

CM p -divisible Groups over Finite Fields

by
Xinyun Sun

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2011

Doctoral Committee:

Associate Professor Kartik Prasanna, Co-Chair
Professor Brian D. Conrad, Co-Chair, Stanford University
Professor Jeffrey C. Lagarias
Associate Professor James P. Tappenden
Assistant Professor Wenliang Zhang

TABLE OF CONTENTS

CHAPTER

I. Abelian Varieties and CM Lifting Problems	1
1.1 Basics of Abelian Varieties	1
1.2 Abelian Varieties Over Finite Fields	4
1.3 CM Lifting Questions	6
II. p-divisible Groups and Dieudonné Modules	13
2.1 p -divisible Groups	13
2.2 p -divisible Groups of CM Type	14
2.3 Dieudonné Modules	15
2.4 Dieudonné modules and CM lifting	18
2.5 Questions of Importance to This Dissertation	20
III. Classification of Dieudonné Modules	22
3.1 Classification up to Isomorphism	22
3.2 Classification up to Isogeny	33
BIBLIOGRAPHY	36

CHAPTER I

Abelian Varieties and CM Lifting Problems

1.1 Basics of Abelian Varieties

We begin with a brief treatment of the topic of abelian varieties. A more detailed introduction to this subject may be found in Mumford [14].

Definition I.1. A complete algebraic variety A over a field K is an *abelian variety* if there exist morphisms of varieties $m : A \times A \rightarrow A$ and $i : A \rightarrow A$ such that m and i give A the structure of an abelian group (i.e., m is the group operation, and i the inverse map). An abelian variety A over a field K is *simple* (over K) if the abelian subvarieties of A are exactly A and 0 .

Let A and B be abelian varieties over K . A homomorphism $f : A \rightarrow B$ is called an *isogeny* if it is surjective with finite kernel. If an isogeny from A to B exists, we also say that A is *isogenous* to B . In most cases related to this dissertation, it will be useful to consider abelian varieties up to isogeny (as opposed to considering them up to isomorphism). As a beginning example, we may, up to isogeny, decompose any abelian variety into the product of simple abelian varieties:

Theorem I.2. (*Poincaré complete reducibility theorem*) *If A is an abelian variety, and B an abelian subvariety of A , then there exists an abelian subvariety C of A such that A is isogenous to $B \times C$.*

Remark I.3. For a statement and proof of this theorem, see Chapter 4, Section 19 of [14].

Corollary I.4. *For any non-zero abelian variety A , there exist simple abelian varieties A_i not isogenous to each other and positive integers n_i such that A is isogenous to the product $\prod_i A_i^{n_i}$. Furthermore, except for reordering the indices, the A_i and n_i are uniquely determined (the former up to isogeny).*

From a slightly different perspective we may view the above theorem as giving a decomposition of A into powers of simple abelian varieties (in place of a decomposition of A into simple abelian varieties).

Definition I.5. An abelian variety A is *isotypic* if there exists a simple abelian variety B such that A is isogenous to B^e for some $e \geq 1$.

Remark I.6. Corollary I.4 decomposes A into isotypic parts.

Let A be an abelian variety over a field K . We call $\text{End}^0(A) := \mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(A)$ the *endomorphism algebra of A (over K)*. The (up to isogeny) decomposition of A into simple abelian varieties imparts a decomposition of $\text{End}^0(A)$:

Corollary I.7. *(to Theorem I.2) If A is simple, then $\text{End}^0(A)$ is a division ring. For any non-zero abelian variety A , if $A = \prod_i B_i^{n_i}$ where the B_i are simple and not isogenous to each other, let $D_i = \text{End}^0(B_i)$. Then*

$$\text{End}^0(A) = M_{n_1}(D_1) \times M_{n_2}(D_2) \times \cdots \times M_{n_k}(D_k),$$

where $M_{n_i}(D_i)$ is the ring of $n_i \times n_i$ matrices over D_i .

As a consequence, $\text{End}^0(A)$ is a semisimple \mathbb{Q} -algebra for any abelian variety A . Further, it is simple if and only if A is isotypic, and a division algebra if and only if A is simple.

Theorem I.8. *Let A be an abelian variety of dimension $g > 0$. For any commutative semisimple \mathbb{Q} -subalgebra $L \subseteq \text{End}^0(A)$, $[L : \mathbb{Q}] \leq 2g$. Furthermore,*

- *if $[L : \mathbb{Q}] = 2g$, then L is its own centralizer in $\text{End}^0(A)$;*
- *if $[L : \mathbb{Q}] = 2g$ and L is a field, then A is isotypic and L is a maximal commutative subfield of $\text{End}^0(A)$.*

Remark I.9. For a proof, see Section 3 of [5] and Section 3 of [13].

The latter cases (i.e., there exists $L \subseteq \text{End}^0(A)$ such that $[L : \mathbb{Q}] = 2g$) are important enough to warrant a separate definition.

Definition I.10. Let A be an abelian variety of dimension $g > 0$ over a field K . We say that A *admits sufficiently many complex multiplications (over K)* if there exists a commutative semisimple \mathbb{Q} -subalgebra $L \subseteq \text{End}^0(A)$ such that $[L : \mathbb{Q}]$ attains the maximum value $2g$.

Remark I.11. One can prove that A admits sufficiently many complex multiplications if and only if each simple factor of A does ([13], Remark 3.5).

Usage of the term “admits sufficiently many complex multiplications” comes from the specific case where A is an elliptic curve over \mathbb{C} . In this case, the ring of endomorphisms of A can be identified with a subring of \mathbb{C} . Then A admits sufficiently many complex multiplications if this subring contains an element not in \mathbb{Z} . In the general case, admitting sufficiently many complex multiplications also implies some “ \mathbb{C} -like” structure within $\text{End}^0(A)$.

Definition I.12. A *CM field* is a totally imaginary quadratic extension of a totally real field. A *CM algebra* is a finite product of CM fields.

Theorem I.13. *Let A be an abelian variety of nonzero dimension which admits sufficiently many complex multiplications. Then the algebra L of Definition I.10*

may be taken to be a CM algebra. If A is isotypic, then L can be taken to be a CM field.

Remark I.14. For a proof of this theorem, see Section 4 of [5].

Definition I.15. Let A be an abelian variety over K which admits sufficiently many complex multiplications and L a CM algebra such that $[L : \mathbb{Q}] = 2 \cdot \dim A$. If i is an embedding $L \hookrightarrow \text{End}^0(A)$, then we call the pair (A, i) a *CM abelian variety with complex multiplication by L* and i a *CM-structure on A over K* .

Remark I.16. As a partial converse to Theorem I.13, if A is a CM abelian variety of dimension $g > 0$ with complex multiplication by a CM field of degree $2g$, then A is necessarily isotypic. This follows from Corollary I.7 (due to the structure of maximal commutative subalgebras).

1.2 Abelian Varieties Over Finite Fields

In this section, we assume k is a finite field, and let $p = \text{char}(k)$ and $q = |k|$. Let A be an abelian variety over k , and π_A the q -Frobenius endomorphism of A . Observe that π_A commutes with all endomorphisms of A . If A is simple, as mentioned in Corollary I.7, then $D := \text{End}^0(A)$ is a division algebra of finite dimension over \mathbb{Q} .

Definition I.17. A *Weil q -number* (in a field of characteristic 0) is an algebraic integer π such that for every embedding $\psi : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$ we have $|\psi(\pi)| = \sqrt{q}$. Let $W(q)$ denote the set of Weil q -numbers in \mathbb{C} .

Definition I.18. ([13], pg. 79) Two Weil q -numbers π and π' are conjugate if one of the following (equivalent) conditions holds:

1. $f_\pi = f_{\pi'}$ (where for $\tau \in \overline{\mathbb{Q}}$, f_τ denotes the minimal polynomial of τ over \mathbb{Q}).
2. There exists a field isomorphism $\psi : \mathbb{Q}[\pi] \rightarrow \mathbb{Q}[\pi']$ such that $\psi(\pi) = \pi'$.

3. Under the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $W(q)$, π and π' lie in the same orbit.

The concept of Weil q -numbers is a useful tool in the study of q -Frobenius endomorphisms of simple abelian varieties. We observe that for any simple abelian variety A over k and any homomorphism $\psi : \mathbb{Q}[\pi_A] \rightarrow \overline{\mathbb{Q}}$, $\psi(\pi_A)$ is a Weil q -number, well-defined up to conjugacy. Further, an isogeny $A \rightarrow B$ of simple abelian varieties over k defines an isomorphism $\text{End}^0(A) \rightarrow \text{End}^0(B)$ carrying π_A to π_B , hence mapping $\mathbb{Q}[\pi_A]$ isomorphically to $\mathbb{Q}[\pi_B]$. Therefore the conjugacy class of π_A depends only on the isogeny class of A . Put formally:

Theorem I.19. *(Honda-Tate)[19] Let k be a finite field of size q . For A a simple abelian variety over k and $\pi \in W(q)$, let \bar{A} and $\bar{\pi}$ denote, respectively, the isogeny class of A and the conjugacy class of π . The mapping $\bar{A} \mapsto \bar{\pi}_A$ is well-defined and is a bijection between the set of isogeny classes of simple abelian varieties over k and the set of conjugacy classes of $W(q)$.*

Remark I.20. The injectivity of this map was proven by Tate, and the surjectivity was proven by Honda and Tate.

Since π_A commutes with every endomorphism of A , $\mathbb{Q}(\pi_A)$ is a field which is contained in the center of $D := \text{End}^0(A)$. Tate proved a stronger statement which makes abelian varieties over finite fields an ideal setting in which to study questions involving CM-structure:

Theorem I.21. *(Tate)[19, 20] Let A be a simple abelian variety over k . Let D denote $\text{End}^0(A)$ and L denote $\mathbb{Q}(\pi_A)$. Then;*

1. L is the center of D ;
2. $[L : \mathbb{Q}] \cdot \sqrt{[D : L]} = 2 \cdot \dim A$ – hence A admits sufficiently many complex multiplications;

3. if $f_A, Irr_A \in \mathbb{Z}[T]$ are, respectively, the characteristic polynomial and the minimal polynomial of π_A , then

$$f_A = (Irr_A)\sqrt{[D:L]};$$

4. the central simple algebra D over L

- does not split at any real place of L ;
- does split at every finite place not above $p := \text{char}(k)$;
- for a discrete valuation w of L with $w|p$, letting L_w denote the local field obtained from L by completing at w , the quantity

$$\text{inv}_w(D) = \frac{w(\pi_A)}{w(q)} \cdot [L_w : \mathbb{Q}_p] \pmod{\mathbb{Z}}$$

is an invariant of D ;

- if \bar{w} is the conjugate of w and $\text{inv}_{\bar{w}}$ is the similarly defined invariant for \bar{w} , then $\text{inv}_w(D) \equiv -\text{inv}_{\bar{w}}(D) \pmod{\mathbb{Z}}$.

