM type of A. On the other hand, if A is an abelian variety in characteristic p with complex multiplication by O_L, there is the notion of Lie type to describe the representation of O_L/p on $\mathrm{Lie}(A)$; see (3.1) for its definition and basic properties. As an analogy of the CM type, the Lie type turns out to be a useful tool in characteristic p, but it is *not* invariant under L-linear isogenies. Concerning the interaction between the invariants in characteristic 0 and p, the following question (with slight variation) was asked in [1] (4.1.9):

Lie types of closed fibers of CM abelian schemes isogeneous to a CM lift (LTI)

> Consider the family $\mathcal{P}(L,\Phi)$ of abelian schemes $\mathcal{A}$ that have sufficiently many complex multiplications by L with CM type Φ over a complete discrete valuation ring of characteristic 0 with residue field $\overline{\mathbb{F}}_p$, such that the whole ring of integers O_L operates on the closed fiber $\mathcal{A}_{\overline{\mathbb{F}}_p}$ via the induced CM structure $L \hookrightarrow \mathrm{End}^0(\mathcal{A}_{\overline{\mathbb{F}}_p})$. Let $\mathrm{LTI}(L,\Phi)$ be the set of Lie types of the closed fiber of CM abelian schemes in $\mathcal{P}(L,\Phi)$. What can we say about the subset $\mathrm{LTI}(L,\Phi)$ of the set $\mathrm{LT}(O_L,p)$ of all Lie types for the CM field L?

In particular, (sCML) amounts to asking whether every Lie type of dimension g is contained in at least one of the $\mathrm{LTI}(L,\Phi)$'s when Φ runs over all CM types for L.

Main results and tools. It is known that the closed fibers of abelian schemes in the family $\mathcal{P}(L,\Phi)$ are L-linearly isogeneous to each other, due to the assumption that their generic fibers have the same CM type. In particular, they are L-linearly isogeneous to the closed fiber of an abelian scheme in characteristic 0 with complex multiplication by O_L, whose Lie type can be concretely written down from Φ; see (3.1.3) and (3.1.4). We will refer to this constraint on $\mathrm{LTI}(L,\Phi)$ as the "L-linear isogeny constraint" in the future. In this article we will first show examples of Φ such that the L-linear isogeny constraint on $\mathrm{LTI}(L,\Phi)$ is not the only constraint. For a place w of L above p, Φ induces a p-adic CM type for L_w. If the reflex field of this p-adic CM type has a "small" residue field, then there is an extra symmetry on the w-component of the Lie types in $\mathrm{LTI}(L,\Phi)$. If there exists such a common extra symmetry on all the $\mathrm{LTI}(L,\Phi)$'s when Φ runs over all CM types, then we obtain counterexamples to (sCML).

On the other hand, we will show that for a certain class of CM types Φ, the L-linear isogeny constraint on $\mathrm{LTI}(L,\Phi)$ is the only constraint; see (6.1) and (6.2). This leads to a lot of examples of abelian varieties over k with O_L-action such that they admit CM liftings over characteristic 0 with actions by orders (usually smaller than O_L) in L. As a corollary, we prove that the answer to the question (sCML) is affirmative when every place v of L_0 above p is inert in L; see (6.3).

In this article we mainly work with p-divisible groups and their finite locally free subgroup schemes, not only over a field, but also over a complete discrete valuation ring of mixed characteristic. To construct CM liftings of CM abelian varieties with O_L-action, it suffices to construct CM liftings of O_F-linear CM p-divisible groups, where F is a p-adic local field. The main tool we employ in computations is the theory of Kisin modules from p-adic Hodge theory. For each p-adic CM type Φ for F, we construct via Kisin modules a class of O_F-linear CM p-divisible groups with p-adic CM type Φ over the ring of integers in any finite extension of the reflex field; see (5.1). An important unresolved problem in integral p-adic Hodge theory is that the theory does not behave well under base change. However, this base change problem for O_F-linear CM p-divisible groups has a satisfactory solution; see (3.1.5). We would like to thank C.-L. Chai for that observation. Therefore we are able to tell whether the constructions are compatible with base change; see (5.1.7). For each positive integer m, the p^m-torsion points on the geometric generic fiber of the constructed p-divisible group become rational over a certain finite abelian extension of the base ring. In the Kisin module after such a base change, we can explicitly compute the elements corresponding to the torsion points with the help of the theory of Lubin-Tate formal group law; see (5.2.7). These constructions and computations serve as the foundation of our approach on the strong CM lifting problem, but they are interesting in their own right as well.

Let $\mathcal{X}$ be an O_F-linear CM p-divisible group constructed above with p-adic CM type Φ over a complete discrete valuation ring R_0 with residue field $\overline{\mathbb{F}}_p$. If we can lift an O_F-stable subgroup G of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ into a finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{X}_R$, where R is a finite extension of R_0, then $\mathcal{X}/\mathcal{G}$ is an F-linear CM lifting of the O_F-linear CM p-divisible group $\mathcal{X}_{\overline{\mathbb{F}}_p}/G$. Therefore to construct an F-linear CM-lifting for an O_F-linear CM p-divisible group that is F-linearly isogeneous to $\mathcal{X}_{\overline{\mathbb{F}}_p}$, we are reduced to lifting certain O_F-stable subgroups of $\mathcal{X}_{\overline{\mathbb{F}}_p}$ into finite locally free subgroup schemes of $\mathcal{X}_R$ for some finite extension R of R_0; see (6.5). One advantage of using Kisin modules is that, for a p-divisible group or its finite locally free subgroup scheme over a complete discrete valuation ring of mixed characteristic, we can write down the Dieudonne module of the closed fiber in a direct way from its Kisin module. To be more specific, a Kisin module is a $W(\kappa)[[u]]$-module satisfying certain additional conditions, where κ is a perfect field of characteristic p and $W(\kappa)$ is the ring of Witt vectors over κ. We can associate a p-divisible group or a finite locally free subgroup scheme in mixed characteristic to a Kisin module, and roughly speaking the Dieudonne module of the closed fiber is the quotient module by "modulo u"; for a precise statement, see (3.2.2) or [1] (B.4.17). The localized $W(\kappa)((u))$-module of the Kisin module carries the information on the generic fiber. For a finite locally free subgroup scheme of $\mathcal{X}$, this localized $W(\kappa)((u))$-module is generated by the elements that we have computed corresponding to the torsion points. Hence, in order to lift a certain subgroup of $\mathcal{X}_{\overline{\mathbb{F}}_p}$, it suffices to find an appropriate collection of torsion points such that the attached $W(\kappa)((u))$-module contains a lifting of the Dieudonne module of the subgroup; see (6.6.3). This computation is possible because of our knowledge on the torsion points, based on the explicit information on their coordinates provided by the Lubin-Tate theory; see (5.3.5).

What's next. In this article, we mainly study the p-adic CM type Φ that is induced from an unramified extension of $\mathbb{Q}_p$. In the future, we will consider the case when Φ is induced from a primitive p-adic CM type for a ramified p-adic local field. We will give examples to indicate why the ramification index matters in the study of this CM lifting problem, and show that the answer to the question (sCML) is affirmative under a broader condition on the CM field L. Besides that, for a special example of p-adic CM type Φ for a p-adic local field F of degree 4, we compute the closed fiber of every finite locally free subgroup scheme of the O_F-linear CM p-divisible groups with a primitive p-adic CM type in mixed characteristic. It reveals an interesting phenomenon that the finite locally free subgroup schemes seem to "try very hard" to have an O_F-stable reduction. As a corollary, we can have a complete description on the closed fiber of all the F-linear CM p-divisible groups with a primitive p-adic CM type in mixed characteristic. As a further corollary, we will obtain a counterexample to (sCML) which does *not* come from the obstruction we explain in §2 and §4 of this article. So in particular, the L-linear isogeny constraint and the symmetry caused by the residue field of the reflex field do not exhaust all the constraints on $\mathrm{LTI}(L, \Phi)$.

Acknowledgement. This work is part of the author's doctoral 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. A Counterexample

Throughout this article, let p be a prime number, q be a power of p, and $k := \overline{\mathbb{F}}_p$. For a perfect field κ of characteristic p, let $W(\kappa)$ be the ring of Witt vectors over κ, and let $B(\kappa) := W(\kappa)[\frac{1}{p}]$. Denote the Frobenius automorphism on $B(\kappa)$ by σ. For a p-adic local field F, we denote its maximal unramified subextension of

$\mathbb{Q}_p$ by F^{ur}, and its residue field by κ_F. Let L be a CM field of degree $2g$, L_0 be its maximal totally real subfield, and ι be the complex conjugation.

We first give a counterexample to (sCML). In this subsection, we consider the example where $p = 3$, $L = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$. The maximal totally real subfield $L_0 = \mathbb{Q}(\sqrt{5})$, in which p is inert. Denote the completion of L at its unique place above p by F. Pick and fix an isomorphism of F^{ur} with $B(\mathbb{F}_{p^2})$ in $B(k)$. The degree 4 extension $F \cong F^{\mathrm{ur}}[\pi]/(\pi^2 + p)$ is Galois. The involution on F induced by complex conjugation on L sends π to $-\pi$ and acts trivially on $B(\mathbb{F}_{p^2})$; we still denote this involution by ι. Define $\tau : F \to F$ such that $\tau|_{B(\mathbb{F}_{p^2})} = \sigma$, $\tau(\pi) = \pi$. The Galois group $\mathrm{Gal}(F/\mathbb{Q}_p) = \langle \tau | \tau^2 = 1\rangle \times \langle \iota | \iota^2 = 1\rangle$.

Let B be an abelian surface over k with O_L-action, such that the Dieudonne module M attached to $B[p^\infty]$ with O_F-action is as follows: $M = W(k)[\pi]/(\pi^2 + p)e_1 \oplus W(k)[\pi]/(\pi^2 + p)e_2$, where the O_F-action is $\pi \cdot e_i = \pi e_i, a \cdot e_1 = ae_1, a \cdot e_2 = a^\sigma e_2$ for $a \in W(\mathbb{F}_{p^2})$, and the O_F-linear Frobenius and Verschiebung maps are defined by $Fe_1 = Ve_1 = e_2, Fe_2 = Ve_2 = pe_1$. See (3.1.7) for the existence of such an abelian surface. We claim B does *not* have an L-linear CM lifting to characteristic 0.

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

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

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

Since F'_m is totally ramified over F', its residue field $\kappa_{F'_m} = \kappa_{F'} = \mathbb{F}_p$. Over the closed fiber, $X := \mathcal{X}_k$ is F-linearly isomorphic to $(\mathcal{Y}_1 \times_{\mathrm{Spec}\, O_{F'_m}} \mathrm{Spec}\, \kappa_{F'_m}) \times_{\mathrm{Spec}\, \kappa_{F'_m}} \mathrm{Spec}\, k$. Now suppose the closed fiber $X := \mathcal{X}_k$

has a compatible O_F-action. This implies that $\mathcal{G}_1 \times_{\operatorname{Spec} O_{F'_m}} \operatorname{Spec} k$ is invariant under the O_F-action on $(\mathcal{Y} \times_{\operatorname{Spec} O_{F'}} \operatorname{Spec} O_{F'_m}) \times_{\operatorname{Spec} O_{F'_m}} \operatorname{Spec} k$, therefore $\mathcal{G}_1 \times_{\operatorname{Spec} O_{F'_m}} \operatorname{Spec} \kappa_{F'_m}$ is invariant under the O_F-action on $(\mathcal{Y} \times_{\operatorname{Spec} O_{F'}} \operatorname{Spec} O_{F'_m}) \times_{\operatorname{Spec} O_{F'_m}} \operatorname{Spec} \kappa_{F'_m}$, too. So $\mathcal{Y}_1 \times_{\operatorname{Spec} O_{F'_m}} \operatorname{Spec} \kappa_{F'_m}$ is an O_F-linear CM p-divisible group and its base change to $\operatorname{Spec} k$ is O_F-linearly isomorphic to X. In other words, X together with its O_F-structure descents to $\mathbb{F}_p$.

