5-2012

Local Torsion on Abelian Surfaces

Adam Gamzon
University of Massachusetts Amherst

LOCAL TORSION ON ABELIAN SURFACES

A Dissertation Presented

by

ADAM B. GAMZON

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2012

Department of Mathematics and Statistics

LOCAL TORSION ON ABELIAN SURFACES

A Dissertation Presented

by

ADAM B. GAMZON

Approved as to style and content by:

Tom Weston, Chair

Paul Gunnells, Member

Siman Wong, Member

David Barrington, Outside Member

Michael Lavine, Department Head
Mathematics and Statistics

DEDICATION

In memory of Sandy Gamzon and Michael Weston.

Two inspirational people who changed this world for the better.

ACKNOWLEDGEMENTS

Many thanks to Tom Weston for suggesting this problem and helping me see this dissertation to fruition. I would also like to thank Jenia Tevelev and Siman Wong for several useful discussions as well as Brian Conrad for suggesting that I learn about smooth Honda systems. Last but not least, I owe a debt of gratitude to my wife, Allison Gamzon, for her support and encouragement throughout all the difficult times.

ABSTRACT

LOCAL TORSION ON ABELIAN SURFACES

MAY 2012

ADAM B. GAMZON, B.A., UNIVERSITY OF CONNECTICUT

M.S., UNIVERSITY OF MASSACHUSETTS AMHERST

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Tom Weston

Fix an integer $d > 0$. In 2008, Chantal David and Tom Weston showed that, on average, an elliptic curve over $\mathbf{Q}$ picks up a nontrivial p-torsion point defined over a finite extension K of the p-adics of degree at most d for only finitely many primes p. This dissertation is an extension of that work, investigating the frequency with which a principally polarized abelian surface A over $\mathbf{Q}$ with real multiplication by $\mathbf{Q}(\sqrt{5})$ has a nontrivial p-torsion point defined over K. Averaging by height, the main result shows that A picks up a nontrivial p-torsion point over K for only finitely many p.

The proof of our main theorem primarily rests on three lemmas. The first lemma uses the reduction-exact sequence of an abelian surface defined over an unramified extension K of $\mathbf{Q}_p$ to give a mod p^2 condition for detecting when A has a nontrivial p-torsion point defined over K. The second lemma employs crystalline Dieudonné theory to count the number of isomorphism classes of lifts of abelian surfaces over $\mathbf{F}_p$ to $\mathbf{Z}/p^2$ that satisfy the condition from our first lemma. Finally, the third lemma addresses the issue of the assumption in the first lemma that K is an unramified extension of $\mathbf{Q}_p$. Specifically, it shows that if A has a nontrivial p-torsion point over a ramified extension K of $\mathbf{Q}_p$

and $p-1 > d$ then this p-torsion point is actually defined over the maximal unramified subextension of K. We then combine these algebraic results to reduce the main analytic calculation to a series of straightforward estimates.

TABLE OF CONTENTS

LIST OF TABLES

C H A P T E R 1

INTRODUCTION

Let A be an abelian variety over $\mathbf{Q}$ without complex multiplication. The goal of this thesis is to address the following conjecture.

Conjecture 1.1 (David, Weston) *Fix an integer $d \geq 1$. Then there are finitely many primes p such that $A(K)[p] \neq 0$ where K is a finite extension of $\mathbf{Q}_p$ of degree at most d.*

More specifically, we prove that this conjecture holds on average for abelian surfaces with real multiplication by $\mathbf{Q}(\sqrt{5})$. Indeed, [20] shows that the fine moduli space, $X(\mathbf{Q})$, for principally polarized abelian surfaces over $\mathbf{Q}$ with real multiplication by $\mathbf{Q}(\sqrt{5})$ is a double cover of $\mathbf{P}^2(\mathbf{Q})$ (ramified over a rational curve of degree 10). This essentially means that pairs of such abelian surfaces are parameterized by points in $\mathbf{P}^2(\mathbf{Q})$. It turns out that one of the abelian surfaces in a fiber of this map has a p-torsion point if and only if the other one does. Let $[a : b : c]$ be homogeneous coordinates on $\mathbf{P}^2$, let $A_{[a:b:c]}$ be any abelian surface in the fiber over $[a : b : c]$, and let

$$\pi^d_{[a:b:c]}(x) = \#\{p \leq x : A_{[a:b:c]}(K)[p] \neq 0 \text{ and } [K : \mathbf{Q}_p] \leq d\}.$$

Furthermore, we can assume that, after scaling, $a, b, c \in \mathbf{Z}$ and $\gcd(a, b, c) = 1$. Define a height function H on $\mathbf{P}^2(\mathbf{Q})$ by $H([a : b : c]) = \max\{|a|, |b|, |c|\}$. Then the following theorem is our main result.

Theorem 1.2 *Let* $S_M = \{[a:b:c] \in \mathbf{P}^2(\mathbf{Q}) : H([a:b:c]) \leq M\}$. *If* $M \geq x^{4/3+\varepsilon}$ *for some* $\varepsilon > 0$ *then*

$$\frac{1}{\#S_M} \sum_{[a:b:c] \in S_M} \pi^d_{[a:b:c]}(x) \ll d \quad as \quad x \to \infty.$$

The motivation for Conjecture 1.1 and Theorem 1.2 stem from results on elliptic curves and from a conjecture of Barry Mazur regarding the deformation theory of Galois representations. In [8], Chantal David and Tom Weston prove an analogous statement to Theorem 1.2 in the case of elliptic curves. Let $S_{A,B}$ be the set of all elliptic curves of the form $y^2 = x^3 + ax + b$ where $a \leq A, b \leq B$ and $\pi^d_E(x)$ be the number of primes $p \leq x$ such that E has a nontrivial p-torsion point over a finite extension of $\mathbf{Q}_p$ of degree at most d.

Theorem 1.3 (David, Weston) *Fix* $d \geq 1$. *Assume* $A, B \geq x^{7/4+\varepsilon}$ *for some* $\varepsilon > 0$. *Then*

$$\frac{1}{\#S_{A,B}} \sum_{E \in S_{A,B}} \pi^d_E(x) \ll d^2 \quad as \quad x \to \infty.$$

Furthermore, as summarized in the following table, they computed $\pi^1_E(10^6)$ for the 5113 isomorphism classes of elliptic curves over $\mathbf{Q}$ with conductor at most 1000 using the Magma Computational Algebra System.

Table 1. Local Torsion Primes on Curves of Small Conductor

Curves	# curves	$\#E$ such that $\pi^1_E(10^6) =$					
		0	1	2	3	4	5+
All curves	5113	568	3687	828	15	1	14
Curves with no torsion	1364	484	733	117	15	1	14

The 14 curves with $\pi^1_E(10^6) \geq 5$ all have complex multiplication. In fact, they all have between 22 and 36 primes less than 10^6 such that E possesses a nontrivial p-torsion point over $\mathbf{Q}_p$. Furthermore, most (99.1%) of the primes that occurred were 2, 3, 5, or 7, with only 2 curves possessing such a p-torsion point with $p > 1000$. Although the precise ratios that these calculations yielded should be taken lightly, it is quite clear that this data and Theorem 1.3 support Conjecture 1.1.

Theorems 1.2 and 1.3 relate to the deformation theory of Galois representations via a conjecture of Mazur and subsequent work on this conjecture by Weston. Pick any newform $f = \sum a_n q^n$ of level N and weight $k \geq 2$. Set $K_f = \mathbf{Q}(\{a_n\})$. It is well known that this is a number field. Let $\mathfrak{p}$ be any prime of the ring of integers $\mathcal{O}_{K_f}$ lying over a prime $p \in \mathbf{Z}$. Deligne constructed a (semi-simple) mod $\mathfrak{p}$ representation

$$\overline{\rho}_{f,\mathfrak{p}} : \mathrm{Gal}(\mathbf{Q}_{S\cup\{p\}}/\mathbf{Q}) \to \mathrm{GL}_2(k_{f,\mathfrak{p}})$$

where S is a finite set of primes dividing N, $\mathbf{Q}_{S\cup\{p\}}$ is the maximal algebraic extension of $\mathbf{Q}$ unramified outside of $S \cup \{p\}$, and $k_{f,\mathfrak{p}}$ is the residue field $\mathcal{O}_{K_f}/\mathfrak{p}$. A deformation of $\overline{\rho}_{f,\mathfrak{p}}$ is an equivalence class of lifts of $\overline{\rho}_{f,\mathfrak{p}}$ to a representation,

$$\rho : \mathrm{Gal}(\mathbf{Q}_{S\cup\{p\}}/\mathbf{Q}) \to \mathrm{GL}_2(R),$$

where R is a complete noetherian local ring with residue field $k_{f,\mathfrak{p}}$. Two such lifts are equivalent if they are equal up to conjugation by an element in the kernel of the natural reduction map $\mathrm{GL}_2(R) \to \mathrm{GL}_2(k_{f,\mathfrak{p}})$.

It is known that $\overline{\rho}_{f,\mathfrak{p}}$ is absolutely irreducible for almost all $\mathfrak{p}$ (see lemma 7.13 in [11]). For such $\mathfrak{p}$, there is a *universal deformation ring*, $R^{\mathrm{univ}}_{f,\mathfrak{p}}$, which parameterizes deformations of $\overline{\rho}_{f,\mathfrak{p}}$ to such local rings R. That is, there is a universal deformation

$$\rho^{\mathrm{univ}}_{f,\mathfrak{p}} : \mathrm{Gal}(\mathbf{Q}_{S\cup\{p\}}/\mathbf{Q}) \to \mathrm{GL}_2(R^{\mathrm{univ}}_{f,\mathfrak{p}})$$

in the category of inverse limits of artinian local rings with residue field $k_{f,\mathfrak{p}}$, so that any deformation ρ of $\overline{\rho}_{f,\mathfrak{p}}$ comes from $\rho^{\mathrm{univ}}_{f,\mathfrak{p}}$ by composition with a unique map $R^{\mathrm{univ}}_{f,\mathfrak{p}} \to R$.

It is also known that $R^{\mathrm{univ}}_{f,\mathfrak{p}}$ is a quotient of a power series ring in

$$d_1 := \dim H^1(\mathrm{Gal}(\mathbf{Q}_{S\cup\{p\}}/\mathbf{Q}), \mathrm{ad}\,\overline{\rho}_{f,\mathfrak{p}})$$

variables over the ring of Witt vectors, denoted $W(k_{f,\mathfrak{p}})$, by an ideal generated by at most

$$d_2 := \dim H^2(\mathrm{Gal}(\mathbf{Q}_{S\cup\{p\}}/\mathbf{Q}), \mathrm{ad}\,\overline{\rho}_{f,\mathfrak{p}})$$

elements. It is a standard fact that $d_1 - d_2 \geq 3$ and that $d_1 = 3$ if $d_2 = 0$ (see [14] or [21] for example). We say that the deformation theory of $\overline{\rho}_{f,\mathfrak{p}}$ is *unobstructed* if $d_2 = 0$. Therefore, when the deformation theory of $\overline{\rho}_{f,\mathfrak{p}}$ is unobstructed, $R^{\text{univ}}_{f,\mathfrak{p}} \cong W(k_{f,\mathfrak{p}})[[x_1, x_2, x_3]]$.

In [22], Mazur conjectured that the deformation theory of the mod $\mathfrak{p}$ Galois representation $\overline{\rho}_{f,\mathfrak{p}}$ attached to a modular form f is unobstructed for all but finitely many $\mathfrak{p}$ when f has weight 2. Furthermore, it is known that the analogous statement when f has higher weight is true (see [36]). If we assume that K_f is totally real then the abelian variety A_f associated to f has dimension $[K_f : \mathbf{Q}]$ and admits an action of $\mathcal{O}_{K_f}$ (i.e., the ring of integers $\mathcal{O}_{K_f} \hookrightarrow \text{End}(A_f)$). Weston has shown [35] that if $K_f = \mathbf{Q}$ (that is, A_f is an elliptic curve) then Mazur's conjecture holds when f has weight 2 if there are only finitely many primes p such that $A_f(L)[p] \neq 0$ where L is the unramified quadratic extension of $\mathbf{Q}_p$. Furthermore, when $[K_f : \mathbf{Q}] > 1$ (that is, when A_f is a higher dimension abelian variety) the same statement should still be true, but the proof still requires some work. Thus, assuming K_f is totally real, Conjecture 1.1 should imply that the deformation theory of $\overline{\rho}_{f,\mathfrak{p}}$ is unobstructed for almost all $\mathfrak{p}$.