Corollary I.22. *Let A be an abelian variety over a finite field. Then A admits sufficiently many complex multiplications, and if A is isotypic then it admits a structure of CM abelian variety with complex multiplication by a CM field.*

Proof. The first statement follows from Theorem I.21 by passing to products. The second statement follows from the first and Theorem I.13. \square

1.3 CM Lifting Questions

We now make precise the most basic version of the CM lifting question and introduce some variations. This material is indebted to the work of Conrad, Chai, and Oort, and a more detailed treatment of the subject may be found in their paper [2]. First, we need some additional terminology.

Definition I.23. Let S be a scheme. A *group scheme over S* is a scheme G such that $\text{Mor}_S(-, G)$ represents a group functor on the category of schemes over S . A group scheme A over S is an *abelian scheme* if A is smooth and proper with geometrically irreducible fibers.

Remark I.24. In the case where $S = \text{Spec}(K)$ for some field K , A/S is an abelian scheme if and only if A is an abelian variety over K .

We first give the definition of a lifting:

Definition I.25. Let A_0 be an abelian variety over a field K of nonzero characteristic. We say A/R is a *lifting* of A_0 to characteristic zero if R is an integral domain of characteristic zero with a ring homomorphism $R \rightarrow K$, and $A \rightarrow \text{Spec}(R)$ is an abelian scheme such that $A \otimes_R K = A_0$.

Now, the above definition can be modified to include the preservation of CM-structure.

Definition I.26. Let A_0 be an abelian variety over a field K of nonzero characteristic such that A_0 admits sufficiently many complex multiplications, and let A/R be a lifting of A to characteristic zero. We say A/R is a *CM lifting* of A_0 to characteristic zero if A/R admits sufficiently many complex multiplications on its generic fiber.

The most basic question to ask at this point is, does every abelian variety admitting sufficiently many complex multiplications have a CM lifting? A partial answer was given by Honda:

Theorem I.27. (*Honda*)[9] *Let A_0 be an abelian variety over a finite field $k = \mathbb{F}_q$. Then there exist a finite extension $k' \supseteq k$ and an abelian variety B_0 over k' such that B_0 is isogenous to $A_0 \otimes_k k'$ and has a CM lifting (i.e., there exists B/R which is a CM lifting of B_0).*

In other words, we know that for an abelian variety over a finite field, CM lifting exists up to isogeny and up to a finite extension of the base field. Now we can ask questions like: is an isogeny necessary? Is a field extension necessary? In the following, we will consider these and similar CM lifting questions, and give a survey of results that are currently known.

Let us fix a finite field \mathbb{F}_q and an abelian variety A_0 of dimension $g > 0$ over \mathbb{F}_q . Assume A_0 is isotypic over \mathbb{F}_q . By results from previous sections, we know that A_0 admits a structure of a CM abelian variety with complex multiplication by a CM field. Consider the following types of questions about the existence of a CM lifting of A_0 .

- (CML) CM lifting: there exists a local domain R with characteristic 0 and residue field \mathbb{F}_q , an abelian scheme A over R of relative dimension g with a CM field $L \subseteq \text{End}^0(A)$ satisfying $[L : \mathbb{Q}] = 2g$ and an isomorphism $\phi : A \otimes_R \mathbb{F}_q \simeq A_0$ over \mathbb{F}_q .
- (R) CM lifting after finite residue field extension: there exists a local domain R of characteristic 0 and residue field k of finite degree over \mathbb{F}_q , an abelian scheme A over R with relative dimension g whose generic fiber admits sufficiently many complex multiplications by a CM field L with $[L : \mathbb{Q}] = 2g$, and an isomorphism $\phi : A \otimes_R k \simeq A_0 \otimes_{\mathbb{F}_q} k$ over k .
- (I) CM lifting up to isogeny: there exists a local domain R of characteristic 0 and residue field \mathbb{F}_q , an abelian scheme A over R with relative dimension g whose generic fiber admits sufficiently many complex multiplications by a CM field L with $[L : \mathbb{Q}] = 2g$ and an isogeny $A \otimes_R \mathbb{F}_q \sim A_0$ over \mathbb{F}_q .
- (NI) CM lifting to normal domains up to isogeny: there exists a normal local

domain R with characteristic 0 and residue field \mathbb{F}_q such that (I) is satisfied for A_0 using R .

- (NIR) CM lifting to normal domains up to isogeny after finite residue field extension: there exists a normal domain R with characteristic 0 and residue field k of finite degree over \mathbb{F}_q such that (R) is satisfied for A_0 using R except that ϕ is only required to be an isogeny over k .

For many of the above questions, answers are known.

Theorem I.28. (Oort) [17] *For all $g \geq 3$ and all $1 \leq f \leq g - 2$, there exists an abelian variety A over $\overline{\mathbb{F}_p}$ of dimension g and p -rank equal to f such that A does not admit a CM lifting to characteristic zero.*

Since we can express a local ring as a direct limit of local subrings, there is no loss of generality in replacing k with an algebraic closure of \mathbb{F}_q or with an arbitrary extension of \mathbb{F}_q in (R). Therefore, by the theorem above, we know in general (R) does not hold, and so the stronger statement (CML) does not generally hold either. Therefore we know an isogeny is necessary. Chai, Conrad, and Oort recently proved that (I) always holds ([3]). Therefore a field extension is not necessary.

Since whenever the base ring is normal, we can extend maps between abelian schemes easily, it is especially interesting to consider questions like (NI) and (NIR). Results of Honda and Tate imply that (NIR) can always be fulfilled with R a p -adic integer ring and $L \subseteq \text{End}^0(B)$ any CM field such that $[L : \mathbb{Q}] = 2g$ (see [2] for further explanation). In contrast, (NI) does not always hold. Chai, Conrad, and Oort [2] give a necessary and sufficient condition for (NI) to hold. They call it the *residue reflex condition*. We will give a detailed description of this condition and an example of its use.

Let L be a CM field, and p a prime number. Complex conjugation induces an involution ι on L . Let $\overline{\mathbb{Q}_p}$ be an algebraic closure of \mathbb{Q}_p . A subset $\Phi \subseteq \text{Hom}(L, \overline{\mathbb{Q}_p})$ is called a *p-adic CM type* if $\Phi \amalg \Phi \cdot \iota = \text{Hom}(L, \overline{\mathbb{Q}_p})$. Associated to the *p*-adic CM type Φ for L there is the *reflex field* $E \subseteq \overline{\mathbb{Q}_p}$ of finite degree over \mathbb{Q} , which can be defined as a subfield of $\overline{\mathbb{Q}}$ generated by the elements $\sum_{\phi \in \Phi} \phi(x)$, $x \in L$ (where $\overline{\mathbb{Q}}$ denotes the algebraic closure of \mathbb{Q} in $\overline{\mathbb{Q}_p}$). Equivalently, $\text{Gal}(\overline{\mathbb{Q}}/E)$ is the subgroup of elements of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ stabilizing the subset $\Phi \subseteq \text{Hom}(L, \overline{\mathbb{Q}})$.

Let A be an abelian variety of dimension $g > 0$ over \mathbb{F}_q and let $L \subseteq \text{End}^0(A)$ be a CM field with $[L : \mathbb{Q}] = 2g$. Let $\Phi \subseteq \text{Hom}(L, \overline{\mathbb{Q}_p})$ be a *p*-adic CM type. We say (L, Φ) satisfies the *residue reflex condition* if

1. for each *p*-adic place v on L ,

$$\frac{\text{ord}_v(\text{Fr}_{A,q})}{\text{ord}_v(q)} = \frac{\#\{\phi \in \Phi : \phi \text{ induces } v \text{ on } L\}}{[L_v : \mathbb{Q}_p]}$$

where $\text{Fr}_{A,q} \in \mathcal{O}_L$ acts on A by the q -Frobenius endomorphism.

2. Let $E \subseteq \overline{\mathbb{Q}_p}$ be the reflex field attached to (L, Φ) , and let v be the induced *p*-adic place of E . The residue field k_v of $\mathcal{O}_{E,v}$ can be realized as a subfield of \mathbb{F}_q .

It is not hard to show that if (NI) holds, the residue reflex condition must be satisfied – that is, this is a necessary condition for (NI) to hold.

Remark I.29. Clause (1) of the residue reflex condition basically tells us the slopes of A are given in terms of (L, Φ) by the Shimura-Taniyama formula. Any CM field $L \subseteq \text{End}^0(A)$ with $[L : \mathbb{Q}] = 2g$ admits a *p*-adic CM type Φ such that (1) holds, so (1) is not a significant constraint. Clause (2) is more interesting. Brian Conrad uses Honda-Tate theory to give examples such that for $L \subseteq \text{End}^0(A)$ a CM field of degree

$2g$, every p -adic CM type (L, Φ) satisfies (1) but violates (2). Clause (2) essentially tells us that the residue field should not be too big.

Theorem I.30. *(Conrad, Chai, Oort)[2] Let A be an abelian variety of dimension $g > 0$ over \mathbb{F}_q and let $L \subseteq \text{End}^0(A)$ be a CM field with $[L : \mathbb{Q}] = 2g$. Let $\Phi \subseteq \text{Hom}(L, \overline{\mathbb{Q}_p})$ be a p -adic CM type, and let $E \subseteq \overline{\mathbb{Q}_p}$ be the associated reflex field. Assume that (L, Φ) satisfies the residue reflex condition. Then A satisfies (NI) using a lifting of the L -action over a p -adic integer ring with residue field \mathbb{F}_q .*

Next, we give an example for which (NI) fails to hold. This example is due to Brian Conrad.