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

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

3. Preliminaries

3.1. **CM p-divisible groups.** In this subsection we review some facts on CM p-divisible groups.

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

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

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

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

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

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

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

We call $\epsilon(\delta)$ the *dimension* of δ, and $\frac{\epsilon(\delta)}{[F:\mathbb{Q}_p]}$ the *slope* of δ. Two Lie types are said to be *isogeneous* if they have the same slope. These definitions naturally generalize to the situation when F is a finite product of p-adic local fields. When $\delta = [\mathrm{Lie}(X)]$, these definitions are all compatible with the corresponding definitions for the p-divisible group X; see [1] (4.2.6) (i), (ii) and (iii).

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

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

The p-adic CM type of F-linear CM p-divisible groups is invariant under isogenies. Conversely, if the residue field of R is algebraically closed and two F-linear CM p-divisible groups over R have the same p-adic CM type, then they are F-linearly isogeneous. There exists an O_F-linear CM p-divisible group $(\mathcal{X}, \alpha : O_F \to \mathrm{End}_R(\mathcal{X}))$ over R with p-adic CM type Φ if and only if $\mathrm{Frac}\, R$ contains the reflex field F'. If we assume the residue field of R is algebraically closed, then the O_F-linear CM p-divisible group with p-adic CM type Φ over R is unique up to an O_F-linear isomorphism; see [1] (3.7.3) and (3.7.4).

3.1.4. Suppose F is a p-adic local field. Define a map from the set of p-adic CM types to $R_k(O_F)$:

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

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

Proposition 3.1.5. *Let κ be a perfect field of characteristic p, and R be a complete discrete valuation ring of characteristic 0 with residue field κ. Suppose $\mathcal{X}_1$ and $\mathcal{X}_2$ are O_F-linear CM p-divisible groups over R with the same p-adic CM type Φ. Let X_1 and X_2 be their closed fibers over κ, respectively. Then for any O_F-linear isomorphism $\gamma : X_1 \to X_2$, there exists a unique O_F-linear isomorphism $\tilde{\gamma} : \mathcal{X}_1 \to \mathcal{X}_2$ such that $\tilde{\gamma}_\kappa = \gamma$.*

Proof. Let $\alpha_i : O_F \hookrightarrow \mathrm{End}(\mathcal{X}_i)$ be the O_F-structure on $\mathcal{X}_i$ for $i = 1, 2$. For every map $\operatorname{Spec} R' \to \operatorname{Spec} R$, let $(\alpha_i)_{R'} : O_F \hookrightarrow \mathrm{End}((\mathcal{X}_i)_{R'})$ be the induced O_F-structure on $(\mathcal{X}_i)_{R'}$. Let $\tilde{R}$ be the ring of integers in the compositum $\operatorname{Frac} R \cdot B(\overline{\kappa})$, then there exists an O_F-linear isomorphism $\tilde{\theta} : (\mathcal{X}_1)_{\tilde{R}} \to (\mathcal{X}_2)_{\tilde{R}}$ because they have the same p-adic CM type Φ. We first show any O_F-linear isomorphism between $(X_1)_{\overline{\kappa}}$ and $(X_2)_{\overline{\kappa}}$ over the closed fiber has a unique lifting to an O_F-linear isomorphism between $(\mathcal{X}_1)_{\tilde{R}}$ and $(\mathcal{X}_1)_{\tilde{R}}$. Let $\beta : (X_1)_{\overline{\kappa}} \to (X_2)_{\overline{\kappa}}$ be an O_F-linear isomorphism over the closed fiber. Then $\beta \circ (\theta^{-1}|_{\kappa})$ is an O_F-linear automorphism of $(X_2)_{\overline{\kappa}}$. Since $(\alpha_2)_{\overline{\kappa}}(O_F)$ is equal to its own centralizer in $\mathrm{End}((X_2)_{\overline{\kappa}})$, there exists $b \in O_F$ such that $\beta \circ \theta_{\overline{\kappa}}^{-1} = (\alpha_2)_{\overline{\kappa}}(b)$. Then $(\alpha_2)_{\tilde{R}}(b) \circ \theta$ is a lifting of β to $\tilde{R}$. By the faithfulness of the specialization functor $\mathcal{Y} \rightsquigarrow \mathcal{Y}_{\overline{\kappa}}$ for p-divisible groups over the Noetherian local ring $\tilde{R}$ (see [1] (1.4.2.3)), this lifting is unique.

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

Remark 3.1.6. The closed fibers X_1 and X_2 are indeed O_F-linearly isomorphic because they have the same Lie type. We would like to thank C.-L. Chai for his observation on (3.1.5).

3.1.7. Suppose L is a CM field of degree $2g$, and L_0 is its maximal totally real subfield, and ι is the complex conjugation. Let S_0 and S be the set of places above p in L_0 and L, respectively. Then for each place $v \in S_0$, $L_v := L \otimes_{L_0} L_{0,v}$ is a 2-dimensional commutative $L_{0,v}$-algebra, and the involution in $\mathrm{Aut}(L_v/L_{0,v})$ is induced by ι. For any field κ of characteristic p, the Grothendieck group $R_\kappa(O_L)$ is naturally isomorphic to $\prod_{v \in S_0} R_\kappa(O_{L_v})$. If A is a g-dimensional abelian variety over κ with O_L-action, then $\mathrm{Lie}(A)$ is a finitely generated module over $O_L \otimes_{\mathbb{Z}} \kappa$, and we define the class $[\mathrm{Lie}(A)]$ in $R_\kappa(O_L)$ to be the *Lie type* of A. The Lie type of the abelian variety A is equal to the Lie type of its attached p-divisible group $A[p^\infty]$ via the natural isomorphism $R_\kappa(O_L) \xrightarrow{\cong} R_\kappa(O_L \otimes_{\mathbb{Z}} \mathbb{Z}_p)$, and the latter is further naturally isomorphic to $\prod_{v \in S_0} R_\kappa(O_{L,v}) \cong \prod_{w \in S} R_\kappa(O_{L,w})$. When $\kappa = k$, we define a class in $R_k(O_L)$ to be a *Lie type*, if for each $w \in S$ its component in $R_k(O_{L,w})$ is a Lie type in the sense of (3.1.2). Denote the set of Lie types in $R_k(O_L)$ by $\mathrm{LT}(O_L, p)$.

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

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

Analogous to the question (sCML) for abelian varieties (see §1 for the statement), we can formulate the following question (sCML) for p-divisible groups:

> (sCML) *relative to (F, F_0) for p-divisible groups*: Let F, F_0, ι be as above. Let X_i be an O_{F_i}-linear CM p-divisible group over k with dimension $[F_{0,i} : \mathbb{Q}_p]$ for $i = 1, 2, \cdots, n$. Let $X := \prod_{i=1}^{n} X_i$. Does there exist an F-linear CM p-divisible group $\mathcal{X}$ over a complete discrete valuation ring of characteristic 0 with residue field k, such that the p-adic CM type of $\mathcal{X}$ is compatible with ι, and the closed fiber of $\mathcal{X}$ is F-linearly isomorphic to X?

Remark 3.1.9. If we drop the requirement that the p-adic CM type is compatible with ι, then the answer is trivially affirmative. The compatibility condition with ι on the p-adic CM type is for the purpose of algebraization; see (3.1.10) below.

Proposition 3.1.10. *The answer to question (sCML) for abelian varieties is affirmative if and only if the answer to question (sCML) relative to $(L_p, L_{0,p})$ for p-divisible groups is affirmative.*

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

Second, in the question (sCML) for abelian varieties over k, we may assume the base ring of the CM lifting is a complete discrete valuation ring of characteristic 0 with residue field k. To see this, let D be a local domain of characteristic 0 with residue field k, and $\mathcal{A}$ be a CM lifting over D of A. Since $\mathcal{A}$ is of finite type over D, we may assume D is Noetherian. By taking the completion along a minimal prime of characteristic 0, we may assume D is a complete local Noetherian domain. For such D, the residue field of every maximal ideal $\mathfrak{m}$ in $D[\frac{1}{p}]$ is a finite extension of $B(k)$ ([4] (7.1.9)), therefore by a base change to $\mathrm{Spec}\, D/(\mathfrak{m} \cap D)$ if necessary, we may assume D is a 1-dimensional complete local Noetherian domain of characteristic 0 with residue field k. Then by a base change to the normalization of $\mathrm{Spec}\, D$ and restricting to an irreducible component of characteristic 0, we may assume D is a complete discrete valuation ring R of characteristic 0 with residue field k, and we have produced a CM lifting over R of A.

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

3.1.11. Let F, F_0, ι as in (3.1.8). Consider the family of F-linear CM p-divisible groups $\mathcal{X}$ with p-adic CM type Φ over a complete discrete valuation ring of characteristic 0 with residue field k, such that O_F operates on the closed fiber $\mathcal{X}_k$ via the induced CM structure $F \hookrightarrow \mathrm{End}^0(\mathcal{X}_k)$. Let $\mathrm{LTI}(F, \Phi)$ be the set of Lie types of $\mathcal{X}_k$ when $\mathcal{X}$ runs over the family above. Analogous to the question (LTI) for abelian varieties (see §1), we can ask what we can say about $\mathrm{LTI}(F,\Phi)$. Let $\mathcal{X}_1$ and $\mathcal{X}_2$ be two F-linear CM p-divisible groups over R_1 and R_2 in the family. For a complete discrete valuation ring R of characteristic with residue field k such that R contains both R_1 and R_2, we deduce $(\mathcal{X}_1)_R$ and $(\mathcal{X}_2)_R$ are F-linear isogeneous since they have the same p-adic CM type. Because there exists O_F-linear CM p-divisible groups in the family, the Lie types in $\mathrm{LTI}(F,\Phi)$ are all isogeneous to $\xi(\Phi)$ by (3.1.4). We call this constraint on $\mathrm{LTI}(F,\Phi)$ as the "*F-linear isogeny constraint*".

If $\Phi \subset \mathrm{Hom}(L,\overline{\mathbb{Q}_p})$ is a CM type for a CM field L, $\Phi = \coprod_{v\in S_0} \Phi_v$ where each Φ_v is a p-adic CM type for L_v. Under the naturally ismorphism $R_k(O_L) \xrightarrow{\cong} \prod_{v\in S_0} R_k(O_{L_v})$, each v-component of $\mathrm{LTI}(L,\Phi)$ is isogeneous to $\xi(\Phi_v)$. We call this constraint on $\mathrm{LTI}(L,\Phi)$ as the "*L-linear isogeny constraint*"; cf. §1.