Seen in this light, David and Weston's result on elliptic curves corresponds to the case $K_f = \mathbf{Q}$ in Mazur's conjecture whereas my result for abelian surfaces with real multiplication by $\mathbf{Q}(\sqrt{5})$ corresponds to the $K_f = \mathbf{Q}(\sqrt{5})$ case of Mazur's conjecture. Thus, combining the two results, gives a good indication that Mazur's conjecture is in fact true when K_f is either $\mathbf{Q}$ or $\mathbf{Q}(\sqrt{5})$.

The outline of this dissertation is as follows. Chapter 2 lays out the necessary details of Crystalline Dieudonné theory to carry out our calculations of isomorphism classes of lifts of Barsotti-Tate groups over a finite field k to $W(k)/p^2$. Chapter 3 discusses ℓ-adic Galois representation attached to abelian varieties. In particular, we focus on describing the determinant of such representations as well as their image for abelian surfaces with real multiplication. Chapter 4 contains all of our algebraic results, which regard detecting nontrivial p-torsion over an unramified p-adic field as well as counting the number of

abelian surfaces over $W(k)/p^2$ with "elevated p-rank". We also show that for p large enough, if an abelian surface over $\mathbf{Q}$ has a nontrivial p-torsion point over a p-adic field K then it has a nontrivial p-torsion point defined over the maximal unramified subfield of K. In Chapter 5, we review Manoharmayum's result on the moduli space of principally polarized abelian surfaces with real multiplication by $\mathbf{Q}(\sqrt{5})$ and a level-$\sqrt{5}$ structure. The main result of Chapter 6 is the proof of Theorem 1.2. Finally, the appendix discusses an alternate theory we could have employed to carry out our counting results of Chapter 4.

CHAPTER 2

CRYSTALLINE DIEUDONNÉ THEORY

Let k be a finite field of characteristic p, let $W := W(k)$ be the ring of Witt vectors over k and let K be the field of fractions of W.

One of our principal algebraic results regards counting the number of isomorphism classes of lifts of the p-divisible group of an abelian variety over k to $W_2 := W/p^2$. To do this one can either make use of crystalline Dieudonné theory or of smooth Honda systems (see the appendix). Crystalline Dieudonné theory sets up an equivalence between Barsotti-Tate groups over W_2 and some "linear algebraic" objects. It turns out that crystalline Dieudonné theory is ideally suited to our purposes.

We begin with a brief review of the classification of Barsotti-Tate groups over k by Dieudonné-modules. One can think of the classical theory of complex Lie groups and Lie algebras, which (often) creates a dictionary between problems on Lie groups and linear algebra data coming from Lie algebras as the meta-idea motivating the construction. The main reference for this material is [13], but [6] is a good introduction to the theory and [28] gives an accessible overview of the more general setting.

Definition 2.1 *A* Barsotti-Tate group G *over a scheme* S *is a group scheme such that*

- $G = \varinjlim G[p^n]$ *where* $G[p^n]$ *is the kernel of multiplication by* p^n*,*
- *multiplication by* p *is an epimorphism on* G*,*
- $G[p]$ *is a finite, locally-free group scheme.*

Remark 2.2 *The main examples of Barsotti-Tate groups we will be interested in are those associated to abelian schemes over* $S = \operatorname{Spec} k$. *Namely,* $A[p^\infty] := \varinjlim A[p^n]$, $\mathbf{Q}_p/\mathbf{Z}_p := \varinjlim \mathbf{Z}/p^n\mathbf{Z}$ *and* $\mu_{p^\infty} := \varinjlim \mu_{p^n}$. *For this reason, our discussion of crystalline Dieudonné theory is somewhat simplified, but the results are true in a much more general setting.*

Remark 2.3 *Since* $G[p]$ *is a finite, locally free group scheme, it follows that the order of* $G[p]$ *is of the form* p^h *where* h *is a locally constant function on* S *with values in* $\mathbf{N}$ *and, moreover,* $G[p^n]$ *has order* p^{nh}. *In the case that* $S = \operatorname{Spec} k$, *the function* h *is constant and we call it the* height *of* G, *denoted* $\operatorname{ht}(G)$.

Let σ denote the automorphism on W (and K) that extends the Frobenius automorphism $x \mapsto x^p$ on k. Define the Dieudonné ring to be

$$D_k = W[F, V]/(FV - p)$$

where F (for Frobenius) and V (for Verschiebung) satisfy $F\alpha = \alpha^\sigma F$ and $V\alpha = \alpha^{\sigma^{-1}} V$ for all $\alpha \in W$. We call a D_k-module a *Dieudonné* module. One can associate to each Barsotti-Tate group G over $\operatorname{Spec} k$ the D_k-module $\mathcal{M}(G) := \operatorname{Hom}(G, \widehat{CW}_k)$ where $\widehat{CW}_k$ denotes the formal affine commutative k-group scheme representing the Witt covector k-group functor CW_k and the F and V action come from their action on the functor CW_k (see the appendix for more on Witt covectors). This gives an antiequivalence of categories.

Theorem 2.4 *The functor* $G \rightsquigarrow \mathcal{M}(G)$ *is an antiequivalence of categories between Barsotti-Tate groups over* k *and* D_k*-modules that are free* W*-modules of rank* $\operatorname{ht}(G)$.

Proof. See [13]. ◇

Remark 2.5 *A free* W*-module* M *of finite rank with an injective* σ*-linear endomorphism* F *such that* $pM \subset FM$ *is sometimes called an* F-crystal *over* k. *Note that in this case,*

F is bijective on the vector space $M \otimes_W K$, so we define $V := pF^{-1}$. One can check that M is stable under the action of V.

The dictionary given by Theorem 2.4 between group schemes and linear algebra also successfully translates many group-scheme theoretic concepts into the Dieudonné module world.

Theorem 2.6 *Let G be a Barsotti-Tate group over k and let $\mathcal{M}(G)$ be as before. Then G is étale if and only if F is injective on $\mathcal{M}(G)$ and G is connected if and only if the action of F is topologically nilpotent. Define $\mathcal{M}(G)^* = \mathrm{Hom}_W(\mathcal{M}(G), K/W)$ and let F and V act as duals to the actions of V and F on $\mathcal{M}(G)$ respectively. This gives $\mathcal{M}(G)^*$ the structure of a D_k-module and, moreover, there is a natural isomorphism of D_k-modules*

$$\varphi_G : \mathcal{M}(G^*) \to \mathcal{M}(G)^*$$

where G^* is the Serre dual of G.

Proof. Again, see [13]. ◇

We illustrate these ideas with an example that also mimics the computations that play an integral role in our algebraic results.

Example 2.7 *Let E be an ordinary elliptic curve over k. We show that the Barsotti-Tate group $E[p^\infty] \cong \mathbf{Q}_p/\mathbf{Z}_p(\chi) \times \mu_{p^\infty}(\chi^{-1})$ where χ is a character $\mathrm{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p) \to \mathbf{Z}_p^\times$. Indeed, one can argue using Cartier duality that the connected-étale exact sequence for $E[p^n]$ is*

$$0 \to \mu_{p^n}(\chi^{-1}) \to E[p^n] \to \mathbf{Z}/p^n\mathbf{Z}(\chi) \to 0,$$

so in the limit we also have an exact sequence

$$0 \to \mu_{p^\infty}(\chi^{-1}) \to E[p^\infty] \to \mathbf{Q}_p/\mathbf{Z}_p(\chi) \to 0.$$

Thus one way of showing that $E[p^\infty] \cong \mu_{p^\infty}(\chi^{-1}) \times \mathbf{Q}_p/\mathbf{Z}_p(\chi)$ is by proving that

$$\mathrm{Ext}^1_k(\mathbf{Q}_p/\mathbf{Z}_p(\chi), \mu_{p^\infty}(\chi^{-1})) = 0.$$

To do this, apply $\mathcal{M}$ to the exact sequence of Barsotti-Tate groups to obtain an exact sequence of D_k-modules

$$0 \to \mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p(\chi)) \to \mathcal{M}(E[p^\infty]) \to \mathcal{M}(\mu_{p^\infty}(\chi^{-1}) \to 0,$$

reducing our problem to computing extensions of D_k-modules.

As W-modules, $\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p(\chi)) = We_1$ and $\mathcal{M}(\mu_{p^\infty}(\chi^{-1}) = W\overline{e_2}$. Let e_2 be any lift of $\overline{e_2}$ to $\mathcal{M}(E[p^\infty])$ and, abusing notation, let $\langle e_1 \rangle$ also denote the image of the module $\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p(\chi))$ in $\mathcal{M}(E[p^\infty])$. Then noting that $\mathcal{M}(E[p^\infty])$ is a free W-module of rank 2, we see that $\mathcal{M}(E[p^\infty]) = We_1 \oplus We_2$. Also, we know that F acts as an automorphism on $\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p(\chi))$ since $\mathbf{Q}_p/\mathbf{Z}_p$ is étale and, similarly, V acts as an automorphism on $\mathcal{M}(\mu_{p^\infty}(\chi^{-1}))$ since μ_{p^∞} is connected. Using this and the fact that $FV = VF = p$, we can describe the action of F and V as matrices:

$$F = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, V = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}, \text{ and } FV = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$$

for some a, c' in $W^\times$ and some a', b', b, c in W. Therefore, $a' = pa^{-1}$, $c = pc'^{-1}$ and $ab' + c'b = 0$. We can inductively normalize this basis so that in the limit we get a basis such that $F(e_1) = ae_1$ and $F(e_2) = ce_2$. Thus using the normalized basis, we now have $b = 0$, which forces $b' = 0$. So the only extension of $\mathcal{M}(\mu_{p^\infty}(\chi^{-1}))$ by $\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p(\chi))$ is the trivial extension.

The establishment of a crystalline Dieudonné theory for Barsotti-Tate groups is essentially due to five people: Berthelot [3],[4], Breen [3], Grothendieck [15], [16], Messing [3], [4], [23], [24] and Mazur [23]. The main result of interest to us is about deformations of a Barsotti-Tate group over Spec k to a Barsotti-Tate group over Spec W_2. To define the Grothendieck-Messing crystals, we first need divided powers and a notion of a crystalline site.

Definition 2.8 *Let A be a ring and I an ideal of A. Call the pair (I, γ)* an ideal with

divided powers *if γ is a family of maps $\gamma_n : I \to I$, $n \geq 1$ such that for all $x, y \in I$ and $\lambda \in A$:*

- $\gamma_1(x) = x$,
- $\gamma_n(\lambda x) = \lambda^n \gamma_n(x)$,
- $\gamma_n(x)\gamma_m(x) = \frac{(m+n)!}{m!n!}\gamma_{n+m}(x)$,
- $\gamma_n(x+y) = \gamma_n(x) + \sum_{i=1}^{n-1} \gamma_{n-i}(x)\gamma_i(y) + \gamma_n(y)$,
- $\gamma_m(\gamma_n(x)) = \frac{(mn)!}{(n!)^m m!}\gamma_{mn}(x)$.

By convention, define γ_0 by $\gamma_0(x) = 1$ for all $x \in I$.

Definition 2.9 *Given an ideal with divided powers (I, γ), the divided powers are* nilpotent *if there is an N such that the ideal generated by elements of the form $\gamma_{i_1}(x_1) \cdots \gamma_{i_k}(x_k)$ where $i_1 + \cdots + i_k \geq N$ is zero. In particular, this condition implies that $I^N = 0$ (by taking $k = N$ and $i_1 = \cdots = i_N = 1$).*

Example 2.10 *Let $p \geq 3$. Take $A = W/p^n W$ and $I = pW/p^n W$. Let $m \geq 1$. It is well known that the p-adic valuation of $m!$ is bounded:*

$$\mathrm{ord}_p(m!) \leq \frac{(m-1)\,\mathrm{ord}_p(p)}{p-1} < m - 1$$

(see [32] for example). Define $\gamma_m(p) = p^m/m! \in I$ and extend γ_m to all of A so that it satisfies conditions 1 - 4 of Definition 2.8. Then (I, γ) is an ideal with nilpotent divided powers.

Definition 2.11 *For a scheme X, its* crystalline site*, denoted* $\mathrm{Crys}(X/S)$*, is the category whose objects are triples $(U \hookrightarrow T, \gamma)$ such that:*

- *U is a Zariski open subscheme of X,*
- *$U \hookrightarrow T$ is a locally nilpotent immersion,*

- $\gamma = (\gamma_n)$ *are locally nilpotent divided powers on the defining ideal* I *of* U *in* T.