Example I.31. Let $\pi = p \cdot \zeta_5$. This is a Weil p^2 -number. Assume $p \equiv 2 \pmod{5}$ or $p \equiv 3 \pmod{5}$, so p is inert in $\mathbb{Q}(\zeta_5)/\mathbb{Q}$. By the Honda-Tate Theorem I.19 and Theorem I.21, there is (uniquely up to isogeny) a simple abelian variety B over \mathbb{F}_{p^2} such that the center of $\text{End}_{\mathbb{F}_{p^2}}^0(B)$ may be identified with $F := \mathbb{Q}[\pi] = \mathbb{Q}(\zeta_5)$ by $\pi \mapsto \text{Fr}_{B, p^2}$. Also, the central division algebra $D := \text{End}_{\mathbb{F}_{p^2}}^0(B)$ over F is split away from the unique p -adic place of F . Therefore, it is split globally, so $D = F$. Thus

$$2 \dim(B) = [F : \mathbb{Q}] \cdot \sqrt{[D : F]} = 4,$$

so $\dim(B) = 2$ and $\text{End}_{\mathbb{F}_{p^2}}^0(B) \cong F = \mathbb{Q}(\zeta_5)$.

The only CM structure on B is the canonical one by the action of $\mathbb{Q}(\zeta_5)$ (up to automorphisms of $\mathbb{Q}(\zeta_5)$). Since F is Galois over \mathbb{Q} , for any CM type Φ on F , the reflex field E associated to (F, Φ) is contained in the canonical image of F in $\overline{\mathbb{Q}}$. Note that the reflex field is also a CM field. Thus $E \cong F$ because F has no proper CM subfield. Assume there is an abelian scheme X over a normal local domain R of characteristic 0 and residue field \mathbb{F}_{p^2} which is a CM lifting of B up to isogeny over $k = \mathbb{F}_{p^2}$. By the necessity of the residue reflex field condition, the residue field of R

(\mathbb{F}_{p^2}) should contain the residue field of E , the reflex field associated to (F, Φ) . Since $E \cong F$ and p is inert in F , E admits a unique p -adic place at which E has residue field \mathbb{F}_{p^4} . Therefore, we have a contradiction, so no such X exists and B does not satisfy (NI).

CHAPTER II

p -divisible Groups and Dieudonné Modules

In characteristic zero, the tangent space of an abelian variety is a useful invariant, whereas in positive characteristic the tangent space fails to be an isogeny invariant. Therefore, we need a good substitute. The concept of p -divisible groups is the right one to use for this purpose, as well as for studying infinitesimal properties, when $\text{char}(k) = p > 0$.

2.1 p -divisible Groups

Definition II.1. Let S be a scheme and h a nonnegative integer. A p -divisible group of height h over S is an inductive system $\{(G_n, i_n)\}_{n \geq 0}$ where for all n , G_n is a finite flat group scheme over S of rank p^{hn} , and the sequence

$$0 \rightarrow G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{\times p^n} G_{n+1}$$

is exact. A *morphism* of between p -divisible groups $\{(G_n, i_n)\}$ and $\{(H_n, j_n)\}$ is a sequence of morphisms $f_n : G_n \rightarrow H_n$ at each level such that for every n , $f_{n+1} \circ i_n = j_n \circ f_n$. We write $G := \varinjlim G_n$ in the category of inductive systems of finite group schemes.

Remark II.2. A p -divisible group is also known by the term Barsotti-Tate group.

Example II.3. For any abelian scheme A over S and any integer $u \geq 0$, the group scheme $A[u]$ is a finite flat group scheme of rank u^{2g} over S , where $g = \dim A$. Therefore, $\{A[p^n]\}_{n \geq 0}$ forms a p -divisible group of height $2g$. We denote this p -divisible group by $A[p^\infty]$.

Let $G = \varinjlim (G_n, i_n)$ be a p -divisible group over a base scheme S . By Cartier duality, the associated surjections $p_n : G_{n+1} \rightarrow G_{n+1}/G_1 = G_n$ give closed immersions $D(p_n) : D(G_n) \rightarrow D(G_{n+1})$, where $D(G_n)$ denotes the Cartier dual of G_n . Then $G^\vee := \varinjlim D(G_n)$ is a p -divisible group, called the *Serre dual* of G . The height of G^\vee equals the height of G . If A^\vee denotes the dual abelian scheme to A , then by Cartier-Nishi duality, there is a natural isomorphism $A^\vee[p^\infty] \cong (A[p^\infty])^\vee$.

2.2 p -divisible Groups of CM Type

Let R be a complete local Noetherian domain of generic characteristic zero. A p -divisible group \mathcal{H} over R is said to be of *CM type* if there exists a commutative semi-simple algebra L over \mathbb{Q}_p and a monomorphism $i : L \rightarrow \text{End}^0(\mathcal{H})$ such that $\dim_{\mathbb{Q}_p} L$ equals the height of \mathcal{H} . For a particular such L , we say that \mathcal{H} has CM by L . The *CM type* Φ of (\mathcal{H}, i) is a subset of $\text{Hom}_{\mathbb{Q}_p}(L, \overline{\text{frac}(R)})$ such that the action of L decomposes the tangent space $\text{Lie}(\mathcal{H}) \otimes_R \overline{\text{frac}(R)}$ (over $\overline{\text{frac}(R)}$) into the direct sum of eigenlines $\bigoplus_{\phi \in \Phi} E_\phi$, for which L acts through ϕ on E_ϕ .

Let H be a p -divisible group over a field k of characteristic $p > 0$. We say that H admits a *CM lifting* if there is a p -divisible group \mathcal{H} of CM type over a complete Noetherian local domain R of generic characteristic 0 with maximal ideal \mathfrak{m} , and a ring homomorphism $R/\mathfrak{m} \rightarrow k$ such that (taking tensor products with respect to this homomorphism) $\mathcal{H} \otimes_{\text{Spec}(R)} \text{Spec}(k) \cong H$.

We will now examine how the CM lifting of an abelian variety can be related to

the CM lifting of an associated p -divisible group. Assume A_0 is an abelian variety with complex multiplication by L over k , where L is a CM field and k is a finite field with characteristic p . Fix an action of an order of \mathcal{O}_L . The Serre-Tate theorem [18] tells us that the following two constructions are equivalent (in that one can be done if and only if the other can be done);

- constructing a formal abelian scheme A over a complete Noetherian local domain R (with generic characteristic zero and residue field k) such that A/R is a lifting of A_0 and the action lifts to A ;
- constructing a p -divisible group \mathcal{H} over R such that it is a lifting of $A_0[p^\infty]$ and the action lifts to \mathcal{H} .

Of course, we may ask if the formal scheme obtained is algebraic. We will answer this question later.

Informally, the Serre-Tate theorem tells us that deformations of abelian varieties are controlled by their associated p -divisible groups. Correspondingly, p -divisible groups and their deformations are more or less controlled by their Dieudonné modules (as we will see in the following section).

2.3 Dieudonné Modules

In this section, we present basic Dieudonné module theory for p -divisible groups (for more detail, see [4]). This theory gives us a framework for a categorical (i.e., via functors) equivalence between p -divisible groups and modules over some non-commutative rings. As a result it provides us with a way to translate lifting problems for p -divisible groups into linear algebra problems involving modules over noncommutative rings. Such a result plays an important role in solving related CM lifting

problems, as it replaces abstract, algebraic objects with ones on which we can do concrete computations.

There are different versions of Dieudonné module theory. Here we explain covariant Dieudonné module theory for p -divisible groups over a perfect field of characteristic $p > 0$ (although in this case, the covariant and contravariant versions are anti-equivalent).

Our setup is as follows. Let k be a perfect field of characteristic p and $W(k)$ the associated ring of Witt vectors. We note that $W(k)$ is a complete discrete valuation ring with residue field k . Denote by $\sigma : W(k) \rightarrow W(k)$ the Teichmüller lift of the automorphism $x \mapsto x^p$ of k . Let D_k be the ring generated by $W(k)$, F , and V , such that $F \cdot V = V \cdot F = p$, and for all $a \in W(k)$, $F \cdot a = (\sigma a) \cdot F$ and $a \cdot V = V \cdot (\sigma a)$. A *Dieudonné module* is a left D_k -module M such that, viewed as a $W(k)$ -module, M is free and has finite rank.

Remark II.4. Note that D_k is a free left (or right) module over $W(k)$ with basis $\{\dots, V^2, V, F, F^2, \dots\}$. Further, if $k = \mathbb{F}_p$, then $D_k = \mathbb{Z}_p[F, V]/(F \cdot V - p)$ is a regular commutative ring with Krull dimension 2. In all other cases D_k is non-commutative.

To describe the correspondence between p -divisible groups and Dieudonné modules, we first make use of a decomposition which simplifies matters.

Theorem II.5. *Let G be a p -divisible group over a perfect field $k \supseteq \mathbb{F}_p$. Then there is a unique decomposition*

$$G = G_e \oplus G_m \oplus G_u$$

where G_e is the maximal étale quotient of G , G_m is the maximal multiplicative p -divisible subgroup of G , and G_u has no non-trivial étale quotient or multiplicative p -divisible subgroup.

Remark II.6. This theorem follows from an analogous theorem for finite commutative group schemes, found in Chapter 1 of [11]. We will see later (via the Serre-Tate Theorem, referenced in Section 2.4) that G_e and G_m always have a canonical lift to $W(k)$, so G_{ll} will be our primary concern.

Theorem II.7. (*Oda and Oort [16]*) *Given k , let D_k be defined as above.*

1. *There is an equivalence of categories between the category of p -divisible groups over k and the category of Dieudonné modules over D_k . Denote by $\mathbb{D}(G)$ the covariant Dieudonné module associated with G .*
2. *The rank of $\mathbb{D}(G)$ over $W(k)$ equals the height of G . Further, there is a functorial isomorphism $\text{Lie}(G) \cong \mathbb{D}(G)/V \cdot \mathbb{D}(G)$ (i.e. $\mathbb{D}(G)/V \cdot \mathbb{D}(G)$ is isomorphic to the tangent space of G).*
3. *The Dieudonné module $\mathbb{D}(G^\vee)$ and the linear dual of $\mathbb{D}(G)$*

$$(\mathbb{D}(G))^\vee := \text{Hom}_{W(k)}(\mathbb{D}(G), W(k))$$

are canonically isomorphic as $W(k)$ -modules. The actions of F and V on $(\mathbb{D}(G))^\vee$ satisfy

$$(F \cdot f)(x) = \sigma(f(Vx))$$

$$\sigma((V \cdot f)(x)) = f(Fx)$$

for all $f \in (\mathbb{D}(G))^\vee$ and $x \in \mathbb{D}(G)$.