It is clear that $\prod_{v\in S_0} \mathrm{LTI}(L_v,\Phi_v)$ is contained in the $\mathrm{LTI}(L,\Phi)$. Note that Φ is a CM type if and only if for each $v \in S_0$, Φ_v is compatible with ι. For a g-dimensional abelian variety A over k with O_L-action, the answer to question (sCML) for A is affirmative if for each $v \in S_0$, the v-component $[\mathrm{Lie}(A[v^\infty])] \in R_k(O_{L_v})$ of $[\mathrm{Lie}(A)] \in R_k(O_L)$ falls into at least one of the sets $\mathrm{LTI}(L_v,\Phi_v)$'s, when Φ runs over the p-adic CM types for L_v compatible with ι.

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

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

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

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

Let p-div$/O_E$ (resp. p-Gr$/O_E$) be the category of p-divisible groups (resp. finite locally free group schemes with order equal to a power of p) over O_E, and let $(p\text{-div}/O_E)^f$ (resp. $(p\text{-Gr}/O_E)^c$) be the full subcategory of connected objects. By [7] (2.2.22), when $p > 2$ there exists equivalences of exact categories:

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

When $p = 2$, it was proved in [6] (1.2.8) that there exists an equivalence between the subcategories:

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

For a Kisin module $\mathfrak{M}$ in $\mathrm{BT}^{\phi}_{/\mathfrak{S}}$, let $\mathcal{X}$ be the associated p-divisible group over O_E under p-$\mathrm{Div}_{\mathrm{Kis}}$, then $\mathrm{rank}_{\mathfrak{S}}\mathfrak{M} = \mathrm{ht}\mathcal{X}$, where $\mathrm{ht}\mathcal{X}$ is the height of $\mathcal{X}$; it is a consequence of the isomorphism (1.2.9) in [6]. The Lie algebra $\mathrm{Lie}(\mathcal{X}) \cong \phi^*\mathfrak{M}/\psi\mathfrak{M}$, see [1] (B.4.16).

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

3.2.3. Suppose $\mathfrak{M}^{\vee}$ is the Kisin module attached to the Serre dual $\mathcal{X}^{\vee}$. The description of $\mathfrak{M}^{\vee}$ was given in §3 of [8]. Namely, $\mathfrak{M}^{\vee}$ is naturally isomorphic to $\mathrm{Hom}_{\mathfrak{S}}(\mathfrak{M}, \mathfrak{S})$, with $\phi_{\mathfrak{M}^{\vee}}(T) := \frac{1}{c}(1 \otimes T) \circ \psi_{\mathfrak{M}}$ for $T \in \mathfrak{M}^{\vee}$, and $\psi_{\mathfrak{M}^{\vee}}(T) := cT \circ (1 \otimes \phi)$. To be more explicit, let $(e_1, e_2, \cdots, e_n)$ be an $\mathfrak{S}$-basis of $\mathfrak{M}$, and suppose $\phi_{\mathfrak{M}}(e_1, e_2, \cdots, e_n) = (e_1, e_2, \cdots, e_n)A$, where A is an $n \times n$ matrix with entries in $\mathfrak{S}$. Let $(e_1^{\vee}, e_2^{\vee}, \cdots, e_n^{\vee})$ be the dual $\mathfrak{S}$-basis of $\mathfrak{M}^{\vee}$, then $\phi_{\mathfrak{M}^{\vee}}(e_1^{\vee}, e_2^{\vee}, \cdots, e_n^{\vee}) = (e_1^{\vee}, e_2^{\vee}, \cdots, e_n^{\vee}) \cdot \frac{1}{c}E(u)(A^{-1})^t$.

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

To see this, fist by a devissage argument it suffices to prove the case when $\mathfrak{M}$ is killed by p. The condition that the projective dimension of $\mathfrak{M}$ (as an $\mathfrak{S}$-module) is equal to one then implies that $\mathfrak{M}$ is a free $\kappa[[u]]$-module of finite rank. Let $\mathcal{G}$ be the associated finite locally free group scheme over O_E. It suffices to prove the order of $\mathcal{G}$ is equal to $p^{\mathrm{rank}_{kappa[[u]]}\mathfrak{M}}$. Applying (3.2.2), we are reduced to proving the order of a finite p-torsion group G over κ is equal to $p^{\mathrm{rank}_{\kappa}M}$, where M is the attached Dieudonne module. Without loss of generality, we may and do assume κ is algebraically closed. Therefore G has a filtration with each subquotient isomorphic to $\mathbb{Z}/p\mathbb{Z}$, μ_p, or α_p. Then it becomes clear since each of them has order p and the rank of the attached Dieudonne module over κ is equal to one, too.

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

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

Definition 3.2.7. Let $\mathfrak{M}$ be a finitely generated $\mathfrak{S}$-module. A submodule $\mathfrak{N} \subset \mathfrak{M}$ is said to be *saturated* (in $\mathfrak{M}$) if $\mathfrak{N} = \mathfrak{N}^0 \cap \mathfrak{M}$.

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

Corollary 3.2.8. *Let $\mathfrak{M}$ be a finite Kisin module, and $\mathcal{G}$ be the associated finite locally free group scheme over O_E. Then a finite Kisin submodule $\mathfrak{N} \subset \mathfrak{M}$ corresponds to a finite locally free subgroup scheme $\mathcal{H} \subset \mathcal{G}$ if and only if $\mathfrak{N}$ is saturated in $\mathfrak{M}$.*

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

Proposition 3.2.9. *Let $\mathfrak{M}$ be a finite Kisin module, and $\mathfrak{N} \subset \mathfrak{M}$ be a saturated submodule. Then $\mathfrak{N}$ is a finite Kisin submodule if and only if $\mathfrak{N}$ is invariant under $\phi_{\mathfrak{M}}$.*

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

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

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

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

With the notion of Lie types for O_F-linear CM p-divisible groups, it is straightforward to summarize the argument in §2 into the following proposition.

Proposition 4.1. *Let $F = \prod_{i=1}^{n} F_i$ be a finite dimensional commutative semisimple $\mathbb{Q}_p$-algebra, where each F_i is a p-adic local field. Let Φ be a p-adic CM type for F, and F' be the reflex field for (F, Φ). Let κ_{F_i} be the residue field of F_i, and $\kappa_{F'}$ be the residue field of F'. Suppose R is a complete discrete valuation ring of characteristic 0 with residue field k, and X is an F-linear CM p-divisible group over R with p-adic CM type Φ. If X_k has a compatible O_F-action, then the class of $[\mathrm{Lie}(X_k)]$ in the Grothendieck group $R_k(O_F)$ is in the image of homomorphism $R_{\kappa_{F'}}(O_F) \to R_k(O_F)$ induced by the inclusion $\kappa_{F'} \hookrightarrow k$.*

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

In other words, if Φ is a p-adic CM type such that the residue field of the reflex field is "small", then there is an extra symmetry on the Lie types when we consider the reduction of CM p-divisible groups with p-adic CM type Φ. In terms of question (LTI) for p-divisible groups (see (3.1.11)), the statement of Proposition (4.1) can be written as $\mathrm{LTI}(\Phi, F) \subset \mathrm{Im}(R_{\kappa_{F'}}(O_F) \to R_k(O_F))$.

4.2. **Counterexamples to (sCML).** Let (F, F_0) be a pair as in (3.1.8). Based on Proposition (4.1), if there exists an O_F-linear CM p-divisible group X over k such that $[\mathrm{Lie}(X)]$ is not in $\mathrm{Im}(R_{\kappa_{F'}}(O_F) \to R_k(O_F))$ for all p-adic CM types Φ for F that are compatible with ι, then X is a counterexample to question (sCML) relative to (F, F_0) for p-divisible groups. Concerning question (sCML) for abelian varieties, if $(L_p, L_{0,p})$

is equal to one of the following pairs (F, F_0), then the answer to question (sCML) for abelian varieties is negative.

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

When $p > 2$, the following proposition says that the list above gives all the "essential" counterexamples to question (sCML) caused by the extra symmetry in Proposition (4.1)*.

Proposition 4.3. *Suppose $p > 2$. Let L be a CM field, L_0 be its maximal totally real subfield. Let ι be the complex conjugation on L. Let S_0 be the set of places of L_0 above p.*

(a) *Let $v \in S_0$, and $L_v := L \otimes_{L_0} L_{0,v}$. Let κ_v be the residue field of L_v when L_v is a field, or the residue field of $L_{0,v}$ when $L_v \cong L_{0,v} \times L_{0,v}$. Suppose for all p-adic CM types for L_v that are compatible with ι, the residue field of the reflex field does not contain κ_v, then there are only two possibilities for $(L_v, L_{0,v})$:*

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

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

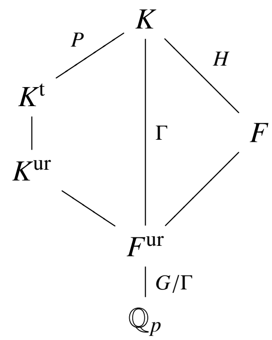
(b) *Let $X = \prod_{v \in S_0} X[v^\infty]$ be an $O_{L,p}$-linear CM p-divisible group over k, where each $X[v^\infty]$ is an $O_{L,v}$-linear CM p-divisible group. For a p-adic CM type Φ for L_p, let κ'_Φ be the residue field of the reflex field F'_Φ. If for all p-adic CM types Φ for L_p that are compatible with ι, $[Lie(X)]$ is not contained in $\mathrm{Im}(R_{\kappa'_\Phi}(O_L) \to R_k(O_L))$, then there exists a place $v \in S_0$, such that $(L_v, L_{0,v})$ and the O_{L_v}-linear CM p-divisible group $X[v^\infty]$ are in the list given in (4.2).*

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

Now we prove (a). Let $F := L_v$, and $F_0 := L_{0,v}$. Let $n := [\kappa_F : \mathbb{F}_p]$, $e := [F : F^{\mathrm{ur}}]$. Fix an embedding of F in $\overline{\mathbb{Q}_p}$. Let K be the Galois closure of F in $\overline{\mathbb{Q}_p}$, and let K^{t} be the maximal tamely ramified subextension of K, K^{ur} be the maximal unramified extension of K. Denote $d := [K^{\mathrm{ur}} : F^{\mathrm{ur}}]$. Let ζ_e be a fixed primitive e-th root of unity in $\overline{\mathbb{Q}_p}$. Let $G := \mathrm{Gal}(K/\mathbb{Q}_p)$, $\Gamma := \mathrm{Gal}(K/F^{\mathrm{ur}})$, $H := \mathrm{Gal}(K/F)$, $P := \mathrm{Gal}(K/K^{\mathrm{t}})$. The various

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

fields and Galois groups are shown in the following diagram:



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

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

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

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

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

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

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

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

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

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

5.1. **The construction of Kisin modules.** We first give a generalized definition of the reflex norm of the p-adic CM type (F, Φ) and some other related notions. Let $R = F_1 \times F_2 \times \cdots \times F_n$ be a product of fields, and V be a finitely generated R-module. Then $V = V_1 \times V_2 \times \cdots \times V_n$, where each V_i is a finite dimensional F_i-vector space.

Definition 5.1.1. For any $T \in \text{End}_R(V)$, let T_i be the induced endomorphism on V_i for $i = 1, 2, \cdots, n$, and $P_{T_i}(u)$ be the characteristic polynomial of T_i on V_i. Define the determinant of T to be $\det(T) := (\det(T_1), \det(T_2), \cdots \det(T_n))$, and the characteristic polynomial to be $P_T(u) := (P_{T_1}(u), P_{T_2}(u), \cdots, P_{T_n}(u))$.