The morphisms from $(U \hookrightarrow T, \gamma)$ *to* $(U' \hookrightarrow T', \gamma')$ *are the commutative diagrams*

$$\begin{array}{ccc} U & \longrightarrow & T \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \overline{f}} \\ U' & \longrightarrow & T' \end{array}$$

such that $f : U \to U'$ *is the inclusion and* $\overline{f} : T \to T'$ *is a divided powers morphism (meaning, the sheaf of rings morphism* $\overline{f}^{-1}(\mathcal{O}_{T'}) \to \mathcal{O}_T$ *is a divided powers morphism).*

Remark 2.12 *To be completely accurate, one should define the crystalline site with regard to a base scheme and should impose a compatibility condition on the divided powers (see [27], for example). For our purposes, though this will suffice.*

Define a Grothendieck topology on this site via a pre-topology where

$$(U_i \hookrightarrow T_i, \gamma_i) \to (U \hookrightarrow T, \gamma)$$

is a covering family when each T_i is the open sub-scheme of T such that $U_i = U \times_T T_i$ and $\cup U_i = U$ (or, equivalently, $\cup T_i = T$). To define a sheaf on $\mathrm{Crys}(X)$, it suffices to give an ordinary sheaf $F_{(U \hookrightarrow T, \gamma)}$ for each object $(U \hookrightarrow T, \gamma)$ of $\mathrm{Crys}(X)$ along with morphisms $\overline{f}^{-1}(F_{(U' \hookrightarrow T', \gamma')}) \to F_{(U \hookrightarrow T, \gamma)}$ for each morphism $(U \hookrightarrow T, \gamma) \to (U' \hookrightarrow T', \gamma')$. Moreover, the maps $\overline{f}^{-1}$ should satisfy an obvious transitivity condition for morphisms

$$(U \hookrightarrow T, \gamma) \to (U' \hookrightarrow T', \gamma') \to (U'' \hookrightarrow T'', \gamma'')$$

as well as the condition that if T is the open subscheme of T' such that $U = U' \times_{T'} T$ then the morphism $\overline{f}^{-1}(F_{(U' \hookrightarrow T', \gamma')}) \to F_{(U \hookrightarrow T, \gamma)}$ is an isomorphism.

As an example, note that we have a sheaf of rings on $\mathrm{Crys}(X)$ defined by the system $\mathcal{O}_{(U \hookrightarrow T, \gamma)} = \mathcal{O}_T$. We call this the *structure sheaf* and denote it by $\mathcal{O}_{X_{\mathrm{Crys}}}$.

Definition 2.13 *A* crystal in modules *is a sheaf* F *of* $\mathcal{O}_{X_{\mathrm{Crys}}}$*-modules such that all maps* $f^* F_{(U' \hookrightarrow T', \gamma')} \to F_{(U \hookrightarrow T, \gamma)}$ *are isomorphisms for all maps* $\overline{f} : (U \hookrightarrow T, \gamma) \to (U' \hookrightarrow T', \gamma)$ *of* $\mathrm{Crys}(X)$*. Here* f^* *is the module pullback; i.e.,* $\overline{f}^{-1}$ *tensored with the structure sheaf.*

Example 2.14 *The structure sheaf $\mathcal{O}_{X_{\mathrm{Crys}}}$ is a crystal in modules.*

Parallel to the Dieudonné module situation and Barsotti-Tate groups over k, one can associate to each Barsotti-Tate group G over a scheme S where p is locally nilpotent, a locally free crystal in modules $\mathbf{D}(G)$. Following Messing [24], one first constructs a "universal extension" $E(G)$ of G by $\underline{\omega}_{G^\vee}$ where $\underline{\omega}_{G^\vee}$ is the module of invariant differentials of the Serre dual $G^\vee$ of G. He then "crystalizes" it using the method of "exponentials" to get a crystal in groups $\mathbf{E}(G)$. The contravariant functor $G \rightsquigarrow \mathbf{D}(G)$ comes from taking the Lie algebra of $\mathbf{E}(G^\vee)$.

Remark 2.15 *In [24], Messing constructs the covariant Dieudonné crystal which is canonically isomorphic to the contravariant Dieudonné crystal via the Serre dual as we hinted at above. We chose to work with the contravariant functor because of the analogy with Fontaine's functor. For more details about the relations between the different Dieudonné theories, see [5].*

Definition 2.16 *Let S be a scheme where p is nilpotent, $S \hookrightarrow S'$ be an object of* $\mathrm{Crys}(S)$*, and G' be a Barsotti-Tate group over S'. Denote by $CF(S')$ the category of pairs (G, V) where G is a Barsotti-Tate group over S and V is a locally direct factor of $\mathbf{D}(G)_{S \hookrightarrow S'}$ such that V reduces to $\underline{\omega}_G \subset \mathbf{D}(G)_{S \hookrightarrow S}$ on S.*

Theorem 2.17 *The functor $G' \rightsquigarrow (G, V)$ is an anti-equivalence of categories between Barsotti-Tate groups over S' and $CF(S')$.*

The last section of [23] discusses how we recover the usual Dieudonné module correspondence when $S = \operatorname{Spec} k$. That is, for $p \geq 3$, let $S = \operatorname{Spec} k \hookrightarrow \operatorname{Spec} W/p^n W =: S_n$ be the nilpotent immersion coming from the ring homomorphism $W/p^n W \to W/pW = k$ with divided powers as in Example 2.10. Then

$$\mathcal{M}(G) = \varprojlim \mathbf{D}(G)_{S \hookrightarrow S_n}.$$

In particular, $\mathcal{M}(G) \otimes W/p^n = \mathbf{D}(G)_{S \hookrightarrow S_n}$, so from this we have the following special case of Theorem 2.17 that we use in Chapter 4.

Corollary 2.18 *Let G be a Barsotti-Tate group over k and let $L = \underline{\omega}_G \subset \mathcal{M}(G) \otimes k$. Then the pairs $(\mathcal{M}(G) \otimes k, L')$ classify deformations of G to a Barsotti-Tate group over W_2, where $L' \subset \mathcal{M}(G) \otimes W_2$ is a W_2-submodule that is a direct summand and $L' \otimes k \cong L$.*

As an example of Corollary 2.18, we show that there are unique lifts of $(\mathbf{Q}_p/\mathbf{Z}_p)^2$ over k and of its Serre dual $(\mu_{p^\infty})^2$ over k to Barsotti-Tate groups over W_2 respectively.

Lemma 2.19 *There is a unique lift of $(\mathbf{Q}_p/\mathbf{Z}_p)^2$ over k to a Barsotti-Tate group over W_2.*

Proof. Note that $(\mathbf{Z}/p^n\mathbf{Z})^2$ is étale for all n, so the sheaf of relative differentials of $(\mathbf{Z}/p^n\mathbf{Z})^2$ over k is zero for all n. Thus, in the limit, $L = 0$ too. Since L' must be a direct summand of $\mathcal{M}(G) \otimes W/p^2W$ and $L' \otimes k = L$, this implies that $L' = 0$. $\diamond$

Lemma 2.20 *There is a unique lift of $\mu_{p^\infty}^2$ over k to a Barsotti-Tate group over W_2.*

Proof. In this case, note that $\mathrm{Lie}(G)$ is the dual of the sheaf of relative differentials, so $\underline{\omega}_{\mu_{p^\infty}} = \mathrm{Lie}(\mu_{p^\infty}^2)^\vee$ is two-dimensional. That is, $L = \mathcal{M}(G) \otimes k$, so $L' = \mathcal{M}(G) \otimes W/p^2W$. $\diamond$

Finally, we state here for later use the Serre-Tate lifting theorem, which Messing [24] showed is a consequence of Theorem 2.17.

Theorem 2.21 (Serre-Tate Lifting) *Let $S = \operatorname{Spec} R$ be a scheme with p nilpotent on it and let I be a nilpotent ideal of R. There is a functor $A \mapsto (A \times_S S_0, A[p^\infty])$ where A is an abelian scheme over S, and $S_0 = \operatorname{Spec} R/I$. Moreover, this functor is an equivalence of categories between abelian schemes over S and the category of pairs (A_0, G) where A_0 is an abelian scheme over S_0 and G is a Barsotti-Tate group lifting $A_0[p^\infty]$.*

Thus, thanks to Serre-Tate lifting, deforming an abelian surface A over k to W/p^2W is equivalent to deforming $A[p^\infty]$ to a Barsotti-Tate group over W/p^2W. Moreover, such deformations are parameterized as in Corollary 2.18.

CHAPTER 3

GALOIS REPRESENTATIONS

Let A be an abelian surface over a number field K. Assume that A has (maximal) real multiplication by a real quadratic extension F of $\mathbf{Q}$. That is, assume there is a homomorphism $i : \mathfrak{o}_F \hookrightarrow \mathrm{End}_K(A)$ where $\mathfrak{o}_F$ is the ring of integers of F. We call a prime ideal λ in $\mathfrak{o}_F$ a prime of F and let F_λ denote the λ-adic completion of F. Finally, let $G = \mathrm{Gal}(\overline{K}/K)$.

Definition 3.1 *A λ-adic representation of G on a finite dimensional F_λ vector space V is a continuous homomorphism*

$$\rho : G \to \mathrm{Aut}(V).$$

The representations of interest to us are the ones attached the ℓ-adic Tate module of A.

Definition 3.2 *The* ℓ-adic Tate module *of A is*

$$T_\ell(A) := \varprojlim A[\ell^n].$$

Let $V_\ell := T_\ell(A) \otimes \mathbf{Q}$. It well known that $T_\ell(A)$ is a free $\mathbf{Z}_\ell$-module of rank 4 and, hence, V_ℓ is a 4-dimensional $\mathbf{Q}_\ell$ vector space. Moreover, G acts continuously on $A[\ell^n]$ for all n and this action commutes with multiplication by ℓ, so we get an ℓ-adic representation

$$\rho_\ell : G \to \mathrm{Aut}(T_\ell(A)) \subset \mathrm{Aut}(V_\ell).$$

In our case, the inclusion $F \subset \mathrm{End}(A) \otimes \mathbf{Q}$, gives even more structure to $T_\ell(A)$ and, hence, V_ℓ. Indeed, $\mathrm{End}(A) \otimes \mathbf{Q}$ acts on V_ℓ, so we can view V_ℓ as an $F_\ell := F \otimes \mathbf{Q}_\ell$ module. Furthermore, by definition, the endomorphisms in $\mathrm{End}(A)$ are defined over K, so the action of G on V_ℓ is F_ℓ-linear. The decomposition $F_\ell = \prod_{\lambda|\ell} F_\lambda$ gives a decomposition

$$V_\ell = \prod_{\lambda|\ell} V_\lambda \quad \text{where} \quad V_\lambda := V_\ell \otimes_{F_\ell} F_\lambda.$$

Thus the ℓ-adic representation ρ_ℓ can be decomposed as the sum of λ-adic representations $\rho_\lambda : G \to \mathrm{Aut}_{E_\lambda} V_\lambda$.

Proposition 3.3 *As an F_ℓ-module, V_ℓ is free of rank 2. Moreover, the F_λ-dimension of V_λ is independent of λ.*

Proof. Let h_λ be the F_λ-dimension of V_λ and let $d_\lambda = [F_\lambda : \mathbf{Q}_\ell]$. Then $4 = \sum_\lambda d_\lambda h_\lambda$. The key is to show that $h_\lambda = 2$ for all λ.

To do this, let $\alpha \in F$ be such that $F = \mathbf{Q}(\alpha)$ and let $f(x)$ be its minimal polynomial. Note that for $\lambda|\ell$, the image of α in F_λ generates F_λ over $\mathbf{Q}_\ell$. Let $f_\lambda(x)$ be the minimal polynomial of $\alpha \in F_\lambda$. Then $f(x) = \prod_{\lambda|\ell} f_\lambda(x)$ in $\mathbf{Q}_\ell[x]$. Note that the action of α on V_ℓ has characteristic polynomial $f(x)^2$ (see [31]) while the characteristic polynomial of the α-action on each V_λ is $f_\lambda(x)^{h_\lambda}$. Therefore, since $V_\ell = \prod_{\lambda|\ell} V_\lambda$, we have $f(x)^2 = \prod_{\lambda|\ell} f_\lambda(x)^{h_\lambda}$, so unique factorization in $\mathbf{Q}_\ell[x]$ implies that $h_\lambda = 2$ for all λ. $\diamond$

As an immediate consequence to Proposition 3.3 we have the following corollary.