4. *G is étale if and only if V is bijective on $\mathbb{D}(G)$. G is multiplicative if and only if F is bijective on $\mathbb{D}(G)$. G is local-local if and only if both F and V are topologically nilpotent on $\mathbb{D}(G)$.*

Lemma II.8. *Let G and H be two p -divisible groups of the same height and $f : G \rightarrow H$ a homomorphism. The following conditions are equivalent:*

- $\ker(f)$ is finite.
- f is an epimorphism.
- $\mathbb{D}(f) : \mathbb{D}(G) \rightarrow \mathbb{D}(H)$ is injective.

A proof of the lemma can be found in [6], Chapter IV, section 1. A homomorphism f satisfying the conditions of the lemma is called an *isogeny* (of p -divisible groups). We say G and H are *isogenous* if there is an isogeny from G to H .

2.4 Dieudonné modules and CM lifting

In this section, we explain how the problems of CM lifting can be translated into problems involving Dieudonné modules.

Let A be an abelian variety over a finite field k of characteristic p , such that A admits complex multiplication by a CM field K . There exists an abelian variety B isogenous to A over k such that \mathcal{O}_K acts on B (i.e., there is an embedding $\mathcal{O}_K \hookrightarrow \text{End}(B)$). Since the properties we will study only depend on the K -linear k -isogeny class of A , there is no loss of generality in assuming our abelian variety A has CM structure $i : \mathcal{O}_K \hookrightarrow \text{End}(A)$. For the dual abelian variety A^\vee , there is a natural action by \mathcal{O}_K , given by $i^\vee : \mathcal{O}_K \hookrightarrow \text{End}(A^\vee)$ such that $i^\vee(a) = i(\bar{a})^\vee$, where \bar{a} is the complex conjugation of a . By a lemma of Kottwitz ([10], lemma 9.2), the abelian variety (A, i) as defined above admits an \mathcal{O}_K -linear polarization $\lambda : A \rightarrow A^\vee$. Thus $\lambda i(a) = i(\bar{a})^\vee \lambda$ for all $a \in \mathcal{O}_K$.

Let $A[p^\infty]$ be the p -divisible group of A . The triple (A, λ, i) gives rise to the triple $(A[p^\infty], \lambda_p, i_p)$, where

$$i_p : \mathcal{O}_{K,p} \hookrightarrow \text{End}(A[p^\infty])$$

is the induced $\mathcal{O}_{K,p}$ action on $A[p^\infty]$ and

$$\lambda_p : A[p^\infty] \rightarrow A[p^\infty]^\vee$$

is the induced quasi-polarization of $A[p^\infty]$, such that $\lambda_p i_p(\bar{a}) = i_p(a)^\vee \lambda_p$ for all $a \in \mathcal{O}_{K,p}$.

Let $M = \mathbb{D}(A[p^\infty])$ be the covariant Dieudonné module of $A[p^\infty]$. Note that M is an $\mathcal{O}_{K,p} \otimes_{\mathbb{Z}_p} W(k)$ module, and the action of $\mathcal{O}_{K,p}$ commutes with F and V . The $\mathcal{O}_{K,p}$ -linear polarization of $A[p^\infty]$ gives rise to a nondegenerate skew-symmetric pairing $\langle \cdot, \cdot \rangle : M \times M \rightarrow W(k)$ such that $\langle Fx, y \rangle = \sigma(\langle x, Vy \rangle)$ for all $x, y \in M$. Further, the $\mathcal{O}_{K,p}$ action on $A[p^\infty]$ defines a $W(k)$ -linear action of $\mathcal{O}_{K,p}$ on M such that $\langle ax, y \rangle = \langle x, \bar{a}y \rangle$ for all $a \in \mathcal{O}_{K,p}$ and $x, y \in M$, since

$$\begin{aligned} \langle ax, y \rangle &= (\lambda_p(ax))(y) \\ &= (\bar{a}\lambda_p(x))(y) \\ &= \lambda_p(x)(\bar{a}y) = \langle x, \bar{a}y \rangle \end{aligned}$$

By the Serre-Tate theorem [18], lifting (A, λ, i) to a complete Noetherian local integral domain R with generic characteristic zero and residue field k is equivalent to lifting the attached p -divisible group $A[p^\infty]$ over R with additional structures. As k is perfect, by Theorem II.5, $G = A[p^\infty]$ can be expressed as $G_e \oplus G_m \oplus G_u$. Because there is a canonical lifting of $G_e \oplus G_m$ over $W(k)$ ([12], Appendix, pages 171–187), we only need to focus on the lifting of G_u .

Let M be the covariant Dieudonné module of G_u , with associated pairing $\langle \cdot, \cdot \rangle$. The operation V gives us a mod p filtration $\text{Fil} = VM/pM \subseteq M_0 := M/pM$. *Fontaine's theorem* (see [7], Theorem 2, pg. 217 and the remark on pg. 218) tells us that lifting G_u with additional structure to R is equivalent to lifting the triple $(M, \langle \cdot, \cdot \rangle, \text{Fil})$ to R as long as R is a p -adic complete discrete valuation ring such that

$e \leq p - 1$, where e is the ramification index of p in R . Here, to *lift* $(M, \langle \cdot, \cdot \rangle, \text{Fil})$ to R means to find an R -submodule N of $M \otimes_{W(k)} R$ such that;

1. $\langle N, N \rangle = 0$;
2. $N \otimes_R k \cong VM/pM$; and
3. N is stable under the action of $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Remark II.9. The mod p filtration $\text{Fil} = VM/pM \subseteq M_0$ satisfies the condition that the induced pairing $M_0 \times M_0 \rightarrow W(k)/pW(k) \cong k$ annihilates Fil .

Remark II.10. We can see, by an application of Fontaine's theorem, that we have some restrictions on the lifting ring R . We need e , the ramification index of p in R , to satisfy $e \leq p - 1$.

Now we may ask if, by using the approach above, the resulting formal abelian scheme which lifts A is algebraic. By a theorem of Grothendieck ([8], 5.4.5), we know that if we lift A along with an ample line bundle, then this lifting is automatically algebraic. Since lifting the polarization map λ is equivalent to lifting the line bundle associated to A (up to replacing λ with $[2]\lambda$, which is harmless), we do get an algebraic lifting.

2.5 Questions of Importance to This Dissertation

In Chapter I we introduced the notion of a CM lifting problem and discussed some known results. We aim to extend these questions by asking, if a lifting exists over a p -adic discrete valuation ring, what can be said about the ramification of the base ring to which we are lifting? For example:

- Can we determine the minimal ramification needed for a lifting to exist?
- For a fixed ramification, does there exist a lifting with that ramification?

- What if we fix a CM field and a CM type on it to be required to come from the desired lift?

The proofs of the previous results detailed in Chapter I relied heavily on deformation-theoretic methods which prevent any control over the ramification of the base ring. Therefore, different methods are required to answer questions of the type shown above. Translation of CM lifting into the language of Dieudonné modules fills this need, because this turns CM lifting problems into linear algebra problems, giving a concreteness which may make control over the ramification easier to attain.

In the next chapter, we determine (subject to some restrictions on k) invariants which classify, up to isomorphism and up to isogeny, the Dieudonné modules of CM p -divisible groups over a finite field. We also describe the possible pairings $\langle \cdot, \cdot \rangle$ of such Dieudonné modules respecting the CM structure, and how the pairing is changed by moving to a different module within the same isogeny class. These steps must be taken before attempting to solve CM lifting problems, for two reasons. First, as we mentioned in Chapter I, in general an isogeny is necessary for a CM lifting to exist, so we will need to be able to pick a suitable Dieudonné module from within an isogeny class. Second, we may find opportunities to simplify the appearance of $\langle \cdot, \cdot \rangle$ (and thus our calculations involving it) by passing to a different module within the same isogeny class. We must note, however, that we do not (in this dissertation) prove which invariants (as described above) arise from the Dieudonné modules of CM p -divisible groups over a finite field. Completion of this step is required before this description in terms of invariants can be termed a full classification.

CHAPTER III

Classification of Dieudonné Modules

3.1 Classification up to Isomorphism

We recall our setup from the previous chapters, with some new details. We assume we have:

1. k , a finite field of characteristic p and size q ,
2. K , a CM field of degree $2g$ over \mathbb{Q} ,
3. K_0 , the maximal totally real subfield of K ,
4. \mathcal{O}_K and \mathcal{O}_{K_0} , the rings of integers of K and K_0 , respectively,
5. (A, λ, i) , where A is an abelian variety of dimension g over k , $i : \mathcal{O}_K \rightarrow \text{End}(A)$ a ring homomorphism, and λ an \mathcal{O}_K -linear polarization of A , and
6. H , the attached p -divisible group of A .

We also assume throughout this chapter that k contains the residue field of \mathcal{O}_K at any place above p . This assumption serves two purposes. The first is to simplify the computations we will encounter. The second purpose is to guarantee the second requirement of the residue reflex condition of Section 1.3. The main theorem of this section is:

Theorem III.1. *Assume k contains k_v for all places v of K above p , and let $d = [k : \mathbb{F}_p]$. Then $\det_{\mathcal{O}_{K,p}}(V^d | \mathbb{D}(H))$ and $\text{Lie}(H)$ (as a monogenic $\mathcal{O}_K/(p) \otimes_{\mathbb{F}_p} k$ -module) determine H up to \mathcal{O}_K -linear k -isomorphism.*

Remark III.2. Instead of providing a single proof for this theorem, we pass to the v above p , proceeding according to cases, each with its own subtheorem (the combination of which produces this theorem), although the subtheorems use different notation.