Lemma 5.1.2. *Let K_0 be a field of characteristic 0, K be a finite dimensional commutative semisimple K_0-algebra. Let E be a finite field extension of K_0, V be a finitely generated $E \otimes_{K_0} K$-module. There exists a unique map $\Lambda_{E,V} : E[u] \to K[u]$ satisfying the following properties:*

(a) $\Lambda_{E,V}(f(u)g(u)) = \Lambda_{E,V}(f(u))\Lambda_{E,V}(g(u))$, for $f(u), g(u) \in E[u]$.

(b) For every finite field extension E'/E and $x \in (E')^\times$, if we denote the minimal polynomial of x over E by $Q_{E'/E,x}(u)$, denote the characteristic polynomial of the action of x on the finitely generated K-module $E' \otimes_E V$ by $P_{E',x}(u)$, then $\Lambda_{E,V}(Q_{E'/E,x}(u)) = P_{E',x}(u)$.

Proof. It suffices to prove in the case when K is a field. For the K-representation V of E, if we base change to $\overline{K}$, then it splits into $\prod_{\chi \in \chi(V)} (\overline{K})_\chi$, where $\chi(V)$ is a collection of embeddings of E into $\overline{K}$ (allowing repeatedness), and the index χ of $\overline{K}$ indicates the E-action. For the K-representation $E' \otimes_E V$ of E', if we define $\chi(V \otimes_E E')$ in the same way, then $\chi(V \otimes_E E')$ is the pullback of $\chi(V)$ via restriction. Define $\Lambda_{E,V}(f(u)) := \prod_{\chi \in \chi(V)} \chi_* f(u)$ for $f(u) \in E[u]$, then the property clearly follows. □

Let F be a p-adic local field, Φ be a p-adic CM type for F, F' be the reflex field, and E is an extension over F'. Let π_E be a uniformizer in $\mathcal{O}_E$. Let A be a p-adic local subfield of E with finite index. The tensor product $A \otimes_{\mathbb{Q}_p} F$ is a product of fields. We define a reflex norm $N_{\Phi,E,A\otimes_{\mathbb{Q}_p}F} : E^\times \to (A \otimes_{\mathbb{Q}_p} F)^\times$ as follows: consider the finitely generated $\overline{\mathbb{Q}_p} \otimes_{\mathbb{Q}_p} F$-module $\prod_{i\in\Phi}(\overline{\mathbb{Q}_p})_i$, where $x \in F$ acts by mutiplying $i(x)$ on the i-component. It descents to a finitely generated $E \otimes_{\mathbb{Q}_p} F$-module $V_{\Phi,E}$. When view $V_{\Phi,E}$ as an $A \otimes_{\mathbb{Q}_p} F$-module, for any $x \in E^\times$, multiplication by x induces an $A \otimes_{\mathbb{Q}_p} F$-endomorphism on $V_{\Phi,E}$.

Definition 5.1.3. For $x \in E^\times$, define its reflex norm in $(A \otimes_{\mathbb{Q}_p} F)^\times$ with respect to Φ as $N_{\Phi,E,A\otimes_{\mathbb{Q}_p}F}(x) := \det(x|_{V_{\Phi,E}})$, and denote the characteristic polynomial by $P_{\Phi,x,A\otimes_{\mathbb{Q}_p}F}(u) \in A\otimes_{\mathbb{Q}_p} F[u]$. Denote the map $E[u] \to A \otimes_{\mathbb{Q}_p} F[u]$ given in Lemma (5.1.2) by $\Lambda_{\Phi,E,A\otimes_{\mathbb{Q}_p}F}$.

Remark 5.1.4. (a) When $A = \mathbb{Q}_p$, we recover the usual definition of the reflex norm $E^\times \to F^\times$.

(b) If $\Phi_1 \coprod \Phi_2 = \Phi_3$, then $V_{\Phi_1,E} \oplus V_{\Phi_2,E} \cong V_{\Phi_3,E}$ as a direct sum in the sense of $E \otimes_{\mathbb{Q}_p} F$-modules. In particular, this implies $P_{\Phi_1,x,A\otimes_{\mathbb{Q}_p}F}(u)P_{\Phi_1,x,A\otimes_{\mathbb{Q}_p}F}(u) = P_{\Phi_3,x,A\otimes_{\mathbb{Q}_p}F}(u)$. When $\Phi = \mathrm{Hom}(F, \overline{\mathbb{Q}_p})$ is the set of all the embeddings of F into $\overline{\mathbb{Q}_p}$, the corresponding reflex norm of $x \in E^\times$ is simply $\mathrm{Nm}_{E/A}(x)$, and its characteristic polynomial is the minimal polynomial of x over A.

(c) For a finite extension E'/E, one can check $N_{\Phi,E,A\otimes_{\mathbb{Q}_p}F} \circ \mathrm{Nm}_{E'/E} = N_{\Phi,E',A\otimes_{\mathbb{Q}_p}F}$. For $x \in (E')^\times$, the property $\Lambda_{\Phi,E,A\otimes_{\mathbb{Q}_p}F}(Q_{E'/E,x}(u)) = P_{\Phi,x,A\otimes_{\mathbb{Q}_p}F}(u)$ can be viewed an analogy of this property.

Under such definitions, now we construct the Kisin module that corresponds to an O_F-linear CM p-divisible group over O_E with p-adic CM type Φ. Take $A = B(\kappa_E)$. Let $E(u)$ be the minimal Eisenstein polynomial of π_E over $B(\kappa_E)$. Define $c := \frac{\mathrm{Nm}_{E/B(\kappa_E)}(-\pi_E)}{p}$, then cp is the constant term of $E(u)$. Let Φ^c be the complement of Φ in $\mathrm{Hom}(F, \overline{\mathbb{Q}_p})$, then $E(u) = P_{\Phi,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u) \cdot P_{\Phi^c,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u)$.

Define $\mathfrak{M}$ to be the rank 1 free $W(\kappa_E)[[u]]\otimes_{\mathbb{Z}_p} O_F$-module $W(\kappa_E)\otimes_{\mathbb{Z}_p} O_F e$. There is a natural identification $\mu : \phi^*\mathfrak{M} = W(\kappa_E)[[u]] \otimes_{\phi,W(\kappa_E)[[u]]} (W(\kappa_E)[[u]] \otimes_{\mathbb{Z}_p} O_F e) \xrightarrow{\cong} W(\kappa_E)[[u]] \otimes_{\mathbb{Z}_p} O_F e$. Define the ϕ-linear endomorphism $\phi_{\mathfrak{M}} : \mathfrak{M} \to \mathfrak{M}$ by $\phi_{\mathfrak{M}}(e) := \frac{1}{c} P_{\Phi^c,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u)e$, and define the $W(\kappa_E)[[u]]$ homomorphism $\psi_{\mathfrak{M}} : \mathfrak{M} \to \phi^*\mathfrak{M}$ by $\psi_{\mathfrak{M}}(e) = \mu^{-1}(cP_{\Phi,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u))e$.

Proposition 5.1.5. *The p-divisible group associated to the Kisin module $\mathfrak{M}$ constructed above is an O_F-linear CM p-divisible group over O_E with p-adic CM type Φ.*

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

$$\phi^*\mathfrak{M}/\psi_{\mathfrak{M}}\mathfrak{M} \xrightarrow[\mu]{\cong} W(\kappa_E)[[u]] \otimes_{\mathbb{Z}_p} O_F/(P_{\Phi,\pi_E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u))$$

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

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

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

It is an immediate corollary of (3.2.2) that

Proposition 5.1.6. *The Dieudonne module of the closed fiber $\mathcal{X}_k$ of the p-divisible group constructed above is given by $M := W(\kappa_E) \otimes_{\mathbb{Z}_p} O_F e$, $Fe = \frac{p}{N_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(-\pi_E)} e$, $Ve = N_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(-\pi_E) \otimes e$.* □

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

Proposition 5.1.7. *Suppose $E' \supset E \supset F'$ are field extensions in $\overline{\mathbb{Q}_p}$. Let κ_E and $\kappa_{E'}$ be the residue field of E, E', respectively. Let $E^* := B(\kappa_{E'}) \cdot E$, and assume $[E', E^*] < \infty$. Suppose $\pi_{E'}, \pi_E$ are uniformizers in E', E such that $Nm_{E'/E^*}(-\pi_{E'}) = -\pi_E$. Let $\mathfrak{M}, \mathfrak{M}'$ be the Kisin modules constructed above with (E, π_E) and $(E', \pi_{E'})$, respectively. If we denote the p-divisible group associated to $\mathfrak{M}, \mathfrak{M}'$ by $\mathcal{X}, \mathcal{X}'$, then $\mathcal{X}'$ is O_F-linearly isomorphic to $\mathcal{X} \times_{Spec\, O_E} Spec\, O_{E'}$.*

Proof. Let X and X' be the closed fiber of $\mathcal{X}$ and $\mathcal{X}'$ over κ_E and $\kappa_{E'}$, respectively. By (3.1.5), we only need to show $X \times_{\mathrm{Spec}\,\kappa_E} \kappa_{E'}$ is O_F-linearly isomorphic to X'. It suffices to prove in the situations when E'/E is totally ramified or unramified. When E'/E is totally ramified, $E^* = E$. Proposition 5.1.6 it suffices to show $N_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(-\pi_E) = N_{\Phi,E',B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(-\pi_{E'})$, which follows from the condition $\mathrm{Nm}_{E'/E}(-\pi_{E'}) = -\pi_E$. When E'/E is unramified, $\pi_{E'} = \pi_E$ and $E' = B(\kappa'_E) \cdot E$. One can show for any $x \in O_E \subset O_{E'}$, we have $N_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(x) = N_{\Phi,B(\kappa'_E)\cdot E,B(\kappa'_E)\otimes_{\mathbb{Q}_p}F}(x)$, this finishes the proof. □

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

Lemma 5.2.1. *Let $m \geq 1$ be a positive integer. Then there is a natural one-to-one correspondence between the p^m-torsion points on $\mathcal{X}$ and the set $\{x \in p^{-m}\mathfrak{M}/\mathfrak{M} | \phi_{\mathfrak{M}}(x) = \frac{1}{c}E(u)x\}$.*

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

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

5.2.3. The theory of Lubin-Tate formal group law provides us with information on the explicit Eisenstein polynomial of a class field of E. Let us take a brief review on the set up of Lubin-Tate theory. Let E be a p-adic local field and π be a uniformizer. Let κ_E be the residue field, and $N := [\kappa_E : \mathbb{F}_p]$. Let $h(x)$ be a degree p^N

polynomial in $\mathcal{O}_E[[x]]$ such that $h(x) \equiv \pi x +$ terms of degree ≥ 2 and $h(x) \equiv x^{p^N} \mod \pi$. For any positive integer r, let $h^{(r)}(x) := h \circ h \circ \cdots \circ h$ be the r-th iteration of $h(x)$. Since $x|h(x)$, we deduce $h^{(r-1)}(x)|h^{(r)}(x)$. Define $h_r(x) := \frac{h^{(r)}(x)}{h^{(r-1)}(x)}$. It is clear that $h_r(x)$ is an Eisenstein polynomial of degree $p^{Nr} - p^{N(r-1)}$ over E. There exists a unique one dimensional formal group law $F_h(X, Y)$ over $\mathcal{O}_E$ such that $F_h \circ h = h \circ F_h$. For any $a \in \mathcal{O}_E$, there exists a unique element $[a]_h \in \mathcal{O}_E[[x]]$ such that $[a]_h(x) = ax +$ terms of degree ≥ 2 and $F_h \circ [a]_h = [a]_h \circ F_h$; in particular $h = [\pi]_h$. The p-divisible group $\mathcal{X}_h$ attached to F_h is an $\mathcal{O}_E$-linear one dimensional CM p-divisible group over $\mathcal{O}_E$, and the roots of $h^{(r)}(x)$ are the coordinates of π^r-torsion points on $\mathcal{X}_h$. The field $E(\pi, r)$ generated by these coordinates is an abelian extension of E with Galois group $\mathcal{O}_E^\times/\pi^r$, and it corresponds to $E \xrightarrow{\cong} \pi^{\mathbb{Z}} \times \mathcal{O}_E^\times \xrightarrow{\mathrm{pr}_2} \mathcal{O}_E^\times \twoheadrightarrow \mathcal{O}_E^\times/\pi^r$ via local class field theory.