Corollary 3.4 *The ℓ-adic Tate module is a free $\mathfrak{o}_F \otimes \mathbf{Z}_\ell$-module of rank 2. Moreover,*

- *if ℓ is inert or if ℓ ramifies in F then $\rho_\ell : G \to \mathrm{GL}_2(\mathfrak{o}_F \otimes \mathbf{Z}_\ell) \hookrightarrow \mathrm{GL}_4(\mathbf{Z}_\ell)$,*
- *if ℓ splits in F then $\rho_\ell : G \to \mathrm{GL}_2(\mathbf{Z}_\ell) \times \mathrm{GL}_2(\mathbf{Z}_\ell) \hookrightarrow \mathrm{GL}_4(\mathbf{Z}_\ell)$.*

Using the existence of a Weil pairing, we can glean even more information about the determinants of such representations.

Lemma 3.5 *Let A/K be an abelian variety and let $A^\vee$ be its dual. Then, for each $m \in \mathbf{Z}$, there is a nondegenerate bilinear pairing $\overline{e}_m : A[m] \times A^\vee[m] \to \mu_m$ such that*

(1) $\overline{e}_m(x,y)^\sigma = \overline{e}_m(x^\sigma, y^\sigma)$ *for each* $\sigma \in G$,

(2) *if* $f : A \to A$ *is a homomorphism then* $\overline{e}_m(f(x), y) = \overline{e}_m(x, f^\vee(y))$,

(3) $\overline{e}_{mn}(x,y)^n = \overline{e}_m(nx, ny)$.

Proof. See section 16 of [26]. ◇

Using property 3, we define a nondegenerate bilinear pairing

$$e_\ell : T_\ell(A) \times T_\ell(A^\vee) \to T_\ell(\mu) \cong \mathbf{Z}_\ell(1),$$

where $\mathbf{Z}_\ell(1)$ denotes the Tate twist of $\mathbf{Z}_\ell$. Furthermore, e_ℓ satisfies properties 1 and 2 of Lemma 3.5. Suppose that $\omega : A \to A^\vee$ is a principal polarization and that the Rosati involution on $\mathrm{End}(A)$, defined by $\alpha \mapsto \omega^{-1} \circ \alpha^\vee \circ \omega$, fixes all $\alpha \in \mathfrak{o}_F$. Define the pairing $e_\ell^\omega = e_\ell \circ (1 \times \omega)$. Then $e_\ell^\omega : T_\ell(A) \times T_\ell(A) \to \mathbf{Z}_\ell(1)$ is a nondegenerate $\mathbf{Z}_\ell$-bilinear antisymmetric pairing such that

- $e_\ell^\omega(\alpha x, y) = e_\ell^\omega(x, \alpha y)$ for all $\alpha \in \mathfrak{o}_F$,
- $e_\ell^\omega(x^\sigma, y^\sigma) = e_\ell^\omega(x,y)^\sigma = \varepsilon(\sigma) e_\ell^\omega(x,y)$ for all $\sigma \in G$, where $\varepsilon : G \to \mathbf{Z}_\ell^\times$ is the cyclotomic character.

Using e_ℓ^ω, we now compute the determinant of $\rho_\ell : G \to \mathrm{GL}_4(\mathbf{Z}_\ell)$.

Lemma 3.6 *The determinant of ρ_ℓ is ε^2.*

Proof. Fix $\sigma \in G$. Set $t = \varepsilon(\sigma)$ and define $W = T_\ell(A) \otimes \mathbf{Q}_\ell(t^{1/2})$. Then it is straightforward to check e_ℓ^ω defines a symplectic pairing on W and that $t^{-1/2}\rho_\ell(\sigma)$ preserves the pairing. This means $t^{-1/2}\rho_\ell(\sigma)$ lies in the group of symplectic matrices $\mathrm{Sp}(W) \subset \mathrm{SL}(W)$. Hence $\det(t^{-1/2}\rho_\ell(\sigma)) = 1$, so as desired, $\det(\rho_\ell(\sigma)) = \varepsilon(\sigma)^2$. ◇

For simplicity, from now on assume that ℓ does not ramify in F (that is, ℓ is either inert or split in F). This assumption, however, is not a serious restriction for us since, in Chapter 4, when $F = \mathbf{Q}(\sqrt{5})$, other considerations force us to assume $\ell > 5$. The next goal is to compute $\det(\rho'_\ell)$.

Lemma 3.7 *Suppose $S \subset R$ are commutative rings with a G-action. Let M be an R-module with a G-action, an S-linear map $t : R \to S$ and a nondegenerate antisymmetric S-bilinear pairing $\psi : M \times M \to S$ satisfying*

(1) *$(r_1, r_2) \mapsto t(r_1 r_2)$ is a perfect pairing,*

(2) *$\psi(rx, y) = \psi(x, ry)$ for all $x, y \in M$ and $r \in R$,*

(3) *$(rx)^\sigma = r^\sigma x^\sigma$ for all $\sigma \in G$ and for all $r \in R$ and $x \in M$,*

(4) *t and ψ are Galois equivariant. That is, $t(r)^\sigma = t(r^\sigma)$ and $\psi(x, y)^\sigma = \psi(x^\sigma, y^\sigma)$ for all $\sigma \in G$, $r \in R$ and $x, y \in M$.*

Then there is a unique $\varphi : M \times M \to R$ such that $\psi = t \circ \varphi$ and, moreover, φ is nondegenerate, antisymmetric, Galois equivariant and R-bilinear.

Proof. Define φ as follows. Fix $x, y \in M$. Then $r \mapsto \psi(rx, y)$ is an S-linear map $R \to S$, so using (1), there is a unique $\varphi(x, y)$ in R such that $t(r\varphi(x, y)) = \psi(rx, y)$ for all $r \in R$. Letting x and y run over M gives $\varphi(x, y)$ in general. In a like manner, the rest of this lemma follows from a repeated use of (1). For example, for all $r \in R$,

$$\begin{aligned} t(r^\sigma \varphi(x, y)^\sigma) &= t(r\varphi(x, y))^\sigma \\ &= \psi(rx, y)^\sigma \\ &= \psi((rx)^\sigma, y^\sigma) \\ &= t(r^\sigma \varphi(x^\sigma, y^\sigma)), \end{aligned}$$

so (1) implies $\varphi(x, y)^\sigma = \varphi(x^\sigma, y^\sigma)$. ◇

Proposition 3.8 *Let ρ'_ℓ be as above.*

- *If ℓ is inert in F then $\det(\rho'_\ell) = \varepsilon$.*
- *If ℓ splits in F then $\det(p_i \circ \rho'_\ell) = \varepsilon$ for $i = 1, 2$, where p_i denotes the projection $\mathrm{GL}_2(\mathbf{Z}_\ell) \times \mathrm{GL}_2(\mathbf{Z}_\ell) \to \mathrm{GL}_2(\mathbf{Z}_\ell)$ onto the ith factor.*

Proof. First assume ℓ is inert. For simplicity of notation, let $R = \mathfrak{o}_F \otimes \mathbf{Z}_\ell(1)$. Then the determinant of the $\mathbf{Z}_\ell$-bilinear form $(r_1, r_2) \mapsto \mathrm{Tr}_{R/\mathbf{Z}_\ell}(r_1 r_2)$ is the discriminant of $R/\mathbf{Z}_\ell$, which is a unit in $\mathbf{Z}_\ell$. Hence we may apply Lemma 3.7 with $M = T_\ell(A)$, $t = \mathrm{Tr}_{R/\mathbf{Z}_\ell}$ and $\psi = e_\ell^\omega$ to get a nondegenerate, antisymmetric R-bilinear pairing $\varphi : T_\ell(A) \times T_\ell(A) \to R$ such that $\mathrm{Tr}_{R/\mathbf{Z}_\ell} \varphi = e_\ell^\omega$. In particular, φ is Galois equivariant, so for all $\sigma \in G$,

$$\varepsilon(\sigma) e_\ell^\omega(x, y) = \mathrm{Tr}_{R/\mathbf{Z}_\ell}(\det \rho'_\ell \varphi(x, y)). \tag{3.1}$$

Write $R = \mathbf{Z}_\ell(\alpha)$, so $\det \rho'_\ell(\sigma) = a + b\alpha$. We will manipulate equation 3.1 to get two linear equations in a and b, after which we will show that $b = 0$ and $a = \varepsilon(\sigma)$. Using the nondegeneracy of φ, pick $x, y \in T_\ell(A)$ such that $\varphi(x, y) = 1$. Then equation 3.1 becomes

$$2\varepsilon(\sigma) = \mathrm{Tr}_{R/\mathbf{Z}_\ell}(a + b\alpha) = 2a + b \,\mathrm{Tr}_{R/\mathbf{Z}_\ell}(\alpha).$$

Replacing x by αx gives a second equation:

$$\begin{aligned} \varepsilon(\sigma) \,\mathrm{Tr}_{R/\mathbf{Z}_\ell}(\alpha) &= \mathrm{Tr}_{R/\mathbf{Z}_\ell}(a\alpha + b(\mathrm{Tr}_{R/\mathbf{Z}_\ell}(\alpha)\alpha - \mathrm{N}_{R/\mathbf{Z}_\ell}(\alpha))) \\ &= a \,\mathrm{Tr}_{R/\mathbf{Z}_\ell}(\alpha) + b \,\mathrm{Tr}_{R/\mathbf{Z}_\ell}(\alpha)^2 + 2b \,\mathrm{N}_{R/\mathbf{Z}_\ell}(\alpha) \end{aligned}$$

where $\mathrm{N}_{R/\mathbf{Z}_\ell}(\alpha)$ is the norm from R down to $\mathbf{Z}_\ell$ (i.e., the product of the Galois conjugates of α). Eliminating a yields the equation

$$0 = b(\mathrm{Tr}_{R/\mathbf{Z}_\ell}(\alpha)^2 + 4 \,\mathrm{N}_{R/\mathbf{Z}_\ell}(\alpha)),$$

but $\mathrm{Tr}_{R/\mathbf{Z}_\ell}(\alpha)^2 + 4 \,\mathrm{N}_{R/\mathbf{Z}_\ell}(\alpha)$ is the discriminant of the minimal polynomial of α, which is nonzero. Hence $b = 0$, which implies $a = \varepsilon(\sigma)$.

Now suppose that ℓ splits. Then $\mathfrak{o}_F \otimes \mathbf{Z}_\ell = \mathbf{Z}_\ell \times \mathbf{Z}_\ell$. Let $\mathcal{O}_1 = \mathbf{Z}_\ell \times \{0\}$ and $\mathcal{O}_2 = \{0\} \times \mathbf{Z}_\ell$. Let $T_i = \mathcal{O}_i T_\ell(A)$. Then $T_\ell(A) = T_1 \times T_2$. (This is the same decomposition given in Corollary 3.4.) Moreover, for $x \in T_1$ and $y \in T_2$, writing $y = \alpha y'$ for some $\alpha \in \mathcal{O}_2$ and $y' \in T_\ell(A)$ gives

$$\begin{aligned} e_\ell^\omega(x,y) &= e_\ell^\omega(x, \alpha y') \\ &= e_\ell^\omega(\alpha x, y') \\ &= e_\ell^\omega(0, y') \\ &= 0, \end{aligned}$$

so $T_1 \subset T_2^\perp$. Thus, the nondegeneracy of e_ℓ^ω allows us to restrict e_ℓ^ω to a nondegenerate pairing e_i on each T_i satisfying all of the properties of e_ℓ^ω. Finally, repeating the arguments of Lemma 3.6 for each e_i yields the desired conclusion. $\diamond$

Remark 3.9 *Our presentation up until this point is a combination of [29] and [37, Chapter 4]. In fact, both Ribet and Wilson treat abelian varieties of arbitrary dimension and Ribet even addresses the case where* $\dim A \neq [F : \mathbf{Q}]$ *to some extent. Moreover, one of the main results of [29] is that the image of* ρ_ℓ *is maximal for almost all* ℓ*.*

We conclude this chapter with an analysis of the image of ρ'_ℓ when restricted to a decomposition group of ℓ. Although this is surely not original, I have yet to find an explicit description elsewhere. As our focus in Chapter 4 is on odd primes of good, nonsupersingular reduction for abelian surfaces over $\mathbf{Q}$, we assume that A is defined over $\mathbf{Q}$ and has good, nonsupersingular reduction at $\ell \geq 3$. In fact, for reasons discussed in the proof of Lemma 4.8, the description when ℓ splits can be reduced to the argument in this next proposition.

Proposition 3.10 *Let* ℓ *be inert in* F*. Then the image* ρ'_ℓ *restricted to a decomposition group at* ℓ *has the form*

$$\begin{pmatrix} \varepsilon\chi^{-1} & \mu \\ 0 & \chi \end{pmatrix}$$

where χ is an unramified character and μ is either trivial or wildly ramified.