The decomposition $\mathcal{O}_{K_0} \otimes \mathbb{Z}_p = \bigoplus_{v|p} \mathcal{O}_{K_0,v}$ gives rise to a decomposition of p -divisible groups $H = \bigoplus_{v|p} H_v$, such that each H_v is a quasi-polarized p -divisible $\mathcal{O}_{K_0,v}$ group of height $2g_v$, where $g_v = [K_{0,v} : \mathbb{Q}_p]$ (because $\mathcal{O}_{K_0} \otimes \mathbb{Z}_p$ acts faithfully on H , each H_v is non-zero). Let M_v be the Dieudonne module $\mathbb{D}(H_v)$, so M_v is a free rank two module over $\mathcal{O}_{K_0,v} \otimes_{\mathbb{Z}_p} W(k)$. Fix one such v and proceed according to three cases.

Case 1: v splits in K .

Denote by k_v the residue field of \mathcal{O}_{K_0} at v . Let $f = [k_v : \mathbb{F}_p]$, and $e := e(K_{0,v}/\mathbb{Q}_p)$ be the ramification index of $K_{0,v}$. Assume w, \bar{w} are the primes in K above v ; then $K_v = K_w \times K_{\bar{w}}$ and $K_w = K_{\bar{w}} = K_{0,v}$. We may write $H_v = H_w \oplus H_{\bar{w}}$, and $M_v = M_w \oplus M_{\bar{w}}$, where M_w is a free rank one module over $\mathcal{O}_{K,w} \otimes_{\mathbb{Z}_p} W(k)$, and $M_{\bar{w}}$ is a free rank one module over $\mathcal{O}_{K,\bar{w}} \otimes_{\mathbb{Z}_p} W(k)$. Let k_w and $k_{\bar{w}}$ be the residue fields of $\mathcal{O}_{K,w}$ and $\mathcal{O}_{K,\bar{w}}$ at w and \bar{w} , respectively (so $k_w \cong k_v \cong k_{\bar{w}}$). We know that $W(k_w)$ and $W(k_{\bar{w}})$ are isomorphic to the maximal unramified extension of $\mathcal{O}_{K,w}$ and $\mathcal{O}_{K,\bar{w}}$, respectively, over \mathbb{Z}_p .

Let $\sigma_1, \sigma_2, \dots, \sigma_f$ be the embeddings of $W(k_w)$ into $W(k)$. We choose the indices such that for all $i \in \mathbb{Z}/f\mathbb{Z}$, $\sigma_{i+1} = \sigma \circ \sigma_i$, where σ is Frobenius on $W(k)$. Note that if τ denotes complex conjugation on K , $\sigma_1 \circ \tau, \sigma_2 \circ \tau, \dots, \sigma_f \circ \tau$ will be the embeddings

of $W(k_{\bar{w}})$ into $W(k)$. Let $R_{w,i}$ denote the tensor product $\mathcal{O}_{K,w} \otimes_{W(k_w)} W(k)$, using σ_i to embed $W(k_w)$ into $W(k)$. Note that $R_{w,i}$ is a complete discrete valuation ring of ramification index e and residue degree 1 over $W(k)$. Define $R_{\bar{w},i}$ similarly (i.e., \bar{w} in place of w and $\sigma_i \circ \tau$ in place of σ_i). Then we have canonical decompositions:

$$\mathcal{O}_{K,w} \otimes_{\mathbb{Z}_p} W(k) = \prod_{i \in \mathbb{Z}/f\mathbb{Z}} R_{w,i}$$

$$\mathcal{O}_{K,\bar{w}} \otimes_{\mathbb{Z}_p} W(k) = \prod_{i \in \mathbb{Z}/f\mathbb{Z}} R_{\bar{w},i}$$

These decompositions give rise to decompositions of $W(k)$ -modules:

$$M_w = \bigoplus_{i \in \mathbb{Z}/f\mathbb{Z}} M_{w,i}$$

$$M_{\bar{w}} = \bigoplus_{i \in \mathbb{Z}/f\mathbb{Z}} M_{\bar{w},i}$$

For all i , $M_{w,i}$ is a free rank one $R_{w,i}$ module and $M_{\bar{w},i}$ is a free rank one $R_{\bar{w},i}$ module. The operators V and F interact with this decomposition by $VM_{w,i} \subseteq M_{w,i-1}$ and $FM_{w,i} \subseteq M_{w,i+1}$, with corresponding relations holding for the $M_{\bar{w},i}$ (so $V^f M_{w,i}$ and $F^f M_{w,i}$ are each subsets of $M_{w,i}$ itself).

Recall from Theorem II.7 that $\text{Lie}(M_w) \cong M_w/VM_w$. Note that $pM_w \subseteq VM_w$.

We may therefore view $\text{Lie}(M_w)$ as a module over

$$\begin{aligned} \mathcal{O}_{K,w} \otimes_{\mathbb{Z}_p} k &\cong \mathcal{O}_{K,w} \otimes_{W(k_w)} (W(k_w) \otimes_{\mathbb{Z}_p} k) \\ &\cong \prod_{i \in \mathbb{Z}/f\mathbb{Z}} (\mathcal{O}_{K,w}/(p)) \otimes_{(k_w,i)} k \end{aligned}$$

where $(\mathcal{O}_{K,w}/(p)) \otimes_{(k_w,i)} k$ denotes the tensor product using the embedding $\sigma_i : k_w \hookrightarrow k$. This gives us a k -linear decomposition of Lie algebras:

$$\text{Lie}(M_w) = \bigoplus_{i \in \mathbb{Z}/f\mathbb{Z}} \text{Lie}(M_w)_i,$$

and similarly for $\text{Lie}(M_{\bar{w}})$. If we choose a uniformizer π of $\mathcal{O}_{K_0,v} \cong \mathcal{O}_{K,w}$, then for every i , $(\mathcal{O}_{K,w}/(p)) \otimes_{(k_w,i)} k \cong k[\pi]/(\pi)^e$. Since $\text{Lie}(M_w)_i$ is generated by a single element over $(\mathcal{O}_{K,w}/(p)) \otimes_{(k_w,i)} k$, it is isomorphic to $(k[\pi]/(\pi)^e)/I$ for some ideal I . The only ideals of $k[\pi]/(\pi)^e$ are those generated by $\pi^{e'}$ for some $e' \leq e$. Hence, for some sequence of nonnegative integers $e_{w,i}$, we obtain $\text{Lie}(M_w)_i \cong k[\pi]/(\pi^{e_{w,i}})$ as k -vector spaces. The same reasoning yields a corresponding result for the $\text{Lie}(M_{\bar{w}})_i$, for some sequence of integers $e_{\bar{w},i}$. Note that $\sum_i e_{w,i} = \dim H_w$ and $\sum_i e_{\bar{w},i} = \dim H_{\bar{w}}$. Denote the sequence $\{(e_{w,i}, e_{\bar{w},i})\}_{i \in \mathbb{Z}/f\mathbb{Z}}$ by $e(M_v)$.

Choose generators $x_{w,i}$ for $M_{w,i}$ over $R_{w,i}$, and generators $x_{\bar{w},i}$ for $M_{\bar{w},i}$ over $R_{\bar{w},i}$. For $i \in \mathbb{Z}/f\mathbb{Z}$, let $\theta_{w,i} \in R_{w,i}$ and $\theta_{\bar{w},i} \in R_{\bar{w},i}$ be such that $Vx_{w,i} = \theta_{w,i-1}x_{w,i-1}$ and $Vx_{\bar{w},i} = \theta_{\bar{w},i-1}x_{\bar{w},i-1}$.

Remark III.3. For the remainder of this chapter, our convention is that arithmetic on the indices of generators and coefficients is done modulo f (or $2f$ in the case where v is inert), but arithmetic on powers of σ is *not* done modulo f .

For all i , we have the following isomorphisms of k -vector spaces:

$$k[\pi]/(\pi)^{e_{w,i}} \cong \text{Lie}(M_w)_i \cong M_{w,i}/VM_{w,i+1} = R_{w,i}x_{w,i}/\theta_{w,i}x_{w,i} \cong k[\pi]/(\pi)^{\text{ord}_v(\theta_{w,i})},$$

with the second isomorphism arising from the fact that $\text{Lie}(M_w) = M_w/VM_w$ (functorially in M_w). Therefore, for all i , $\text{ord}_v(\theta_{w,i}) = e_{w,i}$, and by a similar argument, $\text{ord}_v(\theta_{\bar{w},i}) = e_{\bar{w},i}$. Since v is split, $\text{ord}_w(\theta_{w,i}) = e_{w,i}$ and $\text{ord}_{\bar{w}}(\theta_{\bar{w},i}) = e_{\bar{w},i}$. We may also obtain an upper bound for $e_{w,i}$ (and by a corresponding argument, $e_{\bar{w},i}$):

$$px_{w,i+1} = FVx_{w,i+1} = F(\theta_{w,i}x_{w,i}) = \sigma(\theta_{w,i})\delta x_{w,i+1}$$

for some $\delta \in R_{w,i+1}$. From this we obtain $\text{ord}_w(p) = e_{w,i} + \text{ord}_w(\delta)$. Since $\text{ord}_w(\delta) \geq 0$, $e_{w,i} \leq \text{ord}_w(p) = \text{ord}_v(p) = e$ for all i .

We observe that

$$V^f x_{w,i} = \left(\prod_{1 \leq j \leq f} \sigma^{j-f}(\theta_{w,i-j}) \right) x_{w,i}.$$

We apply the norm $N_{R_{w,i}/\mathcal{O}_{K,w}}$ to the coefficient, and since for $i, j \in \{1, \dots, f\}$ and $\delta \in R_{w,i}$,

$$N_{R_{w,i-j}/\mathcal{O}_{K,w}}(\sigma^{-j}(\delta)) = N_{R_{w,i}/\mathcal{O}_{K,w}}(\delta)$$

we obtain

$$\Delta_w := \prod_{1 \leq j \leq f} N_{R_{w,j}/\mathcal{O}_{K,w}}(\theta_{w,j})$$

which naturally does not depend on i . Note also that Δ_w is invariant under any change of basis (over all $R_{w,i}$), since if $x'_{w,i} = a_{w,i}x_{w,i}$ for $a_{w,i} \in R_{w,i}^\times$,

$$V^f x'_{w,i} = \frac{\sigma^{-f}(a_{w,i})}{a_{w,i}} \left(\prod_{1 \leq j \leq f} \sigma^{j-f}(\theta_{w,i-j}) \right) x'_{w,i}$$

and $\frac{\sigma^{-f}(a_{w,i})}{a_{w,i}}$ has norm 1. Because $\{x_{w,i}\}_{i \in \mathbb{Z}/f\mathbb{Z}}$ forms a basis for M_w over $\mathcal{O}_{K,w}$, Δ_w is invariant under any change of basis over $\mathcal{O}_{K,w}$ – actually, it is $\det_{\mathcal{O}_{K,w}}(V^f)$. Define $\Delta_{\bar{w}}$ similarly, and let $\Delta(M_w)$ denote the pair $(\Delta_w, \Delta_{\bar{w}})$.