Lemma 5.2.4. *Let r be a positive integer. For any $y_1, y_2 \in \mathcal{O}_E[[x]]$ such that $y_1 \equiv y_2 \mod \pi$, we have $h^{(r)}(y_1) \equiv h^{(r)}(y_2) \mod \pi^{r+1}$.*

Proof. Let $\log_F(x)$ be the logarithm of the Lubin-Tate formal group law $F_h(X, Y)$, it satisfies a functional equation $\log_F(x) = g(x) + \frac{1}{\pi}\log_F(x^{p^N})$ for some $g(x) = x +$ terms of degree ≥ 2; see [3] (I.8.3.6). For any $\alpha(x) \in \mathcal{O}_E[[x]]$ and $\beta(x) \in E[[x]]$ and any positive integer k, we have $\log_F(\alpha(x)) \equiv \log_F(\beta(x)) \mod \pi^k$ if and only if $\alpha(x) \equiv \beta(x) \mod \pi^k$ by [3] (I.2.2). Since $\log_F \circ h^{(r)} = \pi^r \circ \log_F$, it suffices to check $\log_F(y_1) \equiv \log_F(y_2) \mod \pi$. Let v be a valuation on E such that $v(\pi) = 1$. It follows from the functional equation that $\log_F(x) = \sum_{i=0}^{\infty} a_i x^i$, where $p^{Nj}|i$ if $v(a_i) = -j$. This guarantees $a_i y_1^i \equiv a_i y_2^i \mod \pi$ when $y_1 \equiv y_2 \mod \pi$, and the lemma now follows. □

Corollary 5.2.5. *For any positive integer r, $h^{(r-1)}(x^{p^N}) \equiv h^{(r-1)}(x)h_r(x) \mod \pi^r$.* □

5.2.6. Let $\mathcal{X}$ be the p-divisible group over $\mathcal{O}_E$ associated to the Kisin module $\mathfrak{M}$ constructed in (5.1). Now we are ready to compute the coordinates of the torsion points on the geometric generic fiber of $\mathcal{X}$ in the sense of Lemma 5.2.1, after a base change to an abelian extension of E. First let us make some notations:

- Let F' be the reflex field of the p-adic CM type (F, Φ), E be a finite extension of F', π_E be a uniformizer in $\mathcal{O}_E$, and κ_E be the residue field. Let $e(E)$ be the absolute ramification index of E. Define $n := [\kappa_F \cap \kappa_E : \mathbb{F}_p]$, $N := [\kappa_E : \mathbb{F}_p]$.
- Let $h(x)$ be a degree p^N polynomial in $\mathcal{O}_E[[x]]$ such that $h(x) \equiv -\pi_E x +$ terms of degree ≥ 2 and $h(x) \equiv x^{p^N} \mod \pi$. Let $h^{(r)}(x) := h \circ h \circ \cdots \circ h$, and $h_r(x) := \frac{h^{(r)}(x)}{h^{(r-1)}(x)}$ for all positive integers r.
- Let m be a positive integer, and $M := me(E)$. Let π_m be a root of the Eisenstein polynomial $h_M(x)$. Let $E_m := E(\pi_m) = E(-\pi_E, M)$ be the abelian extension of E given by Lubin-Tate theory.
- Let $E(u)$ and $E_m(u)$ be the minimal Eisenstein polynomial of π_E and π_m over $B(\kappa_E)$, and let cp and $c_m p$ be the constant terms of $E(u)$ and $E_m(u)$.
- Let $\mathfrak{M}$ and $\mathfrak{M}_m$ be the Kisin modules constructed as in (5.1) with (E, π_E) and (E_m, π_m), and let $\mathcal{X}$ and $\mathcal{X}_m$ be the associated p-divisible groups.
- Define $v := (\Lambda_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(h^{(M-1)}(u)))^{\phi^{N-1}+\phi^{N-2}+\cdots+\phi+1}e \in \mathfrak{M}_m$; see (5.1.3) for the definition of $\Lambda_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(h^{(M-1)}(u))$.
- For any subgroup A of the finite abelian group $p^{-m}\mathcal{O}_F/\mathcal{O}_F$, define $\mathfrak{N}_A^0$ to be the $\mathfrak{S}^0$-module $\mathfrak{S}^0\{\eta \cdot v | \eta \in A\}$, define $\mathfrak{N}_A$ to be the saturated finite Kisin module $\mathfrak{N}_A^0 \cap (p^{-m}\mathfrak{M}_m/\mathfrak{M}_m)$. Let $\mathcal{G}_A$ be the p^m-torsion finite locally free subgroup scheme of $\mathcal{X}_m$ attached to $\mathfrak{N}_A$.
- For each $\tau \in \mathrm{Hom}(B(\kappa_E) \cap F, \overline{\mathbb{Q}_p})$, choose an embedding $i_\tau \in \mathrm{Hom}(F, \overline{\mathbb{Q}_p})$ such that $i_\tau|_{B(\kappa_E)\cap F} = \tau$. Let $\Phi_\tau := \{i \in \Phi | i|_{B(\kappa_E)\cap F} = \tau\}$. Define $S_\tau := \{\alpha \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/B(\kappa_E))/\mathrm{Gal}(\overline{\mathbb{Q}_p}/E) | \alpha^{-1} \circ i_\tau \in \Phi_\tau\}$. Define

a homomorphism $\phi : O_{B(\kappa_E)\cdot i_\tau(F)}[[u]] \to O_{B(\kappa_E)\cdot i_{\sigma\tau}(F)}[[u]]$, such that $\phi|_{W(\kappa_E)} = \sigma$, $\phi|_{i_\tau(F)} = i_{\sigma\tau}\circ i_\tau^{-1}$, and $\phi(u) = u^p$. Define $\tilde{f}_{\tau,m}(u) := \prod_{\alpha\in S_\tau}(\alpha_* h_M)(u)$, $\tilde{g}_{\tau,m}(u) := \prod_{\alpha\in S_\tau}(\alpha_* h^{(M-1)})(u)$, and $g_{\tau,m}(u) := \tilde{g}_{\tau,m}(u)^{\phi^{N-n}+\phi^{N-2n}+\cdots+\phi^n+1}$.

Proposition 5.2.7. *Notations are as above, then:*

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

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

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

(d) Under the identification of $\mathfrak{M}_m := W(\kappa_E)\otimes_{\mathbb{Z}_p} O_F[[u]]e \xrightarrow{\cong} \bigoplus_{\tau\in Hom(B(\kappa_E)\cap F, B(\kappa_E))} O_{B(\kappa_E)\cdot i_\tau(F)}[[u]]e_\tau$, we have a concrete description of $\phi_{\mathfrak{M}_m}$ and v:

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

Proof. With the element v defined as above, we can compute

$$\begin{aligned}\phi_{\mathfrak{M}_m}v &= (\Lambda_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(h^{(M-1)}(u)))^{\phi^N-1}\cdot\tfrac{1}{c_m}\cdot P_{\Phi^c,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u)v\\ &= (\Lambda_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(h^{(M-1)}(u^{p^N}))(h^{(M-1)}(u))^{-1})\cdot\tfrac{1}{c_m}\cdot P_{\Phi^c,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u)v\\ &\equiv \Lambda_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(h_M(u))\cdot\tfrac{1}{c_m}\cdot P_{\Phi^c,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u)v \mod p^m\\ &= P_{\Phi,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u)\cdot\tfrac{1}{c_m}\cdot P_{\Phi^c,\pi_m,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(u)v\\ &= \tfrac{1}{c_m}E_m(u)v\end{aligned}$$

Since $\phi_{\mathfrak{M}_m}$ commutes with the O_F-action on $\mathfrak{M}_m$, (a) now follows. In particular, we have found $\#(O_F/p^m) = m[F:\mathbb{Q}_p]$ different p^m-torsion points in $\mathcal{X}_m$. Since $\mathrm{ht}(\mathcal{X}_m) = [F:\mathbb{Q}_p]$, all the p^m-torsion points on $(\mathcal{X}_m)_{\overline{\mathbb{Q}_p}}$ are rational over E_m. By the construction of $h_M(x)$ and π_m, we can check $\mathrm{Nm}_{E_m/E}(-\pi_m) = -\pi_E$. By Proposition 5.1.7 we know $\mathcal{X}\times_{\mathrm{Spec}\, O_E}\mathrm{Spec}\, O_{E_m}$ is O_F-linearly isomorphic to $\mathcal{X}_m$ and (b) is proved.

The correspondence in (c) is obviously bijective. To check $\#\mathcal{G}_A = \#A$, recall we have proved in Proposition 3.2.4 that $\#\mathcal{G}_A = p^{\text{length}_{\mathfrak{S}^0}\mathfrak{N}_A^0}$, and it is clear that $\#A = p^{\text{length}_{\mathbb{Z}}A}$. If we look at the natural filtration $0\subset\mathfrak{N}_A^0[p]\subset\mathfrak{N}_A^0[p^2]\subset\cdots\subset\mathfrak{N}_A^0[p^m] = \mathfrak{N}_A^0$, each subquotient $\mathfrak{N}_A^0[p^i]/\mathfrak{N}_A^0[p^{i-1}]$ is equal to $k((u))\{\overline{\eta\cdot v_m}|\eta\in A[p^i]\}$. Its dimension over $k((u))$ is equal to $\dim_{\mathbb{F}_p} A[p^i]/A[p^{i-1}]$. This implies

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

To see (d), with the definition of S_τ, one can check $\Lambda_{\Phi,E,B(\kappa_E)\otimes_{\mathbb{Q}_p}F}(f(u)) = (\prod_{\alpha\in S_\tau}\alpha_* f(u))_\tau$ from the proof of Lemma (5.1.2). Then it follows from a careful examination of the definition of v under the identification $\mathfrak{M}_m \xrightarrow{\cong} \bigoplus_{\tau\in\mathrm{Hom}(B(\kappa_E)\cap F, B(\kappa_E))} O_{B(\kappa_E)\cdot i_\tau(F)}[[u]]e_\tau$. □

Remark 5.2.8. Let d be a positive integer and $\sqrt[d]{\pi_m}$ be a d-th root of π_m. The minimal Eisenstein polynomial of $\sqrt[d]{\pi_m}$ over $B(\kappa_E)$ is $E_m(u^d)$, and its constant term is equal to pc_m. Let $\mathfrak{M}_{m,d}$ be the Kisin module constructed in (5.1) with $(E_m(\sqrt[d]{\pi_m}), \sqrt[d]{\pi_m})$. Its associated p-divisible group is naturally isomorphic to the base change of

$\mathcal{X}_m$ to $O_E[\sqrt[d]{\pi_m}]$. If we replace u with u^d in the definition of v and denote it by $v(u^d)$, then all the solutions x to $\phi_{\mathfrak{M}_{m,d}}(x) = \frac{1}{c_m}E_m(u^d)x$ in $p^{-m}\mathfrak{M}_{m,d}/\mathfrak{M}_{m,d}$ have the form $\eta \cdot v(u^d)$, where η runs over $p^{-m}O_F/O_F$.