Proof. Since ℓ is inert and A has good, nonsupersingular reduction at ℓ, we know that ℓ is actually a prime of ordinary reduction by [1, Proposition 4.1]. Moreover, since A has good reduction at ℓ, we may consider A as an abelian surface over $\mathbf{Q}_\ell$. Consider the reduction exact sequence

$$0 \to \hat{A} \to A \to \tilde{A} \to 0,$$

where $\hat{A}$ is the formal group of A over $\mathbf{Z}_\ell$ and $\tilde{A}$ is the reduction of A modulo ℓ. The Galois equivariance of this sequence combined with Proposition 3.8 shows that $\rho'_\ell|_{G_\ell}$ (where G_ℓ denotes a decomposition subgroup of G at ℓ) has the form

$$\begin{pmatrix} \varepsilon\chi^{-1} & \mu \\ 0 & \chi \end{pmatrix}$$

and that χ is unramified. The last thing to check is that $\mu = 0$ on G_ℓ if and only if $\mu = 0$ on the wild ramification subgroup W.

To see that μ is either trivial or wildly ramified, consider the twist of ρ'_ℓ by $\varepsilon^{-1}\chi$:

$$\begin{pmatrix} 1 & \mu \\ 0 & \varepsilon^{-1}\chi^2 \end{pmatrix}.$$

Then $\mu \in H^1(G_\ell, \mathcal{O}(\varepsilon^{-1}\chi^2))$ where $\mathcal{O}(\varepsilon^{-1}\chi^2) := \varprojlim(\mathfrak{o}_F/\ell^n)(\varepsilon^{-1}\chi^2)$. Consider the inflation-restriction exact sequence

$$0 \longrightarrow H^1(G_\ell/I, \mathcal{O}(\varepsilon^{-1}\chi^2)^I) \xrightarrow{\text{inf}} H^1(G_\ell, \mathcal{O}(\varepsilon^{-1}\chi^2)) \xrightarrow{\text{res}} H^1(I, \mathcal{O}(\varepsilon^{-1}))$$

where I is the inertia subgroup of G_ℓ. If $\tilde{\mu} := \operatorname{res}\mu$ is zero then $\mu \in H^1(G_\ell/I, \mathcal{O}(\varepsilon^{-1}\chi^2)^I)$, but $\mathcal{O}(\varepsilon^{-1}\chi^2)^I = 0$, so $\mu = 0$. Thus we have $\mu = 0$ if and only if its restriction to I is zero. Now consider the inflation-restriction exact sequence

$$0 \longrightarrow H^1(I/W, \mathcal{O}(\varepsilon^{-1})^W) \xrightarrow{\text{inf}} H^1(I, \mathcal{O}(\varepsilon^{-1})) \xrightarrow{\text{res}} H^1(W, \mathcal{O}(\varepsilon^{-1})).$$

If $\operatorname{res}\tilde{\mu} = 0$ then $\tilde{\mu} \in H^1(I/W, \mathcal{O}(\varepsilon^{-1})^W)$, but $\mathcal{O}(\varepsilon^{-1})^W = 0$, so $\tilde{\mu} = 0$. ◇

CHAPTER 4

ALGEBRAIC RESULTS

Assume $p > 2$. Let k be a finite extension of $\mathbf{F}_p$ of degree d. Let W denote the ring of Witt vectors over k and let K be the field of fractions of W. Set $W_2 = W/p^2W$. Define the *p-rank* of a finite abelian group M to be the $\mathbf{F}_p$-dimension of $M \otimes_{\mathbf{Z}} \mathbf{F}_p$ (or, equivalently, the $\mathbf{F}_p$-dimension of the p-torsion subgroup $M[p]$). Denote the p-rank of M by $\operatorname{rank}_p M$. Our first result gives a condition for when an abelian variety over K has a nontrivial p-torsion point defined over K.

Lemma 4.1 *Let A be a g-dimensional abelian variety over K of good reduction. Then* $\operatorname{rank}_p A(W_2) = gd$ *if* $A(K)[p] = 0$ *and* $gd + 1 \leq \operatorname{rank}_p A(W_2) \leq g(d+1)$ *if* $A(K)[p] \neq 0$.

Proof. Consider the commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widehat{A}(pW) & \longrightarrow & A(K) & \longrightarrow & A(k) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \widehat{A}(pW/p^2W) & \longrightarrow & A(W_2) & \longrightarrow & A(k) & \longrightarrow & 0 \end{array}$$

where $\widehat{A}$ is the formal group of A over W. Since $p > 2$, $\widehat{A}(pW) \cong (p\mathbf{Z}_p)^{gd}$ and the morphism $\widehat{A}(pW) \to \widehat{A}(pW/p^2W)$ can be identified with the natural reduction morphism $\mathbf{Z}_p^{gd} \to (\mathbf{Z}/p)^{gd}$. Therefore, taking p-torsion and applying the snake lemma gives the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & A(K)[p] & \longrightarrow & A(k)[p] & \longrightarrow & (\mathbf{Z}/p)^{gd} \\ & & \downarrow & & \downarrow & & \| & & \| \\ 0 & \longrightarrow & (\mathbf{Z}/p)^{gd} & \longrightarrow & A(W_2)[p] & \longrightarrow & A(k)[p] & \longrightarrow & (\mathbf{Z}/p)^{gd}. \end{array}$$

So $\operatorname{rank}_p A(W_2) = gd + \operatorname{rank}_p A(K)[p]$. The lemma then follows from the structure of $A(K)[p]$ and the fact that $A(K)[p]$ injects into $A(k)[p]$. $\diamond$

Let A/S be an abelian scheme of relative dimension g over a W-scheme S (that is, a commutative group scheme such that $A \to S$ is separated, proper and smooth and has connected geometric fibers of dimension g). Then given a relatively ample invertible sheaf L on A, there is an associated homomorphism

$$\Lambda(L) : A \to A^\vee$$

where $A^\vee$ is the dual abelian scheme of A (see [25]).

Definition 4.2 *Let A/S be an abelian scheme.* A principal polarization *of A is an S-isomorphism $\lambda : A \to A^\vee$ such that for all geometric points s of S, the induced map $\lambda_s : A \times_S s \to A^\vee \times_S s$ is of the form $\Lambda(L_s)$ for some ample invertible sheaf L_s on $A \times_S s$.*

Recall that in Example 2.7, we showed that the Bartsotti-Tate group $E[p^\infty]$ of an ordinary elliptic curve over k factors as $\mu_{p^\infty}(\chi^{-1}) \times (\mathbf{Q}_p/\mathbf{Z}_p)(\chi)$. More generally, given a Barsotti-Tate group G over k, there is a canonical splitting $G \cong G_{\text{ét}} \times G_{\text{mult}} \times G_{\text{ll}}$, where $G_{\text{ét}}$ is the maximal étale quotient of G, G_{mult} is the maximal multiplicative subgroup of G and G_{ll} is a Barsotti-Tate group with no non-trivial étale quotient nor non-trivial multiplicative Barsotti-Tate subgroup (see, for example, [9], [10]). Comparing this with our factorization of $E[p^\infty]$, we have $E[p^\infty]_{\text{mult}} = \mu_{p^\infty}(\chi^{-1})$, $E[p^\infty]_{\text{ét}} = (\mathbf{Q}_p/\mathbf{Z}_p)(\chi)$ and $E[p^\infty]_{\text{ll}} = 0$. This fact about the splitting of Barsotti-Tate groups over k will be used in the proofs of the next three results.

Proposition 4.3 *Let A be a principally polarized, ordinary abelian surface over k and assumer that $A(k)[p] \neq 0$. Then exactly $p^{3d} + p^{2d} - p^d$ of the p^{4d} isomorphism classes of lifts of A to an abelian surface A' over W_2 satisfy*

$$\operatorname{rank}_p A'(W_2) \geq 2d + 1.$$

Proof. The Serre-Tate lifting theorem [19] tells us that lifts of A to W_2 are parameterized by lifts of $A[p^\infty]$ to p-divisible groups over W_2. Since A is ordinary, the connected-étale exact sequence for $A[p^n]$ gives the following split exact sequence of group schemes over k:

$$0 \to \mu_{p^\infty}^2((\sigma^{-1})^T) \to A[p^\infty] \to (\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma) \to 0 \tag{4.1}$$

where $\sigma : \mathrm{Gal}(\overline{k}/k) \to \mathrm{GL}_2(\mathbf{Z}_p)$ gives the action of Frobenius on $(\mathbf{Q}_p/\mathbf{Z}_p)^2$. Lemma 2.19 and Lemma 2.20 show that there are unique lifts of $(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma)$ and $\mu_{p^\infty}^2((\sigma^{-1})^T)$ to group schemes over W_2, so, abusing notation, every lift of $A[p^\infty]$ to W_2 is an extension of $(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma)$ by $\mu_{p^\infty}^2((\sigma^{-1})^T)$.

Let $M' = \mathcal{M}(A[p^\infty]) \otimes W_2$ be the Dieudonne module of $A[p^\infty]$ over W_2 and let $L = \underline{\omega}_{A[p^\infty]} \subset M' \otimes k$ be as in Corollary 2.18. Recall that Corollary 2.18 says that lifts of Barsotti-Tate groups over k to Barsotti-Tate groups over W_2 are parameterized by pairs (M', L'), where L' is a W_2-submodule of M' that is a direct summand and $L' \otimes k = L$. Thus it suffices to count the number of such lifts of L.

As a W_2-module, M' is a free module of rank 4. Furthermore, since A is ordinary, $A[p^\infty] \cong A[p^\infty]_{\text{ét}} \times A[p^\infty]_{\text{mult}}$ where $A[p^\infty]_{\text{ét}} = (\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma)$ and the multiplicative subgroup $A[p^\infty]_{\text{mult}} = \mu_{p^\infty}^2((\sigma^{-1})^T)$. Thus the Dieudonné module $\mathcal{M}(A[p^\infty])$ splits as $\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma) \times \mathcal{M}(\mu_{p^\infty}^2((\sigma^{-1})^T))$. From here we may conclude that the submodule $L = \mathcal{M}(\mu_{p^\infty}^2((\sigma^{-1})^T)) \otimes k$ from the proofs of Lemmas 2.19 and 2.20.

Pick a normalized basis e_1, e_2, e_3, and e_4 of $M' \otimes k$ that reflects the splitting of the Dieudonné module $\mathcal{M}(A[p^\infty])$ into its étale and multiplicative parts. That is, e_1 and e_2 are a basis of the submodule $\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma) \otimes k \times \{0\}$ while e_3 and e_4 form a basis of the submodule $\{0\} \times \mathcal{M}(\mu_{p^\infty}^2((\sigma^{-1})^T)) \otimes k$. By abuse of notation, we will also use $e_1, \ldots, e_4$ to denote $e_i \otimes 1$ in M'. Since $L = \langle e_3, e_4 \rangle$, every lift of L to L' may be written in the form $\langle p\alpha_1 e_1 + p\alpha_2 e_2 + e_3, p\beta_1 e_1 + p\beta_2 e_2 + e_4 \rangle$ for some $\alpha_i, \beta_i \in W_2$; thus there are p^{4d} isomorphism classes of lifts of A to A'.

To detect those isomorphism classes of lifts with elevated p-rank, we must determine the L' that admit a map of pairs $(M', L') \to (N, 0)$ such that the composition

$$(\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma) \otimes W_2, 0) \hookrightarrow (M', L') \to (N, 0)$$

is the identity on $(N, 0)$, where $N = \langle e_1 + \alpha e_2 \rangle$ or $N = \langle e_2 \rangle$ for some $\alpha \in W_2$. Such maps exist exactly when the image of the projection $L' \to \mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma) \otimes W_2$ has trivial intersection with N. Hence there are $(p^d + 1)(p^d - 1) + 1 = p^{3d} + p^{2d} - p^d$ isomorphism classes of lifts with elevated p-rank. $\diamond$

Let $\mathfrak{o}$ be the ring of integers in $\mathbf{Q}(\sqrt{5})$ and assume $p > 5$.