Theorem III.4. M_v is determined up to isomorphism by $e(M_v)$ and $\Delta(M_v)$.

Proof. It is clear that if $M_v \cong N_v$, $e(M_v) = e(N_v)$ and $\Delta(M_v) = \Delta(N_v)$. Conversely, assume $e(M_v) = e(N_v)$ and $\Delta(M_v) = \Delta(N_v)$. We will show how to construct an isomorphism between M_w and N_w – the isomorphism between $M_{\bar{w}}$ and $N_{\bar{w}}$ may be constructed similarly.

Let $x_{w,i}$ and $\theta_{w,i}$ be for M_w as above and $y_{w,i}$ the generators of $N_{w,i}$ over $R_{w,i}$. Since $e(M_v) = e(N_v)$, we may choose $u_i \in R_{w,i}^\times$ such that for all $i \in \mathbb{Z}/f\mathbb{Z}$, $Vy_{w,i} = u_{i-1}\theta_{w,i-1}y_{w,i-1}$. We will first find $a_1 \in R_{w,1}^\times$ such that $a_1 = \sigma^{-f}(a_1) \prod_{1 \leq j \leq f} \sigma^{1-j}(u_j)$ – then $x_{w,i} \mapsto a_i y_{w,i}$ will supply the desired isomorphism, where $a_{i-1} = \sigma^{-1}(a_i)u_{i-1}$ for all i .

Since $\Delta(M_v) = \Delta(N_v)$, we have

$$\begin{aligned}
\prod_{1 \leq j \leq f} N_{R_{w,j}/\mathcal{O}_{K,w}}(\theta_{w,j}) &= \prod_{1 \leq j \leq f} N_{R_{w,j}/\mathcal{O}_{K,w}}(u_j \theta_{w,j}) \\
&= \prod_{1 \leq j \leq f} N_{R_{w,j}/\mathcal{O}_{K,w}}(u_j) \cdot \prod_{1 \leq j \leq f} N_{R_{w,j}/\mathcal{O}_{K,w}}(\theta_{w,j}) \\
&= N_{R_{w,1}/\mathcal{O}_{K,w}} \left(\prod_{1 \leq j \leq f} \sigma^{1-j}(u_j) \right) \cdot \prod_{1 \leq j \leq f} N_{R_{w,j}/\mathcal{O}_{K,w}}(\theta_{w,j})
\end{aligned}$$

That is, $\prod_{1 \leq j \leq f} \sigma^{1-j}(u_j)$ has norm 1 and (since $R_{w,1}/\mathcal{O}_{K,w}$ is unramified) is thus equal to $\sigma^f(a)/a$ for some unit a . We may take a_1 to be $\sigma^f(a)$.

We now prove that $x_{w,i} \mapsto a_i y_{w,i}$ is an isomorphism of Dieudonné modules. It is clearly an isomorphism of $\mathcal{O}_{K,w} \otimes_{\mathbb{Z}_p} W(k)$ -modules since each a_i is a unit in $R_{w,i}$. Therefore it remains only to be shown that the mapping respects the action of V and F . The former is evident – $V(a_i y_{w,i}) = \sigma^{-1}(a_i) u_{i-1} \theta_{w,i-1} y_{w,i-1} = a_{i-1} V y_{w,i}$.

For $i \in \mathbb{Z}/f\mathbb{Z}$, fix $\delta_i, \delta'_i \in R_{w,i}$ such that for all i , $F x_{w,i-1} = \delta_i x_{w,i}$ and $F y_{w,i-1} = \delta'_i y_{w,i}$. These play a role similar to the $\theta_{w,i}$, and we may manipulate them in a similar way:

Lemma III.5. *For all i , $\sigma(u_{i-1})\delta'_i = \delta_i$.*

Proof. For every i , $FV x_{w,i} = p x_{w,i}$. It follows that $p = \delta_i \sigma(\theta_{w,i})$. On the other hand, $FV y_{w,i} = p y_{w,i}$, implying $p = \delta'_i \sigma(u_{i-1}) \sigma(\theta_{w,i})$. The desired equality follows immediately. \square

We observe that for all i , $a_{i+1} \sigma(u_i) = \sigma(a_i)$ (this is merely applying σ to the recursive definition of the a_i and shifting indices). Now,

$$\begin{aligned}
F(a_i y_{w,i}) &= \sigma(a_i) \delta'_{i+1} y_{w,i-1} \\
&= \sigma(a_i) / \sigma(u_i) \delta_{i+1} y_{w,i+1} \\
&= a_{i+1} \delta_{i+1} y_{w,i+1} = a_{i+1} F y_{w,i},
\end{aligned}$$

completing the proof. □

Now we consider the pairing $\langle \cdot, \cdot \rangle : M_v \times M_v \rightarrow W(k)$. We first observe that the only non-zero pairings occur in $M_{w,i} \times M_{\bar{w},i}$ and $M_{\bar{w},i} \times M_{w,i}$ for $1 \leq i \leq f$. For example, if $a \in R_{w,i}$ and y is an element of $M_{w,j}$ for any j , then $\langle ax_{w,i}, y \rangle = \langle x_{w,i}, \bar{a}y \rangle = 0$ since the action of $\bar{a} \in R_{\bar{w},i}$ is trivial on $M_{w,j}$ for all j . Arguments for the other possible situations follow the same path. Also, by skew-symmetry, if $a \in R_{w,i}$ and $b \in R_{\bar{w},i}$, then $\langle ax_{w,i}, bx_{\bar{w},i} \rangle = -\langle bx_{\bar{w},i}, ax_{w,i} \rangle$, so the behavior of $\langle \cdot, \cdot \rangle$ restricted to $M_{\bar{w},i} \times M_{w,i}$ is determined by the behavior of $\langle \cdot, \cdot \rangle$ restricted to $M_{w,i} \times M_{\bar{w},i}$. Therefore we may restrict our attention to domains of the latter type.

Define the $W(k)$ -linear homomorphism $\phi : R_{w,i} \rightarrow W(k)$ by letting $\phi(a) = \langle ax_{w,i}, x_{\bar{w},i} \rangle$. By Definition III.2.1 of [15] and the discussion preceding it, there exists $C_{w,i}$ in the inverse different $\delta_{R_{w,i}/W(k)}$ such that $\phi(a) = \text{Tr}_{R_{w,i}/W(k)}(C_{w,i}a)$ for all $a \in R_{w,i}$. It then follows that for all $a \in R_{w,i}$ and $b \in R_{\bar{w},i}$,

$$\langle ax_{w,i}, bx_{\bar{w},i} \rangle = \langle \bar{a}bx_{w,i}, x_{\bar{w},i} \rangle = \phi(\bar{a}b) = \text{Tr}_{R_{w,i}/W(k)}(C_{w,i}\bar{a}b)$$

Note that

$$\langle \sigma^{-1}(a)\theta_{w,i-1}x_{w,i-1}, \sigma^{-1}(b)\theta_{\bar{w},i-1}x_{\bar{w},i-1} \rangle = \langle V(ax_{w,i}), V(bx_{\bar{w},i}) \rangle = p\sigma^{-1}(\langle ax_{w,i}, bx_{\bar{w},i} \rangle).$$

Therefore, we have

$$\text{Tr}_{R_{w,i-1}/W(k)}(C_{w,i-1}\theta_{w,i-1}\overline{\theta_{\bar{w},i-1}}\sigma^{-1}(\bar{a}b)) = \text{Tr}_{R_{w,i-1}/W(k)}(p\sigma^{-1}(C_{w,i})\sigma^{-1}(\bar{a}b))$$

Since a and b are arbitrary, $C_{w,i-1}\theta_{w,i-1}\overline{\theta_{\bar{w},i-1}} = p\sigma^{-1}(C_{w,i})$ for all i . As mentioned before $\text{ord}_v(\theta_{w,i-1}) = e_{w,i-1}$ and $\text{ord}_v(\overline{\theta_{\bar{w},i-1}}) = e_{\bar{w},i-1}$, and these are invariant with respect to change of basis, so $\text{ord}_v(C_{w,i-1}) - \text{ord}_v(C_{w,i}) = \text{ord}_v(p) - e_{w,i-1} - e_{\bar{w},i-1}$

is as well. Note that summing both sides over all $i \in \mathbb{Z}/f\mathbb{Z}$ produces the identity $\text{ord}_v(p^f) = \dim H_v$. Further, each $\text{ord}_v(C_{w,i})$ is itself invariant with respect to change of basis – replacing $x_{w,i}$ with $t_i x_{w,i}$ and $x_{\bar{w},i}$ with $s_i x_{\bar{w},i}$ has the effect of replacing $C_{w,i}$ with $t_i \bar{s}_i C_{w,i}$ for $t_i \in R_{w,i}^\times$ and $s_i \in R_{\bar{w},i}^\times$.

Note none of the above is affected by any change of basis. Further, given any sequence D_i from the inverse different such that $\text{ord}_v(D_i) = \text{ord}_v(C_{w,i})$ for all i , we may change basis so that $C_{w,i}$ is replaced with D_i with respect to the new basis. Specifically, if $D_i = u_i C_{w,i}$ for all i , then letting $x'_{w,i} = u_i x_{w,i}$ and $x'_{\bar{w},i} = x_{\bar{w},i}$ will replace $C_{w,i}$ with D_i .

Case 2: v is inert in K .