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

Let us review the basic notions about Newton polygons: let (F, v) be a complete discrete valuation field, $f(x) = \sum_{i=0}^{d} a_i x^i \in F[x]$ be a monic polynomial of degree d and $a_0 \neq 0$. The *Newton polygon* $\mathrm{NP}(f)$ of $f(x)$ is the lower convex hull of the points $(0, v(a_0)), (1, v(a_1)), \cdots, (d, v(a_d))$. In general, if $f(x) = x^r f_0(x) \in F[u, u^{-1}]$ where r is an integer and $f_0(x)$ is a monic polynomial with nonzero constant term, then $\mathrm{NP}(f)$ is defined as $(r, 0) + \mathrm{NP}(f_0)$. We define the *slopes* of $\mathrm{NP}(f)$ as the slopes of the segments in the polygon. If λ is a slope of $\mathrm{NP}(f)$, we define the *length* (resp. *height*) of λ as the length of the projection to x-axis (resp. y-axis) of the corresponding segment.

The valuation v on F uniquely extends to the splitting field of f. The slopes of a polynomial's Newton polygon are related with the valuations of its roots in the following way.

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

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

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

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

Lemma 5.3.3. *Let F be a p-adic local field, and π be a uniformizer in 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 $g_i(u) \in O_{F^{ur}}[u]$ for $i = 1, 2, \cdots, s-1$ and $g_s(u) \in O_F[u]$ such that:*

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

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

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

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

Proof. By the assumptions on $f(u)$ we can write $f(u) = \sum_{n=r}^{d} a_n u^n$, where $a_d = 1$, $a_r \neq 0$. One can check that $\mathrm{ord}_u\,(a_r) = s$. We can combine the monomials $a_n u^n$ according to $v(a_n)$ by defining $\tilde{g}_i(u) := \pi^{-i} \sum_{v(a_n)=i} a_n u^n$ for $i = 0, 1, \cdots, s-1$, and $\tilde{g}_s(u) := \pi^{-s} \sum_{v(a_n)\geq s} a_n u^n$, then $\tilde{g}_i(u) \in O_F[u]$. For each i, there exists a positive integer $1 \le k \le r$ such that $\sum_{j=1}^{k-1}\alpha_j \le i \le \sum_{j=1}^{k}\alpha_j$. First suppose $\sum_{j=1}^{k-1}\alpha_j < i < \sum_{j=1}^{k}\alpha_j$. If $v(a_n) = i$, then because the point $P_n = (n, v(a_n))$ is inside the Newton polygon, we deduce that n is larger than or equal to the x-coordinate of the intersection of $\mathrm{NP}(f)$ with $y = v(a_n)$. The x-coordinate of the intersection is equal to $d+\sum_{j=1}^{k-1}\lambda_j^{-1}\alpha_j+\lambda_k^{-1}(i-\sum_{j=1}^{k-1}\alpha_j)$ from the information on the slopes of $NP(f)$. Therefore $\mathrm{ord}_u\,\tilde{g}_i \ge d+\sum_{j=1}^{k-1}\lambda_j^{-1}\alpha_j+\lambda_k^{-1}(i-\sum_{j=1}^{k-1}\alpha_j)$. Second, suppose $i = \sum_{j=1}^{k}\alpha_j$. Let $n_0 := d+\sum_{j=1}^{k}\lambda_j^{-1}\alpha_j$. Because $(d+\sum_{j=1}^{k}\lambda_j^{-1}\alpha_j, \sum_{j=1}^{k}\alpha_j)$ is a vertex on $\mathrm{NP}(f)$, $v(a_{n_0})$ must be equal to i, and any other n such that $v(a_n) = i$ (or $v(a_n) \ge s$ when $i = s$) must be larger than $d+\sum_{j=1}^{k}\lambda_j^{-1}\alpha_j$. This proves the estimates on the orders of $\tilde{g}_i(u)$. Finally note that any element in O_F can be written as a finite sum $c_0 + c_1\pi + c_2\pi^2 + \cdots + c_t\pi^t$ with $c_i \in O_{F^{\mathrm{ur}}}$, and the element is a unit in O_F if and only if c_0 is a unit in $O_{F^{\mathrm{ur}}}$. After such a substitution of the coefficients in $\tilde{g}_i(u)$, we may write $\sum_{i=0}^{s}\pi^i\tilde{g}_i(u) = \sum_{i=0}^{s}\pi^i g_i(u)$, with each $g_i(u) \in O_{F^{\mathrm{ur}}}[u]$ when $i < s$, and $g_s(u) \in O_F[u]$. By our knowledge on $\mathrm{ord}_u\,\tilde{g}_i(u)$, we can arrange that $g_i(u)$ is a unit in $O_F((u))$ for all i, with order equal to $\mathrm{ord}_u\,\tilde{g}_i(u)$. □

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

Proposition 5.3.4. *The following statements are true:*

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

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

(c) For any positive integer D, there exists $\widehat{h^{(M-1)}}(u) \in O_E[u, u^{-1}]$ such that $h^{(M-1)}(u)\widehat{h^{(M-1)}}(u) \equiv 1 \mod \pi_E^D$, the vertices of $NP(\widehat{h^{(M-1)}}(u))$ are $(-d, 0)$, $(-Dp^{MN} + (D-1)p^{(M-1)N}, D-1)$, and the slope of $NP(\widehat{h^{(M-1)}}(u))$ is $-\frac{1}{(p^{(M-1)N}-p^{(M-2)N})}$ with height $D-1$.

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

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

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

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

For the same reason, if $i_j > 1$ then after splitting i_j into 1 and $i_j - 1$, the order of $A_0^{-(t+1)}A_{i_1}\cdots A_{i_t}$ also decreases. Hence, among the indices $(i_1, i_2, \cdots, i_t)$ such that $i_1+i_2+\cdots+i_t = k$, the order of $A_0^{-(t+1)}A_{i_1}\cdots A_{i_t}$ is the lowest only when $t = k$ and $i_1 = i_2 = \cdots = i_k = 1$. Therefore $\mathrm{ord}_u(\sum_{\substack{i_1+i_2+\cdots+i_t=k\\ i_j>0}} A_0^{-(t+1)}A_{i_1}\cdots A_{i_t}) = \mathrm{ord}_u A_0^{-(k+1)}A_1^k = -(k+1)p^{MN} + kp^{(M-1)N}$. (c) now follows. □

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

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

$$\mathrm{ord}_u\, g_k \ge \begin{cases} dp^{(M-1)N}((1-p^{-N})(p^{k+1}+\cdots p^l) + p^{x_{l+1}} + \cdots + p^{x_r} - p^{y_1} - \cdots - p^{y_s}), & \text{if } 0 \le k \le l-1 \\ dp^{(M-1)N}(p^{x_{k+1}} + \cdots + p^{x_r} - p^{y_1} - \cdots - p^{y_s}), & \text{if } l \le k \le r-1 \\ dp^{(M-1)N}(-(k-r+1)p^{y_1} - \cdots - p^{y_s}), & \text{if } k \ge r \end{cases}$$

Proof. Replace $h^{(M-1)}(u^d)^{-1}$ by $\widehat{h^{(M-1)}}(u^d)$, and recall that $h^{(M-1)}(u^d)^{\phi^N-1} \equiv h_M(u^d) \mod p^M$, we deduce

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

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

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

are: $-\frac{1}{p^{x_1}(p^{(M-1)N}-p^{(M-2)N})d} > -\frac{1}{p^{x_2}(p^{(M-1)N}-p^{(M-2)N})d} > \cdots > -\frac{1}{p^{x_r}(p^{(M-1)N}-p^{(M-2)N})d} > -\frac{1}{p^{y_1}(p^{(M-1)N}-p^{(M-2)N})d} > \cdots$ the height of each slope $-\frac{1}{p^{x_i}(p^{(M-1)N}-p^{(M-2)N})d}$ is 1, and the height of $-\frac{1}{p^{y_1}(p^{(M-1)N}-p^{(M-2)N})d}$ is $D-1$. Then the statement follows by a direct application of Lemma 5.3.3. □

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

Let F be a p-adic local field, π be a uniformizer in $\mathcal{O}_F$, e be the absolute ramification index, κ_F be the residue field, and let $n := [\kappa_F : \mathbb{F}_p]$. In this section we prove the following theorem:

Theorem 6.1. *Let a be an integer such that $1 \le a \le n-1$. Let $i_0 \in Hom(F^{ur}, \overline{\mathbb{Q}_p})$, $\Phi' := \{i_0, i_0 \circ \sigma, \cdots, i_0 \circ \sigma^{a-1}\} \subset Hom(F^{ur}, \overline{\mathbb{Q}_p})$, and let Φ be the p-adic CM type on F induced from Φ'. Let $\mathcal{X}$ be the $\mathcal{O}_F$-linear CM p-divisible group over $W(k)$ with p-adic CM type Φ. Then for every $\mathcal{O}_F$-stable subgroup G of $\mathcal{X}_k$, there exists a finite extension R over $W(k)$, such that G lifts to a finite locally free subgroup scheme of $\mathcal{X}_R$.*

Theorem (6.1) has the following consequences:

Corollary 6.2. *Notations are as in (6.1). Then every $\mathcal{O}_F$-linear CM p-divisible group over k with dimension ae admits an F-linear CM lifting to characteristic 0 with p-adic CM type Φ.*

Proof. Every O_F-linear CM p-divisible group Y over k with dimension ae is L-linearly isogeneous to $\mathcal{X}_k$, hence there exists an O_F-stable subgroup G of $\mathcal{X}_k$ such that Y is O_F-linearly isomorphic to $\mathcal{X}_k/G$. By Theorem (6.1), there exists a finite totally ramified extension R over $W(k)$ and a finite locally free subgroup scheme $\mathcal{G}$ of $\mathcal{X}_R$, such that $\mathcal{G}_k = G$. Then $\mathcal{X}_R/\mathcal{G}$ is an F-linear CM lifting of Y with p-adic CM type Φ. □

Remark 6.2.1. In the context of question (LTI) for p-divisible groups (see (3.1.11)), Corollary (6.2) implies $\mathrm{LTI}(F,\Phi) = \{$the set of Lie types of dimension $ae\}$. So the F-linear isogeny constraint is the only constraint on $\mathrm{LTI}(F,\Phi)$; cf. (3.1.11).