Definition 4.4 *Let A be an abelian scheme over a $\mathbf{Z}$-scheme S. Say that A has* real multiplication *by $\mathbf{Q}(\sqrt{5})$ if there is a homomorphism $i : \mathfrak{o} \to \mathrm{End}(A)$ with $i(1) = \mathrm{Id}$ such that $\mathrm{Lie}(A)$ is a locally free $\mathfrak{o} \otimes \mathcal{O}_S$-module of rank 1.*

Remark 4.5 *In terms of the results of this chapter, there is nothing special about the choice of $\mathbf{Q}(\sqrt{5})$. As indicated by Proposition 4.3, these techniques are completely general and can be used for abelian surfaces with other types of real multiplication. In fact, should one desire to spend the time working out the linear algebra, with the possible exception of Lemma 4.8, it should be relatively easy to obtain the analogous results for higher dimensional abelian varieties.*

Lemma 4.6 *Let A be a principally polarized, ordinary abelian surface over k with real multiplication by $\mathbf{Q}(\sqrt{5})$. Suppose that $A(k)[p] \neq 0$. If $\mathfrak{o} \otimes W_2 \cong W_2 \times W_2$ then exactly $2p^d - 1$ of the p^{2d} isomorphism classes of lifts of A to an abelian surface A' over W_2 satisfy*

$$\mathrm{rank}_p\, A'(W_2) \geq 2d + 1.$$

Otherwise, $\mathfrak{o} \otimes W_2 \cong W_2[\sqrt{5}]$ and there is a unique isomorphism class lifting A to an abelian surface A' over W_2 satisfying

$$\mathrm{rank}_p\, A'(W_2) \geq 2d + 1.$$

Proof. The argument in this case follows the same logic as in Proposition 4.3 except that now we must include a condition on L and on L' that takes the real multiplication into consideration. More precisely, we require L and L' to be $\mathfrak{o} \otimes W_2$-modules of rank one. Note that

$$\mathfrak{o} \otimes W_2 \cong \begin{cases} W_2 \times W_2, & \text{if } p \text{ splits in } \mathfrak{o} \text{ or if } [k : \mathbf{F}_p] \equiv 0(2), \\ W_2[\sqrt{5}], & \text{otherwise.} \end{cases}$$

We'll treat these two possibilities separately.

Since

$$A[p^\infty] = \mu_{p^\infty}^2((\sigma^{-1})^T) \times (\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma)$$

over k, and since $\mu_{p^\infty}^2((\sigma^{-1})^T)$ is connected while $(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma)$ is étale, each of these direct factors of $A[p^\infty]$ must be stable under the action of $\mathfrak{o} \otimes W_2$. Returning to the Dieudonné module side of the picture, this shows that the action of $\mathfrak{o} \otimes W_2$ on $M' \otimes k$ has the form

$$\begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}$$

where C is a 2×2 matrix.

If $\mathfrak{o} \otimes W_2 \cong W_2 \times W_2$ then the action of $\mathfrak{o} \otimes W_2$ on $M' \otimes k$ is generated by two orthogonal idempotent matrices whose sum is the identity. Their minimal polynomial is $X^2 - X$. Furthermore, since as an $\mathfrak{o} \otimes W_2$-module, $L = (W_2 e_3 \oplus W_2 e_4) \otimes k$ must be (locally) free of rank 1, Cartier duality shows that, up to a change of basis, the action of $\mathfrak{o} \otimes W_2$ on $M' \otimes k$ is generated by

$$f_1 = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{pmatrix} \text{ and } f_2 = \begin{pmatrix} 0 & & & \\ & 1 & & \\ & & 0 & \\ & & & 1 \end{pmatrix}.$$

(Looking back at the proof of Proposition 4.3, one might be concerned about this change of basis because we had normalized the basis e_1, e_2, e_3, e_4 of M'. However, the change of

basis involved in obtaining f_1 and f_2 corresponds to independent change of bases of the subspaces $\langle e_1, e_2\rangle$ and $\langle e_3, e_4\rangle$, so this still reflects the splitting of the Dieudonné module $\mathcal{M}(A[p^\infty])$ into its étale and multiplicative pieces.) A simple check reveals that $e_3 + e_4$ is a basis for L as an $\mathcal{O} \otimes W_2$-module.

Now consider the action of $\mathfrak{o} \otimes W_2$ on M'. A priori, the entries that are zero and the entries that are one in f_1 and f_2 might lift to entries of the form $p\alpha$ and $1 + p\alpha$ respectively for some $\alpha \in W_2^\times$, however, a simple calculation shows that the resulting matrices would not be idempotent. Therefore, f_1 and f_2 still generate the action of $\mathfrak{o}\otimes W_2$ on M'. Moreover, using this, an easy calculation shows that every lift of L to L' has a basis of the form $e := p\alpha_1 e_1 + p\alpha_2 e_2 + e_3 + e_4$ for some $\alpha_i \in W_2$. Hence there are p^{2d} isomorphism classes of lifts of A to A'.

To determine the lifts with elevated p-rank, we need to again detect which L' admit a map of pairs $(M', L') \to (N, 0)$ such that the composition

$$(\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma) \otimes W_2, 0) \hookrightarrow (M', L') \to (N, 0)$$

is the identity on $(N, 0)$ where $N = \langle e_1 + \beta e_2\rangle$ or $N = \langle e_2\rangle$ for $\beta \in W_2$. Such maps exists exactly when the image of the projection $L' \to \mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma) \otimes W_2$ has trivial intersection with N.

Suppose that $p\alpha_1$ and $p\alpha_2$ are nonzero. Then $f_1 e = p\alpha_1 e_1 + e_3$ and $f_2 e = p\alpha_2 e_2 + e_4$, so one can scale each of these independently so that

$$pe_1 + p\beta e_2 + \alpha_1^{-1} e_3 + \beta\alpha_2^{-1} e_4 \quad \text{and} \quad pe_2 + \alpha_2^{-1} e_2$$

are in L'. Therefore, the image of the projection $L' \to M(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma)$ has nontrivial intersection with pN and, hence, with N. This means that $\alpha_1 = 0$ or $\alpha_2 = 0$. From here it is straightforward to conclude that $2p^d - 1$ isomorphism classes of lifts of A to A' have elevated p-rank.

Finally, we treat the case where $\mathfrak{o} \otimes W_2 \cong W_2[\sqrt{5}]$. Now the action of $\mathfrak{o} \otimes W_2$ on $M' \otimes k$ is generated by the identity matrix and a matrix of the form

$$D := \begin{pmatrix} C & 0 \\ 0 & C \end{pmatrix}$$

where C is a 2×2 matrix whose minimal polynomial is $X^2 - 5$. Writing this in rational canonical form shows that, up to a change of basis,

$$C = \begin{pmatrix} 0 & 5 \\ 1 & 0 \end{pmatrix}.$$

(Again, this change of basis does not affect our normalization for reasons similar to those mentioned previously.)

From here, the argument follows as in the case that $\mathfrak{o} \otimes W_2 \cong W_2 \times W_2$ with one exception. If $p\alpha_1 \neq 0$ or $p\alpha_2 \neq 0$ then the image of the projection morphism $L' \to \mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma) \otimes W_2$ has nontrivial intersection with N. Indeed, without loss of generality, we may assume that $p\alpha_1 \neq 0$. Then $\alpha_1 \in W_2^\times$ and $De = p\alpha_1 e_2 + 5e_3 + e_4$. Since $\alpha_1 e_1$ and $\alpha_1 e_2$ are linearly independent over W_2, there is a nonzero W_2-linear combination of e and De such that its image under the projection morphism $L' \to \mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)^2(\sigma) \otimes W_2$ lands in $pN \setminus \{0\}$. One can use an almost identical argument when α_1 and α_2 are both nonzero. Therefore, in this case there is a unique isomorphism class lifting A to an A' with elevated p-rank. $\diamond$

Finally, if p is split in $\mathfrak{o}$ then an abelian surface A over k with real multiplication by $\mathbf{Q}(\sqrt{5})$ can be nonordinary and nonsupersingular (see [1]). Namely,

$$A[p^\infty] \cong A[p^\infty]_{\mathrm{ll}} \times \mu_{p^\infty}(\chi^{-1}) \times \mathbf{Q}_p/\mathbf{Z}_p(\chi)$$

where $\chi : \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(\mathbf{Q}_p/\mathbf{Z}_p)$ give the action of Frobenius on the respective factors of $A[p^\infty]$.

Lemma 4.7 *Let A be a principally polarized, nonordinary and nonsupersingular abelian surface over k with real multiplication by $\mathbf{Q}(\sqrt{5})$. Assume that $A(k)[p] \neq 0$. Then exactly p^d of the p^{2d} isomorphism classes of lifts of A to an abelian surface A' over W_2 satisfy*

$$\operatorname{rank}_p A'(W_2) \geq 2d + 1.$$

Proof. As noted in the paragraph prior to this lemma, p splits in $\mathfrak{o}$, so $\mathfrak{o} \otimes W_2 \cong W_2 \times W_2$. Again considering the Dieudonne module of $A[p^\infty]$ over W_2 gives a free W_2-module M' of rank 4. Take a basis e_1, e_2, e_3, and e_4 of M' such that e_1 and e_2 are a basis of the submodule $\mathcal{M}(A[p^\infty]_{ll}) \otimes W_2$, e_3 is a basis of the submodule $\mathcal{M}(\mu_{p^\infty})(\chi^{-1}) \otimes W_2$ and e_4 is a basis of the submodule $\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)(\chi) \otimes W_2$.

Before looking at the action of $\mathfrak{o} \otimes W_2$ on M', first consider the action of $\mathfrak{o} \otimes W_2$ on $M' \otimes k$. As in the proof of Lemma 4.6, the connected and étale pieces of $M' \otimes k$ must be stable under the action of $\mathfrak{o} \otimes W_2$. Furthermore, applying Cartier duality shows that the submodule $\mathcal{M}(A[p^\infty]_{ll}) \otimes W_2$ is also stable under the $\mathfrak{o} \otimes W_2$ action. Therefore, the action of $\mathfrak{o} \otimes W_2 \cong W_2 \times W_2$ on $M' \otimes k$ is generated by two orthogonal, block diagonal matrices whose sum is the identity. After some consideration, one concludes that, up to a change of basis preserving the submodule structure described in the previous paragraph, generators for the action of $\mathfrak{o} \otimes W_2$ on $M' \otimes k$ are

$$f_1 = \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 0 & \\ & & & 0 \end{pmatrix} \text{ and } f_2 = \begin{pmatrix} 0 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}.$$

Again, these matrices also give the $\mathfrak{o} \otimes W_2$ action on M' so we may assume that $e_1, \ldots, e_4$ are so normalized. Moreover, L is a 2-dimensional subspace of the connected subspace in $M' \otimes k$ with a basis of the form $e_1 + be_2$, e_3 (since $\mathcal{M}(A[p^\infty]_{ll}) \otimes W_2$ and $\mathcal{M}(\mu_{p^\infty})(\chi^{-1}) \otimes W_2$ are direct summands of M'). Therefore, as an $\mathfrak{o} \otimes W_2$-module, we may assume (without loss of generality) that $e_1 + be_2 + e_3$ is a basis of L for some $b \in k$. From here, it is

straightforward to conclude that every lift of L to L' has an $\mathfrak{o} \otimes W_2$-basis of the form $e_1 + \beta e_2 + e_3 + p\gamma e_4$ where $\beta, \gamma \in W_2$ and $\beta \equiv b \bmod pW_2$. Thus there are p^{2d} isomorphism classes of lifts.

To determine the lifts with elevated p-rank, we need to again detect which L' admit a map of pairs $(M', L') \to (\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)(\chi) \otimes W_2, 0)$ such that the composition

$$(\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)(\chi) \otimes W_2, 0) \hookrightarrow (M', L') \to (\mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)(\chi) \otimes W_2, 0)$$

is the identity. Such maps exist exactly when the image of the projection morphism $L' \to \mathcal{M}(\mathbf{Q}_p/\mathbf{Z}_p)(\chi) \otimes W_2$ is trivial. Considering that $L' = \mathcal{O} \otimes W_2(e_1 + \beta e_2 + e_3 + p\gamma e_4)$, this projection is trivial when $\gamma = 0$, so p^d isomorphism classes of lifts of A to A' have elevated p-rank. $\diamond$

Up until this point, we have assumed that K is an unramified extension of $\mathbf{Q}_p$. The last result of this chapter enables us to address the possibility that K may be ramified in the statement of Theorem 1.2.

Lemma 4.8 *Let A be a principally polarized abelian surface over $\mathbf{Q}$ with real multiplication by $\mathbf{Q}(\sqrt{5})$. Suppose $A(K)[p] \neq 0$ and $[K : \mathbf{Q}_p] \leq d$. If $p - 1 > d$ and A has good reduction at p, then $A(K^{\mathrm{ur}})[p] \neq 0$ where K^{ur} is the maximal unramified subfield of K.*

Proof. Since $p - 1 > d$, $A(K)[p]$ injects into $A(k)[p]$. Therefore, A has either ordinary reduction at p or nonordinary, nonsupersingular reduction at p. We consider two cases: when p is inert in $\mathbf{Q}(\sqrt{5})$ and when p splits in $\mathbf{Q}(\sqrt{5})$.