Let k_v be the residue field of \mathcal{O}_K at v and f the residue degree of \mathcal{O}_{K_0} at v . Denote by $\sigma_1, \sigma_2, \dots, \sigma_{2f}$ the embeddings of $W(k_v)$ into $W(k)$, choosing the indices such that for all $i \in \mathbb{Z}/2f\mathbb{Z}$, $\sigma \circ \sigma_i = \sigma_{i+1}$, and $\sigma_{i+f} = \bar{\sigma}_i$ (σ_i composed with complex conjugation in $W(k_v)$, as inherited from the usual isomorphism to the maximal unramified extension of \mathbb{Z}_p in $\mathcal{O}_{K,v}$). For $i \in \mathbb{Z}/f\mathbb{Z}$ let $R_{v,i}$ and $\overline{R_{v,i}}$ denote $\mathcal{O}_{K,v} \otimes_{W(k_v)} W(k)$, using σ_i and $\bar{\sigma}_i$, respectively, to embed $W(k_v)$ into $W(k)$. Then

$$\mathcal{O}_{K,v} \otimes_{\mathbb{Z}_p} W(k) = \prod_{i \in \mathbb{Z}/f\mathbb{Z}} (R_{v,i} \times \overline{R_{v,i}})$$

gives rise to the decompositions

$$M_v = \bigoplus_{i \in \mathbb{Z}/f\mathbb{Z}} (M_{v,i} \oplus \overline{M_{v,i}})$$

$$\text{Lie}(M_v) = \bigoplus_{i \in \mathbb{Z}/f\mathbb{Z}} (\text{Lie}(M_v)_i \oplus \overline{\text{Lie}(M_v)_i})$$

where $M_{v,i} \oplus \overline{M_{v,i}}$ is a free rank one module over $R_{v,i} \times \overline{R_{v,i}}$. As before (by the same argument) we have

$$\text{Lie}(M_v)_i \cong k[\pi]/(\pi^{e_i})$$

$$\overline{\text{Lie}(M_v)_i} \cong k[\pi]/(\pi^{\bar{e}_i})$$

as k -vector spaces for some integers $e_i, \bar{e}_i \leq \text{ord}_v(p) = e = e(K_{0,v}/\mathbb{Q}_p)$. Denote the sequence $\{(e_i, \bar{e}_i)\}_{i \in \mathbb{Z}/f\mathbb{Z}}$ by $e(M_v)$.

Choose generators x_i for $M_{v,i}$ over $R_{v,i}$, and generators \bar{x}_i for $\overline{M_{v,i}}$ over $\overline{R_{v,i}}$. For $i \in \mathbb{Z}/f\mathbb{Z}$, let $\theta_i \in R_{v,i}$ and $\phi_i \in \overline{R_{v,i}}$ be such that $Vx_1 = \phi_f \bar{x}_f$, $V\bar{x}_1 = \theta_f x_f$, and for $i \neq 1$, $Vx_i = \theta_{i-1} x_{i-1}$ and $V\bar{x}_i = \phi_{i-1} \bar{x}_{i-1}$. By an argument similar to the one from Case 1, $\text{ord}_v(\theta_i) = e_i$ and $\text{ord}_v(\phi_i) = \bar{e}_i$ (these are invariant with respect to change of basis).

Using a line of reasoning similar to the one used in Case 1, we may define

$$\Delta(M) := \det_{\mathcal{O}_{K,w}}(V^{2f}) = \prod_{1 \leq j \leq f} N_{R_{v,j}/\mathcal{O}_{K,v}}(\theta_j) \cdot N_{\overline{R_{v,j}}/\mathcal{O}_{K,v}}(\phi_j)$$

which is invariant with respect to change of basis.

Theorem III.6. M_v is determined up to isomorphism by $e(M_v)$ and $\Delta(M_v)$.

Proof. By essentially the same argument as for Theorem III.4. □

Now we consider the pairing $\langle \cdot, \cdot \rangle$. Similarly to Case 1, we need only consider the behavior of this pairing when restricted to $M_{v,i} \times \overline{M_{v,i}}$. As before, there exist constants (now denoted $C_{v,i}$) in the inverse different $\delta_{R_{v,i}/W(k)}$ such that for all $i \in \mathbb{Z}/f\mathbb{Z}$, $a \in R_{v,i}$, and $b \in \overline{R_{v,i}}$,

$$\langle ax_i, b\bar{x}_i \rangle = \text{Tr}_{R_{v,i}/W(k)}(C_{v,i} a\bar{b})$$

As before, we can use the relation $\langle Vax_i, Vb\bar{x}_i \rangle = p\sigma^{-1}\langle ax_i, b\bar{x}_i \rangle$ to obtain, for $i \neq 1$, $\theta_{i-1}\overline{\phi_{i-1}}C_{v,i-1} = p\sigma^{-1}(C_{v,i})$. For $i = 1$, we have,

$$\begin{aligned}
Tr_{\overline{R_{v,f}/W(k)}}(p\sigma^{-1}(C_{v,1})\sigma^{-1}(\overline{ab})) &= p\sigma^{-1}(\langle ax_1, b\bar{x}_1 \rangle) \\
&= \langle Vax_1, Vb\bar{x}_1 \rangle \\
&= \langle \sigma^{-1}(a)\phi_f\bar{x}_f, \sigma^{-1}(b)\theta_f x_f \rangle \\
&= -\langle \sigma^{-1}(b)\theta_f x_f, \sigma^{-1}(a)\phi_f\bar{x}_f \rangle \\
&= Tr_{R_{v,f}/W(k)}(-\theta_f\overline{\phi_f}C_{v,f}\sigma^{-1}(\overline{ab})) \\
&= Tr_{\overline{R_{v,f}/W(k)}}(-\overline{\theta_f}\phi_f\overline{C_{v,f}}\sigma^{-1}(\overline{ab}))
\end{aligned}$$

Therefore, $-\overline{\theta_f}\phi_f\overline{C_{v,f}} = p\sigma^{-1}(C_{v,1})$.

The rest of the analysis goes as it did in the split case. Again, for all $i \in \mathbb{Z}/f\mathbb{Z}$ we have $\text{ord}_v(C_{v,i-1}) - \text{ord}_v(C_{v,i}) = \text{ord}_v(p) - e_{i-1} - \overline{e_{i-1}}$, $\text{ord}_v(C_{v,i})$ is invariant under change of basis, and if D_i is a sequence from the inverse different such that $\text{ord}_v(D_i) = \text{ord}_v(C_{v,i})$ for all i , then there is a change of basis that has the effect of replacing each $C_{v,i}$ with D_i .

Case 3: v is ramified in K .

Let w be the prime in K above v , k_w the residue field of \mathcal{O}_K at w , $f = [k_w : \mathbb{F}_p]$, and $\sigma_1, \sigma_2, \dots, \sigma_f$ be the embeddings of $W(k_w)$ into $W(k)$, with the indices chosen so that for all $i \in \mathbb{Z}/f\mathbb{Z}$, $\sigma \circ \sigma_i = \sigma_{i+1}$. Let $R_{w,i}$ denote $\mathcal{O}_{K,w} \otimes_{W(k_w)} W(k)$, using σ_i to embed $W(k_w)$ into $W(k)$. Then

$$\mathcal{O}_{K,w} \otimes_{W(k_w)} W(k) = \prod_{1 \in \mathbb{Z}/f\mathbb{Z}} R_{w,i}$$

gives rise to the decomposition

$$M_v = \bigoplus_{i \in \mathbb{Z}/f\mathbb{Z}} M_{v,i}$$

where $M_{v,i}$ is a free rank one module over $R_{w,i}$. We also have the corresponding decomposition of the Lie algebra:

$$\mathrm{Lie}(M_v) = \bigoplus_{i \in \mathbb{Z}/f\mathbb{Z}} \mathrm{Lie}(M_v)^i \cong \bigoplus_{i \in \mathbb{Z}/f\mathbb{Z}} k[\pi_w]/(\pi_w^{e_i})$$

for some sequence of integers $e_i \leq \mathrm{ord}_w(p) = 2e$, where π is a uniformizer of $\mathcal{O}_{K,w}$ and $e = e(K_{0,v}/\mathbb{Q}_p)$. As usual, denote the sequence (e_i) by $e(M_v)$.

As before, choose generators x_i for $M_{v,i}$ over $R_{w,i}$, and let $\theta_i \in R_{w,i}$ be such that $Vx_i = \theta_{i-1}x_{i-1}$ for all i . Once again, $\mathrm{ord}_w(\theta_i) = e_i$, and

$$\Delta(M_v) := \prod_{1 \leq i \leq f} N_{R_{w,i}/\mathcal{O}_{K,w}}(\theta_i)$$

invariant with respect to change of basis. As before, and by essentially the same proof, we obtain:

Theorem III.7. *M_v is determined up to isomorphism by $e(M_v)$ and $\Delta(M_v)$.*

Now we study the pairing, whose behavior we only need to consider on $M_{w,i} \times M_{w,i}$ – if, say, $a \in R_{w,i}$ and $y \in M_{w,j}$ for $i \neq j$, then $\langle ax_{w,i}, y \rangle = \langle x_{w,i}, \bar{a}y \rangle = 0$ since $\bar{a} \in R_{w,i}$ acts trivially on $M_{w,j}$. The pairing is determined by C_i in the inverse different $\delta_{R_{w,i}/W(k)}$ such that for all $a, b \in R_{w,i}$,

$$\langle ax_i, bx_i \rangle = \mathrm{Tr}_{R_{w,i}/W(k)}(C_i a \bar{b})$$

Since $\langle Vax_i, Vbx_i \rangle = p\sigma^{-1}\langle ax_i, bx_i \rangle$, we have, much as before, $p\sigma^{-1}(C_i) = C_{i-1}\theta_{i-1}\overline{\theta_{i-1}}$ and $\mathrm{ord}_w(C_{i-1}) - \mathrm{ord}_w(C_i) = \mathrm{ord}_w(p) - 2e_{i-1}$. In this case, we additionally have

$$\begin{aligned}
\text{Tr}_{R_{w,i}/W(k)}(C_i \bar{a} \bar{b}) &= \langle ax_i, bx_i \rangle \\
&= -\langle bx_i, ax_i \rangle \\
&= -\text{Tr}_{R_{w,i}/W(k)}(C_i \bar{a} \bar{b}) \\
&= \text{Tr}_{R_{w,i}/W(k)}(-\overline{C_i} \bar{a} \bar{b})
\end{aligned}$$

and hence $C_i = -\overline{C_i}$. Note that as before, none of these relationships are affected by any change of basis – if x_i is replaced with $t_i x_i$, then C_i is replaced with $t_i \bar{t}_i C_i$. Also, $\text{ord}_w(C_i)$ is invariant with respect to change of basis.