Corollary 6.3. *We have the following positive results on (sCML):*

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

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

Proof. (b) follows from (a) by Proposition (3.1.10), so it suffices to prove (a). Let ι be the involution in $\mathrm{Aut}(K/K_0)$. Let e_K be the absolute ramification index of K, n_K be the inertia degree of K. The set of embeddings $\mathrm{Hom}(K^{\mathrm{ur}}, \overline{\mathbb{Q}_p})$ is isomorphic to $\{1, 2, \cdots, n_K\}$ as $\mathrm{Gal}(K^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathbb{Z}/n_K$-torsors. The involution on $\{1, 2, \cdots, n_K\}$ induced by ι sends i to $i + \frac{n_K}{2} \mod n_K$. Take a p-adic CM type for K^{ur} to be $\Phi' := \{1, 2, \cdots, \frac{n_K}{2}\}$, and let Φ be the p-adic CM type for K induced from Φ'. Then Φ is compatible with ι, i.e., $\Phi \coprod \Phi\circ\iota = \mathrm{Hom}(K, \overline{\mathbb{Q}_p})$. Now if Y is an O_K-linear CM p-divisible group with dimension $[K_0 : \mathbb{Q}_p] = \frac{n_K}{2}\cdot e_K$, then by Corollary (6.2) we deduce that Y admits a K-linear CM lifting with p-adic CM type Φ compatible with ι. This proves (a). □

Here is the plan to prove Theorem (6.1). We have constructed the Kisin module of $\mathcal{X}$ in (5.1). For each $m \geq 1$, after a base change to the totally ramified abelian extension such that the p^m-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}_p}}$ are rational, we have also computed the finite Kisin modules attached to the p^m-torsion finite locally free subgroup schemes in Proposition (5.2.7). If such a finite Kisin module reduces to an O_F-stable Dieudonne module by (3.2.2), then the associated finite locally free subgroup scheme is the lifting of an O_F-stable subgroup.

6.4. **Examples of liftable subgroups.** To illustrate the approach to prove Theorem (6.1), in this subsection we consider the example when $F = B(\mathbb{F}_{p^4})$ is unramified over $\mathbb{Q}_p$ of degree 4. Take an identification of $\mathrm{Hom}(F, B(k))$ with $\{1, 2, 3, 4\}$ as $\mathrm{Gal}(F/\mathbb{Q}_p) \cong \mathbb{Z}/4$-torsors. Take a p-adic CM type $\Phi = \{2, 3\}$. The reflex field F' is equal to F. Take $h(x) = px + x^{p^4}$, it satisfies the requirement in the theory of Lubin-Tate formal group laws as in (5.2.3). Follow the notations in (5.2.3), the Eisenstein polynomial $h_2(x) := \frac{h^{(2)}(x)}{h(x)}$ =p+$(px + x^{p^4})^{p^4-1}$ defines a totally ramified abelian extension F_2 over F with Galois group $\cong O_F/p^2$. Note that the constant term of $h_2(x)$ is equal to p. Let π_2 be a root of $h_2(x)$, and take $R = O_{F_2\cdot B(k)} = W(k)[\pi_2]$. Let $\mathcal{X}$ be the O_F-linear CM p-divisible group over R with p-adic CM type Φ, so the p^2-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}_p}}$ are already rational over Frac R. Let X be the closed fiber of $\mathcal{X}$. We will show some examples of liftable O_F-stable subgroups of X.

The Kisin module attached to $\mathcal{X}$ is isomorphic to $\mathfrak{M} \cong \bigoplus_{i=1}^{4} W(k)[[u]]e_i$, where O_F acts on the i-th component by the embedding i. For simplicity we identify O_F with its image in $W(k)$ under the first embedding.

By (5.2.7 (d)), the ϕ-linear homomorphism $\phi_{\mathfrak{M}}$ is defined as $\phi_{\mathfrak{M}} e_i = e_{i+1}$ if $i = 1, 2$, and $\phi_{\mathfrak{M}} e_i = h_2(u) e_{i+1}$ if $i = 3, 4$. Here we have identified e_{j+4} with e_j.

By Proposition (5.2.7(d)), the solutions to $\phi_{\mathfrak{M}}(x) = h_2(u)x$ in $p^{-2}\mathfrak{M}/\mathfrak{M}$ have the form $\eta \cdot v$ where $\eta \in p^{-2}O_F/O_F$, and

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

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

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

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

Example 6.4.1. Let $N := p^{-1}M_3/M_3$, it is an O_F-stable Dieudonne module. Consider

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

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

Remark 6.4.2. We have actually shown a stronger fact $u^{-(p^5+p^4)}(p^{-2}v) \equiv p^{-1}e_3 \mod u^{p^6-p^4}\mathfrak{M}$. This fact will be useful later.

Example 6.4.3. Let $N := p^{-1}M_3/M_3 \oplus p^{-1}M_4/M_4$, it is an O_F-stable Dieudonne module. For any $\eta_1 = p^{-1}\zeta_1$ with $\zeta_1 \in W(\mathbb{F}_{p^4})^\times$, we have

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

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

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

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

Example 6.4.4. Let $N := p^{-1}M_2/M_2 \oplus p^{-1}M_3/M_3$, it is an O_F-stable Dieudonne module. This time we base change to $\mathcal{X} \times_{\operatorname{Spec} W(k)[\pi_2]} \operatorname{Spec} W(k)[\sqrt[p]{\pi_2}]$ to carry out the computation†, where $\sqrt[p]{\pi_2}$ is a p-th root of π_2.

†Note that every p^2-torsion subgroup of $\mathcal{X}' := \mathcal{X} \times_{\operatorname{Spec} W(k)[\pi_2]} \operatorname{Spec} W(k)[\sqrt[p]{\pi_2}]$ is the base change of a p^2-torsion subgroup of $\mathcal{X}$, so to lift the associated subgroup of X to a finite locally free p^2-torsion subgroup scheme of $\mathcal{X} \times_{\operatorname{Spec} W(k)[\pi_2]} \operatorname{Spec} W(k)[\sqrt[p]{\pi_2}]$ is the same

Let $\mathfrak{M}'$ be the Kisin module attached to $\mathcal{X}\times_{\mathrm{Spec}\,W(k)[\pi_2]}\mathrm{Spec}\,W(k)[\sqrt[p]{\pi_2}]$. By Remark (5.2.8), if we replace u with u^p in the formula for v and denote it by $v' := v(u^p)$, then the p^2-torsion points on $\mathcal{X}'$ correspond to $\eta\cdot v'$, where $\eta\in p^{-2}O_F/O_F$. Take $A := \langle p^{-2}\rangle$. By Example (6.4.1), we already have $u^{-(p^6+p^5)}(p^{-1}v')$ in $\mathfrak{N}_A$ as a lifting of $p^{-1}e_3$, and we need to find another element in $\mathfrak{N}_A$ to lift $p^{-1}e_2$. Consider

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

By Corollary 5.2.5, $h(u)^{\phi^4-1}\equiv h_2(u) \mod p^2$, hence in $\mathfrak{N}_A^0$ we know $h(u)^{-\phi-1}(p^{-2}v')$ is equal to

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

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

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

We have seen the first term in the sum is in $p^{-2}\mathfrak{M}/\mathfrak{M}$ and it reduces to $p^{-1}e_2$ modulo u, and by Remark (6.4.2) we know the second term is divisible by $u^{p^7-p^5-p^4+p^2}$. Therefore we deduce $w\equiv p^{-1}e_2 \mod u$. This proves $\mathfrak{N}_A \mod u = p^{-1}M_2/M_2\oplus p^{-1}M_3/M_3 = N$.

6.5. **The correspondence between subgroups and Lie types.** To prove Theorem (6.1), we need a description of the Dieudonne modules attached the O_F-stable subgroups of an O_F-linear CM p-divisible group. Such a description also allows us to write down the Lie type of the quotient O_F-linear CM p-divisible group directly from the O_F-stable subgroup. We take this subsection to set up some definitions on such a description.

Let F be a p-adic local field. Let X be an O_F-linear CM p-divisible group with Lie type δ. In the natural isomorphism $R_k(O_F)\cong\prod_{\tau\in\mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}_p})}R_k(O_F\otimes_{O_{F^{\mathrm{ur}}},\tau}k)\xrightarrow{\prod\epsilon_\tau}\prod_{\tau\in\mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}_p})}\mathbb{Z}$ (see (3.1.2)), denote the image of δ by $(\delta_\tau)_{\tau\in\mathrm{Hom}(F^{\mathrm{ur}},\overline{\mathbb{Q}_p})}$. The Dieudonne module attached to X_δ is $M_\delta\cong\bigoplus_{\tau\in\mathrm{Hom}(F,\overline{\mathbb{Q}_p})}M_{\delta,\tau}$, where $M_{\delta,\tau}\cong W(k)\otimes_{\tau,O_F^{\mathrm{ur}}}O_Fe_\tau$ is a free $W(k)\otimes_{\tau,O_{F^{\mathrm{ur}}}}O_F$-module of rank 1. The Frobenius and Verschiebung maps satisfy $FM_{\delta,\tau}=\pi_F^{e-\delta_{\sigma\tau}}M_{\delta,\sigma\tau}$ and $VM_{\delta,\sigma\tau}=\pi_F^{\delta_{\sigma\tau}}M_{\delta,\tau}$.

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

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

Definition 6.5.1. Let $\delta=(\delta_\tau)_{\tau\in Hom(F^{\mathrm{ur}},\overline{\mathbb{Q}_p})}$ be a Lie type. A vector of non-negative integers

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

as to lift it to a finite locally free p^2-torsion subgroup scheme of $\mathcal{X}$. We make the base change here for the aim of convenience in computation.

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

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

Proposition 6.5.2. *The mapping $[\underline{d}] \mapsto X(\underline{d})$ is a one-to-one correspondence between the equivalent classes of δ-admissible vectors and the O_F-isomorphic classes of O_F-linear p-divisible groups isogeneous to X_δ. Moreover, the Lie type $[Lie(X(\underline{d}))] = (\delta_\tau - d_\tau + d_{\sigma^{-1}\tau})_{\tau\in Hom(F^{ur},\overline{\mathbb{Q}_p})} \in R_k(O_F)$.*

6.6. **The proof of Theorem (6.1).** In this subsection we prove Theorem (6.1). Notations are as in the beginning of the section. We first claim it suffices to prove in the case when F is unramified over $\mathbb{Q}_p$. To see this, recall that Φ is induced from the p-adic CM type Φ' for F^{ur}. Let $\mathcal{Y}$ be the $O_{F^{ur}}$-linear p-divisible group over $W(k)$ with p-adic CM type Φ', then $\mathcal{X}$ is O_F-linearly isomorphic to the Serre tensor construction $\mathcal{Y} \otimes_{O_{F^{ur}}} O_F$. Now suppose G is an O_F-stable finite subgroup of $\mathcal{X}_k$. The following lemma (6.6.1) reduces the potential liftablity of G to an $O_{F^{\mathrm{ur}}}$-stable finite subgroup of $\mathcal{Y}_k$.