When p is inert, [1, Proposition 4.1] shows that the nonordinary locus of the moduli space of principally polarized abelian surfaces over k with real multiplication (and sufficiently large level structure) consists of supersingular abelian surfaces. Thus we may assume that A has ordinary reduction at p. From Proposition 3.10 we see that the restriction of the p-torsion Galois representation of A to a decomposition group at p has

the form

$$\begin{pmatrix} \varepsilon\chi^{-1} & * \\ 0 & \chi \end{pmatrix}$$

where ε is the cyclotomic character, χ is an unramified character, and $*$ is either trivial or wildly ramified. The assumption $d < p-1$ implies that K is not wildly ramified. Therefore, $*$ is trivial on $\mathrm{Gal}(\overline{\mathbf{Q}_p}/K)$ if and only if it is trivial on $\mathrm{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$. But μ_p is not contained in K (since $d < p-1$), so ε is nontrivial on $\mathrm{Gal}(\overline{\mathbf{Q}_p}/K)$. Hence the only way $A(K)[p] \neq 0$ is if χ factors through $\mathrm{Gal}(K/\mathbf{Q}_p)$ and $*$ is trivial on $\mathrm{Gal}(\overline{\mathbf{Q}_p}/K)$ and, hence, on $\mathrm{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$. Finally, since χ is unramified, it must actually factor through $\mathrm{Gal}(K^{\mathrm{ur}}/\mathbf{Q}_p)$, showing that $A(K^{\mathrm{ur}})[p] \neq 0$.

When p splits, the p-torsion Galois representation injects into $\mathrm{GL}_2(\mathbf{F}_p) \times \mathrm{GL}_2(\mathbf{F}_p)$ (Corollary 3.4). This reflects that fact that $A[p]$ splits as the sum of two Galois-modules $V_1 \oplus V_2$. Moreover, since $A(K)[p] \neq 0$, at least one of the V_i's must contain a nontrivial p-torsion point over K. Composing the representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p) \times \mathrm{GL}_2(\mathbf{F}_p)$ with the projection onto each V_i gives a representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p)$.

Without loss of generality, assume that V_1 has a nontrivial p-torsion point defined over K (if not, relabel the V_i's so that V_1 contains such a point). Recall that $A(K)[p]$ injects into $A(k)[p]$ since $d < p-1$. Thus an argument identical to the proof of Proposition 3.10 shows that, when restricted to a decomposition group at p, the representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p)$ associated with V_1 has the form

$$\begin{pmatrix} \varepsilon\chi^{-1} & * \\ 0 & \chi \end{pmatrix}$$

where ε is the cyclotomic character, χ is an unramified character, and $*$ is either trivial or wildly ramified. So if a nontrivial point in $A(K)[p]$ lies in V_1, the same argument used in the ordinary case shows that it is in fact defined over K^{ur}. $\diamond$

CHAPTER 5

MODULI SPACE FOR ABELIAN SURFACES WITH REAL MULTIPLICATION BY $\mathbf{Q}(\sqrt{5})$

We begin with some generalities on moduli problems. In broad terms, a moduli problem describes families of objects over a base scheme S up to some sort of equivalence. For example, families in our moduli problem will be the quadruplet $(A/S, \lambda, i, (\alpha_1, \alpha_2))$ where

- A/S is an abelian scheme of relative dimension 2,
- λ is a principal polartization (see Definition 4.2),
- $i : \mathfrak{o} \hookrightarrow \mathrm{End}(A)$ is a homomorphism such that $\lambda^{-1} i^{\vee}(\alpha)\lambda = i(\alpha)$ for all $\alpha \in \mathfrak{o}$ and such that $\mathrm{Lie}(A)$ is a locally free $\mathfrak{o} \otimes \mathcal{O}_S$-module of rank 1,
- (α_1, α_2) defines a level-$\sqrt{5}$ structure (see Definition 5.4).

We will consider two such quadruplets, say $(A/S, \lambda, i, (\alpha_1, \alpha_2))$ and $(A'/S, \lambda', i', (\alpha_1', \alpha_2'))$, equivalent if A with its extra structure is isomorphic over S to A' with its extra structure.

Given this information about families over S and a equivalence relation, define the functor

$$\mathbf{F}(S) = \{\text{families of objects over } S\}/\sim .$$

The first thing to investigate about this functor is its representability. Meaning, is it represented by a scheme? If not, in what category is $\mathbf{F}$ representable?

Definition 5.1 *If* $\mathbf{F}$ *is represented by a scheme* M *then call* M *a* fine moduli space *for the moduli problem.*

Given a fine moduli scheme M, let $X \to M$ be the family corresponding to the identity map $\mathbf{1} : M \to M$ in $\mathrm{Hom}(M, M)$. Then X satisfies the universal property that given any family $\varphi : A \to S$, there is a unique morphism $\psi : S \to M$ such that A is the fiber-product of X with S:

$$\begin{array}{ccc} A & \longrightarrow & X \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\mathbf{1}} \\ S & \xrightarrow{\psi} & M. \end{array}$$

We call X the *universal family*. Ideally, we want a fine moduli space since then we can use information about the geometry of M to answer questions about the geometry of the families of interest (and vice versa) via this dictionary given by the universal family.

Unfortunately, there is no guarantee that a fine moduli space exists for a given moduli problem. That is, the functor $\mathbf{F}$ may not be representable in the category of schemes. There are several approaches to getting around this obstruction. For example, we could try to determine if $\mathbf{F}$ is representable in a more general category, such as algebraic spaces or algebraic stacks. Such a strategy has the advantage of retaining the universal properties just mentioned, but at the cost of greater technical difficulties in carrying out geometric investigations. A different idea is to weaken the requirement of representability so that one gets "just enough" information about $\mathbf{F}$ while still working within the category of schemes.

Definition 5.2 *Let* M *be a scheme and let* $\Psi : \mathbf{F} \to \mathrm{Hom}(-, M)$ *be a natural transformation from* $\mathbf{F}$ *to the functor of points of* M*. Call the pair* (M, Ψ) *a* coarse moduli space *if*

- *for any algebraically closed field* Ω*, the map* $\Psi_{\mathrm{Spec}\,\Omega} : \mathbf{F}(\Omega) \to \mathrm{Hom}(\mathrm{Spec}\,\Omega, M)$ *is a bijection of sets,*
- *given another scheme* M' *and natural transformation* $\Psi' : \mathbf{F} \to \mathrm{Hom}(-, M')$*, there*

is a unique morphism $\pi : M \to M'$ *such that the associated natural transformation* $\Pi : \mathrm{Hom}(-, M) \to \mathrm{Hom}(-, M')$ *satisfies* $\Psi' = \Pi \circ \Psi$.

Remark 5.3 *It is a straightforward exercise to show that if a coarse moduli space* M *exists then it is unique up to canonical isomorphism. Furthermore, in conformance with the general convention, we drop the natural transformation* Ψ *from the notation and just refer to* M *as the coarse moduli space, leaving* Ψ *implicit.*

Returning to our specific moduli problem of the quadruplet $(A/S, \lambda, i, (\alpha_1, \alpha_2))$, it is known that a coarse moduli scheme $M_{\sqrt{5}}$ over $\operatorname{Spec} \mathbf{Z}[1/5]$ exists for this moduli problem. Therefore, to show that $M_{\sqrt{5}}$ is a fine moduli scheme, it suffices to check that families do not have any nontrivial automorphisms. Before doing so, however, we define the concept of a level-$\sqrt{5}$ structure.

Definition 5.4 *Let* δ *be a root of* $x^2 - 5$ *and let* A/S *be as in our moduli problem. A* level-$\sqrt{5}$ structure *on* A *is a pair of sections* $\alpha_1, \alpha_2 : S \to A$ *such that*

1. *for all geometric points* $s \in S$*, the images* $\alpha_1(s)$*,* $\alpha_2(s)$ *form a basis of the group scheme* $A_s[\delta] := \ker(\psi_\delta)$ *where* $A_s = A \times s$ *is the fiber of* A *over* s*,*

2. $\psi_\delta \circ \alpha_j = e$ *where* $\psi_\delta = i(\delta) : A \to A$ *is the multiplication by* δ *morphism and* $e : S \to A$ *is the identity section.*

Following the argument in [20], we now show that $M_{\sqrt{5}}$ is in fact a fine moduli space.

Proposition 5.5 *The quadruplet* $(A/S, \lambda, i, (\alpha_1, \alpha_2))$ *has no nontrivial automorphisms.*

Proof. Since any nontrivial automorphism of a family over S induces a nontrivial automorphism over a point $s = \operatorname{Spec} K$ of S (for some field K not of characteristic 5), it is enough to just consider the case $S = \operatorname{Spec} K$. Suppose θ is an automorphism of $(A/K, \lambda, i, (\alpha_1, \alpha_2))$. The strategy is to first show that θ^5 is the identity and then to use this plus some restrictions coming from the Tate module to force θ to be the identity.

To see that θ^5 is the identity, consider the exact sequence

$$0 \longrightarrow A[\delta] \longrightarrow A[5] \xrightarrow{\psi_\delta} A[\delta] \longrightarrow 0.$$

Since θ must fix $A[\delta]$, this sequence shows that we can choose a basis of $A[5]$ such that the action of θ on $A[5]$ is given by a matrix of the form

$$\begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Therefore, θ^5 is the identity on $A[5]$. This, however, implies that θ^5 is the identity automorphism.

Define the Tate module $T_\delta(A) = \varprojlim A[\delta^n]$. Note that $T_\delta(A)$ is free a $\mathbf{Z}_5(\delta)$-module of rank 2. Since θ commutes with multiplication by δ, the action of θ gives an element of $\mathrm{GL}_2(\mathbf{Z}_5(\delta))$ that reduces to the identity modulo δ. Moreover, since $\operatorname{char} K \neq 5$, there is an injection, $\mathrm{End}(A) \hookrightarrow \mathrm{End}(T_\delta(A))$. Hence, we may identify θ with a matrix $B \in \mathrm{GL}_2(\mathbf{Z}_5(\delta))$ such that B^5 is the identity and

$$B \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod \delta.$$

Finally, assume B is not the identity. This means $B = I + \delta^n C$ where I is the identity matrix, $n \geq 1$ and C is a matrix which is not a multiple of δ. Therefore,

$$I = B^5 = I + 5\delta^n C + 10\delta^{2n} C^2 + 10\delta^{3n} C^3 + 5\delta^{4n} C^4 + \delta^{5n} C^5.$$

But considering valuations gives a contradiction, so B must be the identity. $\diamond$

Let $\mathfrak{h}$ denote the complex upper half plane. Define

$$\Gamma(\delta) = \left\{ B \in \mathrm{SL}_2(\mathfrak{o}) : B \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod \delta \right\}.$$

Then the complex points of $M_{\sqrt{5}}$ can be identified with the Hilbert modular surface $\Gamma \backslash \mathfrak{h} \times \mathfrak{h}$ (see [20]).

Definition 5.6 *Let i' denote the composition*

$$\mathfrak{o} \xrightarrow{\ '\ } \mathfrak{o} \xrightarrow{\ i\ } \mathrm{End}_S(A)$$

where $' : \mathfrak{o} \to \mathfrak{o}$ is the Galois involution on $\mathfrak{o}$. Then define an involution $\dagger$ on $M_{\sqrt{5}}$ by $(A/S, \lambda, i, (\alpha_1, \alpha_2))^\dagger = (A/S, \lambda, i', (\alpha_1, \alpha_2))$.

It is straightforward to check that on complex points $\dagger$ gives the same action as the involution $(\tau_1, \tau_2) \mapsto (\tau_2, \tau_1)$ (see [20] for example). Moreover, just as we can compactify $\Gamma\backslash\mathfrak{h} \times \mathfrak{h}$ by adding six cusps, we can similarly construct a compactification $\overline{M_{\sqrt{5}}}$ of $M_{\sqrt{5}}$ by adding six cusps. Finally, Hirzebruch carried out a detailed study of $\overline{\Gamma\backslash\mathfrak{h} \times \mathfrak{h}}$ over $\mathbf{C}$ in [17] and Manoharmayum showed in [20] that Hirzebruch's argument works for $\overline{M}_{\sqrt{5}}$ over $\mathbf{Q}$. For our purposes, the main aspect of their work that we need is the following proposition.