However, we do not have the full range of flexibility that we had in the previous two cases. That is, we are not guaranteed that if, for all i , $\text{ord}_w(D_i) = \text{ord}_w(C_i)$ and $D_i = -\overline{D_i}$, then there is a change of basis which gives $C_i = D_i$. If D_i satisfies the conditions above, then $D_i = u_i C_i$ for some unit u_i such that $\bar{u}_i = u_i$, but we are not guaranteed the existence of a t_i such that $u_i = t_i \bar{t}_i$.

Remark III.8. In each of Theorems III.4, III.6, and III.7, we prove that $\Delta(M_v)$ and $e(M_v)$ (or variants based on w and/or \bar{w} above v) determine M_v up to isomorphism. However, this is just a notationally different way of saying M_v is determined up to isomorphism by $\text{Lie}(M_v)$ and $\det_{\mathcal{O}_{K,v}}(V^f)$. Since this is true for every $v|p$, Theorem III.1 follows.

3.2 Classification up to Isogeny

In this section we sketch a proof of the following theorem towards a classification of Dieudonné modules up to isogeny. The setup and notation is the same as the previous section.

Theorem III.9. *Assume k contains k_v for all v above p . Then $\det_{\mathcal{O}_{K,p}}(V^d | \mathbb{D}(H))$ determines the \mathcal{O}_K -linear k -isogeny class of H .*

As we did in Section 3.1, we would like to consider instead H_v (and the corresponding M_v) for $v|p$, dividing into cases based on the behavior of v in K and providing a corresponding subtheorem for M_v . As the proofs in each case are nearly identical, we only present one – the one where v is split in K . It then suffices to prove (using the notation of Theorem III.4):

Theorem III.10. M_w is determined up to $\mathcal{O}_{K,w}$ -linear isogeny by $\Delta(M_w)$.

Remark III.11. The corresponding theorem for $M_{\bar{w}}$ has identical proof.

Proof. First, suppose M_w and N_w are $\mathcal{O}_{K,w}$ -linearly isogenous, with $\phi : M_w \rightarrow N_w$ an injective homomorphism arising from such an isogeny. Let $x_{w,i}$ and $y_{w,i}$ be generators for $M_{w,i}$ and $N_{w,i}$ respectively over $R_{w,i} := \mathcal{O}_{K,w} \otimes_{W(k_w)} W(k)$ (using σ_i to embed $W(k_w)$ into $W(k)$), and $\theta_{w,i}$ and $\delta_{w,i}$ such that $Vx_{w,i} = \theta_{w,i-1}x_{w,i-1}$ and $Vy_{w,i} = \delta_{w,i-1}y_{w,i-1}$. Let $a_{w,i}$ be nonzero such that $\phi(x_{w,i}) = a_{w,i}y_{w,i}$. Since ϕ commutes with V , we obtain $\sigma^{-1}(a_{w,i})\delta_{w,i-1} = \theta_{w,i-1}a_{w,i-1}$ for all i . If we take the norm of both sides, and then take the product of both sides with i ranging from 1 to f , we obtain

$$\Delta(N_w) \prod_{1 \leq i \leq f} N_{R_{w,i-1}/\mathcal{O}_{K,w}}(\sigma^{-1}(a_{w,i})) = \Delta(M_w) \prod_{1 \leq i \leq f} N_{R_{w,i}/\mathcal{O}_{K,w}}(a_{w,i})$$

Hence, $\Delta(M_w) = \Delta(N_w)$.

Now suppose $\Delta(M_w) = \Delta(N_w)$. First, note that if

$$T = \prod_{1 \leq i \leq f} \sigma^{i-f}(\delta_{w,f-i})$$

$$S = \prod_{1 \leq i \leq f} \sigma^{i-f}(\theta_{w,f-i})$$

then since $\Delta(M_w) = \Delta(N_w)$, $\text{ord}_w(T) = \text{ord}_w(S)$, so $S = u \cdot T$ for some unit u .

Further, $N_{R_{w,f}/\mathcal{O}_{K,w}}(S) = \Delta(M_w) = \Delta(N_w) = N_{R_{w,f}/\mathcal{O}_{K,w}}(T)$, so u has norm 1. Thus

there exists a unit $a \in R_{w,f}$ such that $u = \sigma^{-f}(a)/a$. Let $a_{w,f} = a \cdot b$, with $b \in W(k_w)$

(i.e., $\sigma^{-f}(b) = b$) having ord_w sufficiently large ($\text{ord}_w(S)$ will be large enough). Then we may inductively find $a_{w,i-1}$ satisfying $\sigma^{-1}(a_{w,i})\delta_{w,i-1} = \theta_{w,i-1}a_{w,i-1}$ (since the ord_w of the left hand side is always at least $\text{ord}_w(\theta_{w,i-1})$). Once done with this process, we claim:

Lemma III.12. $\sigma^{-1}(a_{w,1})\delta_{w,f} = \theta_{w,f}a_{w,f}$.

Proof. For $1 \leq j < f$, we have

$$\sigma^{-1}(a_{w,j+1})\delta_{w,j} = \theta_{w,j}a_{w,j}.$$

Applying σ^{-j} to each side of the formula and taking products yields:

$$\begin{aligned} \prod_{1 \leq j < f} \sigma^{-j-1}(a_{w,j+1}) \cdot \prod_{1 \leq j < f} \sigma^{-j}(\delta_{w,j}) &= \prod_{1 \leq j < f} \sigma^{-j}(\theta_{w,j}) \cdot \prod_{1 \leq j < f} \sigma^{-j}(a_{w,j}) \\ \sigma^{-f}(a_{w,f}) \cdot \prod_{1 \leq j < f} \sigma^{-j}(\delta_{w,j}) &= \sigma^{-1}(a_{w,1}) \cdot \prod_{1 \leq j < f} \sigma^{-j}(\theta_{w,j}) \\ \sigma^{-f}(a_{w,f}) \cdot T \cdot \theta_{w,f} &= \sigma^{-1}(a_{w,1}) \cdot S \cdot \delta_{w,f} \\ \sigma^{-f}(a_{w,f}) \cdot T \cdot \theta_{w,f} &= \sigma^{-1}(a_{w,1}) \cdot (T \cdot \sigma^{-f}(a_{w,f})/a_{w,f}) \cdot \delta_{w,f} \\ \theta_{w,f} &= \sigma^{-1}(a_{w,1})/a_{w,f} \cdot \delta_{w,f} \end{aligned}$$

with the third line following from the second by multiplying both sides of the equation by $\theta_{w,f} \cdot \delta_{w,f}$. The final line implies the desired result. \square

As a corollary to the lemma, $x_{w,i} \mapsto a_{w,i}y_{w,i}$ is an injective homomorphism which commutes with V , since for all i ,

$$V(a_{w,i}y_{w,i}) = \sigma^{-1}(a_{w,i})\delta_{w,i-1}y_{w,i-1} = a_{w,i-1}\theta_{w,i-1}x_{w,i-1} = a_{w,i-1}V(x_i).$$

It follows by an argument similar to one employed within Lemma 2.4 of [1] that $x_{w,i} \mapsto a_{w,i}y_{w,i}$ also commutes with F and is therefore an isogeny of Dieudonné modules. \square

BIBLIOGRAPHY

BIBLIOGRAPHY

- [1] Jeffrey D. Achter and Peter Norman. Local monodromy of p -divisible groups. *Transactions of the American Mathematical Society*, 362:985–1007, 2010.
- [2] Ching-Li Chai, Brian Conrad, and Frans Oort. CM lifting of abelian varieties. To appear, 2009.
- [3] Ching-Li Chai, Brian Conrad, and Frans Oort. CM-lifting of abelian varieties up to isogeny. To appear, 2009.
- [4] Ching-Li Chai and Frans Oort. Moduli of abelian varieties and p -divisible groups. Informal notes, 2006.
- [5] Brian Conrad. Algebraic theory of complex multiplication. Intended chapter for book, 2005.
- [6] M. Demazure. *Lectures on p -divisible groups*. Springer-Verlag, Berlin, 1972.
- [7] Jean-Marc Fontaine. Groupes p -divisibles sur les corps locaux. *Astérisque*, 47–48, 1977.
- [8] Alexander Grothendieck and Jean Dieudonné. Elements des géometrie algébrique III. *Publications Mathématiques IHES*, 28, 1966.
- [9] Taira Honda. Isogeny classes of abelian varieties over finite fields. *Journal of the Mathematical Society of Japan*, 20:83–95, 1968.
- [10] Robert E. Kottwitz. Points on some Shimura varieties over finite fields. *Journal of the American Mathematical Society*, 5:373–444, 1992.
- [11] Yuri Ivanovich Manin. Theory of commutative formal groups over fields of finite characteristic. *Uspekhi Mat. Nauk*, 18:3–90, 1963.
- [12] William Messing. *The Crystals Associated to Barsotti-Tate Groups: with applications to abelian schemes*. Springer-Verlag Berlin, 1972.
- [13] J. S. Milne. Complex multiplication. Informal notes, 2006.
- [14] David Mumford. *Abelian Varieties*. Oxford University Press, 1970.
- [15] Jürgen Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1992.
- [16] Tadao Oda and Frans Oort. Supersingular abelian varieties. In *Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977)*, pages 595–621. Kinokuniya Book Store, 1978.
- [17] Frans Oort. CM-liftings of abelian varieties. *Journal of Algebraic Geometry*, 1:131–146, 1992.
- [18] Jean-Pierre Serre and John Tate. Mimeographed notes from the 1964 AMS Summer Institute in Algebraic Geometry at Woods Hole.

- [19] John Tate. Endomorphisms of abelian varieties over finite fields. *Investiones Mathematicae*, 2, 1966.
- [20] John Tate. Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T. Honda). *Séminaires Bourbaki*, 21, 1968–69.