Lemma 6.6.1. *Let F/F_0 be a totally ramified finite extension of degree d between p-adic local fields, and π be a uniformizer of F. Let Y be an O_{F_0}-linear CM p-divisible group over k, and $X := Y \otimes_{O_{F_0}} O_F$ be the Serre tensor construction. Let $Y \hookrightarrow X$ be the canonical embedding, and Y_i be the image of Y under the endomorphism $\pi^i \in End(X)$ for $i = 0, 1, \cdots, d-1$. Then for every O_F-stable finite subgroup $G \subset X$, there exists an O_{F_0}-stable finite subgroup $G_i \subset X_i$ for $i = 0, 1, \cdots, d-1$, such that $G = \prod_{i=0}^{d-1} G_i$.*

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

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

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

From now on we may and do assume that F is unramified over $\mathbb{Q}_p$. Take an identification between the $\mathrm{Gal}(F/\mathbb{Q}_p) \cong \mathbb{Z}/n$-torsors $\mathrm{Hom}(F, B(k))$ and $\{1, 2, \cdots, n\}$, such that $\Phi = \{2, 3, \cdots, a+1\}$. The reflex field F' of (F, Φ) is equal to F. Take $h(x) = px + x^{p^n}$, and construct $h^{(r)}(x), h_r(x)$ for all positive integers r as in (5.2.3). Let π_n be a root of $h_n(x)$, and $\sqrt[p^n]{\pi_n}$ be a p^n-th root of π_n. Define $R := W(k)[\sqrt[p^n]{\pi_n}]$. Let $\mathfrak{M}$ be the Kisin module constructed in §5 over R using the uniformizer $\sqrt[p^n]{\pi_n}$, and let $\mathcal{X}$ be the associated p-divisible group. By (5.2.7) all p^n-torsion points on $\mathcal{X}_{\overline{\mathbb{Q}_p}}$ are already rational over Frac R. By Proposition (5.2.7) and

Remark (5.2.7(d)), the p^n-torsion points on $\mathcal{X}$ are in one-to-one correspondence with $\{\eta \cdot v | \eta \in p^{-n}O_F/O_F\}$, where $v = \sum_{i=1}^{a} h^{(n-1)}(u^{p^n})^{\phi^{n-1}+\phi^{n-2}+\cdots+\phi^{n-a-1+i}+\phi^{i-2}+\phi^{i-3}+\cdots+1} e_i + \sum_{i=a+1}^{n} h^{(n-1)}(u^{p^n})^{\phi^{i-2}+\phi^{i-3}+\cdots+\phi^{i-a-1}} e_i$.

Let $X := \mathcal{X}_k$ be the closed fiber, it is the O_F-linear CM p-divisible group over k with Lie type $\xi(\Phi)$. From the definition of Φ, if a vector of integers $\underline{d} = (d_i)_{i=1,2,\cdots,n}$ is $\xi(\Phi)$-admissible, then $0 \le d_{i+1} - d_i \le 1$ when $1 \le i \le a$, and $-1 \le d_{i+1} - d_i \le 0$ when $a+1 \le i \le n$. Define $q_i := \min\{i-1, n+1-i, a, n-a\}$ for each $i = 1, 2, \cdots, n$. One can easily check that for a positive integer r, there exists a reduced $\xi(\Phi)$-admissible $\underline{d} \in \mathbb{N}^n$ such that the i-th component d_i is equal to r if and only if $1 \le r \le q_i$.

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

Definition 6.6.2. Suppose (s, r) is a pair of integers such that $1 \le s \le n, 1 \le r \le q_s$. Define

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

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

Define integers

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

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

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

Proposition 6.6.3. *For each pair of (s, r) that satisfies the condition in (6.6.2), there exists $w_s^{(r)} \in \mathfrak{N}_{A_s^{(r)}}$ such that $w_s^{(r)} \equiv p^{-r}e_s \mod \mathrm{ord}_u \ge D(s, r)$.*

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

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

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

Then by the choice of $\underline{\lambda_{s+r-a-2}}$ one can easily check that the coefficient of e_i in $v^* - p^{-r}e_s$ vanishes for $a+2-r \le i \le s$. Now we examine the coefficients for e_i with $i \le a+1-r$ or $i \ge s+1$.

When $1 \le i \le a+1-r$, the coefficient of e_i is equal to

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

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

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

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

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

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

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

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

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

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

So far we have been able to write v^* as $p^{-r} e_s + \sum_{\substack{i \le a+1-r \\ \text{or} \\ i \ge s+r+1}} v_i^* e_i + \sum_{s+1 \le i \le s+r} \sum_{j=0}^{r-1} h_{i,j} p^{-r+j} e_i$, knowing:

(a) when $i \le a + 1 - r$ or $i \ge s + r + 1$, $\operatorname{ord}_u v_i^* \ge D(s,r)$.

(b1) when $s + 1 \le i \le s + r$ and $j \le i - s - 1$, $\operatorname{ord}_u h_{i,j} \ge D(s,r)$.

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

Now we define

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

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

$$w_s^{(r)} - p^{-r} e_s \quad = \quad \sum_{\substack{i \le a+1-r \\ \text{or} \\ i \ge s+r+1}} v_i^* e_i + \sum_{\substack{s+1 \le i \le s+r \\ j \le i-s-1}} h_{i,j} p^{-r+j} e_i - \sum_{\substack{s+1 \le i \le s+r \\ j \ge i-s}} h_{i,j}(w_i^{(r-j)} - p^{-r+j} e_i)$$

We have shown the first two terms in the above formula have orders higher than or equal to $D(s,r)$. For the last term, by induction hypothesis $\operatorname{ord}_u (w_i^{(r-j)} - p^{-r+j} e_i) \ge D(i, r-j)$, and we have shown $\operatorname{ord}_u h_{i,j} \ge d(-(j-(i-s)+1)p^{i-a-2} - p^{i-a-3} - \cdots - p^{s-a-1})$, therefore we are reduced to the inequality which is an easy exercise:

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

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

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

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

The coefficient of e_s is equal to $p^{-(a+1-s+r)}h_n(u^{p^n})^{\phi^{-1}+\cdots+\phi^{-a-1+s}}$. Since $h_n(u)$ is an Eisenstein polynomial of degree $p^{n^2}-p^{n(n-1)}$, we can write $p^{-(a+1-s+r)}h_n(u^{p^n})^{\phi^{-1}+\cdots+\phi^{-a-1+s}} = p^{-r}e_s + \sum_{j=0}^{a-s+r} p^{-(a+1-s+r)+j}h_{s,j}$, where $\mathrm{ord}_u\, h_{s,j} \ge (p^{n^2+n}-p^{n^2})p^{-a-1+s}$ if $j \le a+1-s$, and $\mathrm{ord}_u\, h_{s,j} > 0$ if $a+2-s \le j \le a-s+r$. Note that $(p^{n^2+n}-p^{n^2})p^{-a-1+s} \ge D(s,r)$. Apply Lemma 5.3.5 to study the coefficients of other e_i's, we can write v^* as:

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

knowing:

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

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

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

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

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

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

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

Define

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

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

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

- Define a set $H(\underline{d}) := \{(s,r)|1 \le s \le n, 1 \le r \le d_s\} \subset \{1,2,\cdots,n\}\times\mathbb{N}^*$.
- For $k = 1,2,\cdots,a$, define $\Gamma_k := \{(n,k),(n-1,k),\cdots,(a+1,k),(a,k-1),(a-1,k-2),\cdots\}$.
- Define $h_k := \#(H(\underline{d})\cap\Gamma_k)$, $L := \sum_{j=1}^a h_j - 1$, and $m_i := k$ if $\sum_{j=k+1}^a h_j \le i \le \sum_{j=k}^a h_j - 1$.

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

Definition 6.6.4. With the above notations, define $h(\underline{d})$:= the largest integer k such that $H(\underline{d}) \cap \Gamma_k \neq \emptyset$, and $A(\underline{d}) := \prod_{t=0}^{e-1} \prod_{l=0}^{L} \langle p^{-m_l}\zeta_l \rangle \subset p^{-h(\underline{d})}O_F/O_F$.

Proposition 6.6.5. *We have* $\#A(\underline{d}) = p^{\sum_{s=1}^{n} d_s}$*, and* $A_s^{(r)} \subset A(\underline{d})$ *for all* $s = 1, 2, \cdots, n$ *and* $r = 1, 2, \cdots, d_s$.

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

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

By a combination of Proposition (6.6.3) and (6.6.5), we deduce that $\mathfrak{N}_{A(\underline{d})} \mod u = N(\underline{d})$, where $\mathfrak{N}_{A(\underline{d})} \mod u$ is short for $\mathfrak{N}_{A(\underline{d})}/(\mathfrak{N}_{A(\underline{d})} \cap u \cdot p^{-n}\mathfrak{M}/\mathfrak{M})$. This proves for every reduced $\xi(\Phi)$-admissible vector $\underline{d} \in \mathbb{N}^n$, $G(\underline{d})$ lifts to a finite locally free subgroup scheme $\mathcal{G}_{A(\underline{d})}$ of $\mathcal{X}$. For a general $\xi(\Phi)$-admissible vector $\underline{d}' \in \mathbb{N}^n$, there exists a reduced $\xi(\Phi)$-admissible vector $\underline{d}$ and a non-negative integer i, such that $\underline{d}' = \underline{d} + (i, i, \cdots, i)$. If we compose the isogenies $\mathcal{X} \xrightarrow{i} \mathcal{X} \xrightarrow{\pi} \mathcal{X}/\mathcal{G}_{A(\underline{d})}$, the reduction of $\mathrm{Ker}(\pi \circ p^i)$ is equal to $G(\underline{d}')$. This finishes the proof of Theorem (6.1).

Remark 6.6.6. From the definition we can see $A(\underline{d})$ is in fact $p^{h(\underline{d})}$-torsion, where the integer $h(\underline{d})$ is defined in (6.6.4). Therefore in Theorem (6.1), 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 (6.2), 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-L. Chai, B. Conrad & F. Oort, *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs, volume 195, American Mathematical Society, 2013.
[2] G. Faltings & C-L. Chai, *Degeneration of abelian varieties*. Ergebnisse der Mathematik 22, Springer-Verlag, New York, 1990.
[3] M. Hazewinkel, *Formal groups and applications*, Academic Press, 1978
[4] A. J. de Jong, *Crystalline Dieudonne module theory via formal and rigid geometry*. Publ. Math. IHES 82 (1995), 5-96
[5] N. Katz, *Serre-Tate local moduli*, Lect. Notes Math. 868, Springer-Verlag (1981), 138-202.
[6] M. Kisin, *Modularity of 2-adic Barsotti-Tate representations*, Invent. Math. (2009), 587-634
[7] M. Kisin, Moduli of finite flat group schemes, and modularity, Ann. of Math.(2) 170, no. 3 (2009), 1085-1180.
[8] T. Liu, *Torsion p-adic Galois Representation and a Conjecture of Fontaine*, Ann. Scient. de l'E.N.S., vol. 40, no. 4 (2007), 633-674
[9] F. Oort, *CM-liftings of abelian varieties*, Journ. Alg. Geom. 1 (1992), 131-146
[10] J. P. Serre & J. Tate, *Good reduction of abelian varieties*, Ann. Math. 88(1965), 492-517.
[11] S. Shatz, *Group schemes, formal groups, and p-divisible groups*. In Arithmetic geometry(G. Cornell & J. Silverman, ed.), Springer-Verlag, New York, 1986.
[12] G. Shimura & Y. Taniyama, *Complex Multiplication of Abelian Varieties and Its Application to Number Theory*, Math. Soc. Japan, 1961

[13] J. Tate, *p-divisible groups*. In Proc. conference on local fields (T.Springer ed.), Springer-Verlag, 1967, 158-183.