Proposition 5.7 *The quotient $\overline{M_{\sqrt{5}}}/\dagger$ is isomorphic over $\mathbf{Q}$ to $\mathbf{P}^2$. Under this isomorphism, $\overline{M_{\sqrt{5}}}$ is a double cover of $\mathbf{P}^2$ and the six singular points of $\overline{M_{\sqrt{5}}}$ give a collection of six points of $\mathbf{P}^2$ defined over $\mathbf{Q}$.*

We conclude this chapter with the remark that since $\overline{M_{\sqrt{5}}}/\dagger$ and $\mathbf{P}^2$ are schemes of finite type over $\mathrm{Spec}\,\mathbf{Z}[1/5]$, the isomorphism $\overline{M_{\sqrt{5}}}/\dagger \to \mathbf{P}^2$ of Proposition 5.7 is actually defined over $\mathbf{Z}[1/N]$ for some $N \geq 1$. Therefore, in what follows, we will assume that all primes $p > \max\{5, N\}$.

CHAPTER 6

ANALYTIC METHODS

Continuing with the notation of Chapter 4, let k be a finite field of degree d, $W = W(k)$ its ring of Witt vectors, K the fraction field of W and $W_2 = W/p^2$. We will make heavy use of Proposition 5.7 in this chapter. Furthermore, it is clear from Definition 5.6 that one of the abelian surfaces in a fiber of the map given in Proposition 5.7 has a p-torsion point if and only if the other one does. Therefore, letting $[a : b : c]$ be homogeneous coordinates on $\mathbf{P}^2(\mathbf{Q})$ and letting $A_{[a:b:c]}$ be any abelian surface in the fiber over $[a : b : c]$, then it makes sense to define the set

$$\pi^d_{[a:b:c]}(x) = \#\{p \leq x : A_{[a:b:c]}(K)[p] \neq 0 \text{ and } [K : \mathbf{Q}_p] \leq d\}.$$

Finally, we defined a height function H on $\mathbf{P}^2(\mathbf{Q})$ by $H([a : b : c]) = \max\{|a|, |b|, |c|\}$ where, without loss of generality, $a, b, c \in \mathbf{Z}$ and $\gcd(a, b, c) = 1$.

Definition 6.1 *Let*

$$\nu_d(p) = \#\{[a : b : c] \in \mathbf{P}^2(\mathbf{Z}/p^2) : \operatorname{rank}_p A_{[a:b:c]} \geq 2d + 1\}.$$

A priori, this may not seem to be well-defined, but a straightforward check shows that $\operatorname{rank}_p A_{[a:b:c]}$ is independent of the choice of the abelian surface in the fiber over $[a : b : c]$.

Lemma 6.2 *We have*

(a) $\sum_{p \leq x} \nu_d(p) \ll x^4$,

(b) $\sum_{p \leq x} \frac{\nu_d(p)}{p^2} \ll x^2$,

(c) $\sum_{p \leq x} \frac{\nu_d(p)}{p^4} \ll 1$.

Proof. For (a), note that,

$$\nu_d(p) = \sum_{\substack{[a:b:c] \in \mathbf{P}^2(\mathbf{F}_p) \\ A_{[a:b:c]}(k)[p] \neq 0}} \#(\text{lifts of } A_{[a:b:c]} \text{ over } \mathbf{F}_p \text{ to } \mathbf{Z}/p^2 \text{ with } \operatorname{rank}_p \geq 2d+1)$$

where k is the finite field of degree d over $\mathbf{F}_p$. In particular, Lemmas 4.6 and 4.7 yield the bound $\nu_d(p) \leq (2p-1)(p^2+p+1)$, so

$$\sum_{p \leq x} \nu_d(p) \ll x^4.$$

The remaining bounds in (b) and (c) follow using partial summation. $\diamond$

Let $\pi^{d,\text{good}}_{[a:b:c]}(x)$ denote the number of $p \leq x$ such that $A_{[a:b:c]}$ has a p-torsion point over an extension of $\mathbf{Q}_p$ of degree at most d and such that $A_{[a:b:c]}$ has good reduction at p. Similarly, set

$$\pi^{d,\text{bad}}_{[a:b:c]}(x) = \#\{p \in \pi^d_{[a:b:c]}(x) : A_{[a:b:c]} \text{ has bad reduction at } p\}.$$

So we now have

$$\pi^d_{[a:b:c]}(x) = \pi^{d,\text{good}}_{[a:b:c]}(x) + \pi^{d,\text{bad}}_{[a:b:c]}(x).$$

Lastly, recall that

$$S_M = \{[a:b:c] \in \mathbf{P}^2(\mathbf{Q}) : H([a:b:c]) \leq M\}.$$

We are now ready to prove Theorem 1.2, which we now restate.

Theorem 6.3 *If $M \geq x^{4/3+\varepsilon}$ for some $\varepsilon > 0$ then*

$$\frac{1}{\#S_M} \sum_{[a:b:c] \in S_M} \pi^d_{[a:b:c]}(x) \ll d \text{ as } x \to \infty.$$

Proof. Lemma 4.8 implies that

$$\begin{aligned}\frac{1}{\#S_M}\sum_{[a:b:c]\in S_M}\pi^{d}_{[a:b:c]}(x) &= \frac{1}{\#S_M}\sum_{[a:b:c]\in S_M}\pi^{d,\text{good}}_{[a:b:c]}(x)+\pi^{d,\text{bad}}_{[a:b:c]}(x)\\ &= \frac{1}{\#S_M}\left(\sum_{[a:b:c]\in S_M}\pi^{d,\text{ur}}_{[a:b:c]}(x)+d\cdot O(1)+\sum_{[a:b:c]\in S_M}\pi^{d,\text{bad}}_{[a:b:c]}(x)\right),\end{aligned}$$

where $\pi^{d,\text{ur}}_{[a:b:c]}(x)$ denotes the number of $p \le x$ such that $A_{[a:b:c]}$ has a p-torsion point over an unramified extension of $\mathbf{Q}_p$ of degree at most d and such that $A_{[a:b:c]}$ has good reduction at p. Furthermore, it is relatively easy to show that the sum

$$\frac{1}{\#S_M}\sum_{[a:b:c]\in S_M}\pi^{d,\text{bad}}_{[a:b:c]}(x)$$

is analytically irrelevant. Indeed, for the primes of bad reduction, note that the six cusps of $\overline{M_{\sqrt{5}}}$ correspond to six points in $\mathbf{P}^2$ where there is no moduli interpretation (see [20]). That is, $A_{[a:b:c]}$ will have bad reduction at p if and only if $[a:b:c]$ reduces to a point in $\mathbf{P}^2(\mathbf{F}_p)$ corresponding to a cusp of $\overline{M}_{\sqrt{5}}(\mathbf{F}_p)$. With this in mind, let

$$\pi^{d,\text{bad}}_p := \#\{[a:b:c]\in S_M : A_{[a:b:c]}(K)[p]\neq 0, [K:\mathbf{Q}_p]\le d, A_{[a:b:c]} \text{ has bad reduction at } p\}.$$

Assume that $A_{[a:b:c]}(K)[p]\neq 0$ whenever $A_{[a:b:c]}$ has bad reduction at p, and that $(2M/p+O(1))^3$ points in S_M reduce to a given point in $\mathbf{P}^2(\mathbf{F}_p)$. Then even with these most naive assumptions, reversing the order of summation gives

$$\begin{aligned}\frac{1}{\#S_M}\sum_{[a:b:c]\in S_M}\pi^{d,\text{bad}}_{[a:b:c]}(x) &= \frac{1}{\#S_M}\sum_{p\le x}\pi^{d,\text{bad}}_p\\ &\le \sum_{p\le x}\frac{6(2M/p+O(1))^3}{\#S_M}.\end{aligned}$$

Since $\#S_M = M^3/\zeta(3)+O(M^2)$ (see [30]), this is clearly finite as $x\to\infty$.

For the sum

$$\frac{1}{\#S_M}\sum_{[a:b:c]\in S_M}\pi^{d,\text{ur}}_{[a:b:c]}(x),$$

let K_{d_0} be the unramified extension of $\mathbf{Q}_p$ of degree d_0 and let $\widetilde{\pi}^{d_0}_{[a:b:c]}(x)$ denote the number of primes $p\le x$ such that $A_{[a:b:c]}(K_{d_0})[p]\neq 0$ and $A_{[a:b:c]}$ has good reduction at

p. Let

$$\pi_p^{d_0,\text{good}} := \#\{[a:b:c] \in S_M : A_{[a:b:c]}(K_d)[p] \neq 0, A_{[a:b:c]} \text{ has good reduction at } p\}.$$

Finally, note the naive estimate that $(2M/p^2+O(1))$ points in S_M reduce to a given point in $\mathbf{P}^2(\mathbf{Z}/p^2)$. Then reversing the order of summation and applying Lemma 4.1 gives

$$\begin{aligned}
\frac{1}{\#S_M}\sum_{S_M}\widetilde{\pi}^{d_0}_{[a:b:c]}(x) &= \frac{1}{\#S_M}\sum_{p\le x}\pi_p^{d_0,\text{good}} \\
&\le \frac{1}{\#S_M}\sum_{p\le x}\left(\frac{2M}{p^2}+O(1)\right)^3\nu_{d_0}(p) \\
&= \frac{1}{\#S_M}\left(\sum_{p\le x}\frac{8M^3\nu_{d_0}(p)}{p^6}+O\left(\sum_{p\le x}\frac{4M^2\nu_{d_0}(p)}{p^4}+\sum_{[a:b:c]}\frac{2M\nu_{d_0}(p)}{p^2}+\sum_{p\le x}\nu_{d_0}(p)\right)\right).
\end{aligned}$$

Therefore, combining Schanuel's result that $\#S_M = M^3/\zeta(3)+O(M^2)$ with the estimates of Lemma 6.2 and summing over $d_0 \le d$ yields the theorem. $\diamond$

A P P E N D I X

SMOOTH HONDA SYSTEMS

Let k be a finite field of characteristic $p > 2$. Following the notation of [13], set $A = W(k)$, the ring of Witt vectors of k and let K be its field of fractions. Let A' denote the ring of the integers of a totally ramified extension of K of ramification index $e < p-1$. Finally, let $\mathfrak{m}$ be the maximal ideal of A' and set $A'_n = A'/\mathfrak{m}^n$.

As mentioned in Chapter 2, another way to classify the Barsotti-Tate groups of interest is via smooth Honda systems. In the mid-1970s, Fontaine [13] developed a dictionary between smooth finite dimensional formal p-groups over A' and the category $\Lambda^{\ell}_{A'}$ (see Definition A.17) by associating a triple of linear algebra data to such groups. Recently, Brian Conrad [7] and Berbec [2] respectively generalized Fontaine's construction to give a classification of finite flat group schemes over A' and a classification of smooth finite dimensional formal p-groups over A'_n via analogous categories of triples. Moreover, assuming $e = 1$ and restricting to the category of Barsotti-Tate groups over A_n, Berbec's functor gives an anti-equivalence with smooth Honda systems over A_n (see Corollary A.22), which recovers the Grothendieck-Messing crystalline Dieudonné functor from Chapter 2. The purpose of this appendix is to give a brief overview of the results of Fontaine and Berbec.

Remark A.1 *We chose to present our algebraic results of Chapter 4 using the language of Dieudonné crystals since this seemed better suited to the real multiplication condition and was how we originally obtained our lifting results. However, in light of the fact that Berbec's results recover the crystalline functor in the case of interest, Lemmas 4.3 and*

4.6 also follow from slight modifications of our arguments and Berbec's classification of Barsotti-Tate groups over A_n. For more on the connection between Fontaine's functor and the Grothendieck-Messing functor see the final section of [23].

Remark A.2 *The constraint $e < p - 1$ on ramification can be seen as coming from convergence issues of the p-adic logarithm on $\mathfrak{m}$. Although Fontaine does not use this explicitly, the failure of his methods for large e relates to the failure of torsion points over A' to inject to the torsion points of the closed fiber.*

Definition A.3 *A* pseudo-compact *ring S is a separated and complete linearly topologized ring such that the quotient S/I is artinian for all open ideals I of S.*

Example A.4 *The rings k (with the discrete topology), A' and A'_n (with the p-adic topology) are pseudo-compact.*

Definition A.5 *Let $(S, \mathfrak{m})$ be a local pseudo-compact ring with residue field of characteristic p.*

- *A* formal S-group functor *is a functor defined on finite S-algebras with values in abelian groups. (Note that this means that all our group schemes are commutative.)*
- *A* formal S-group *is a pro-representable formal S-group functor. Moreover, we say a formal S-group G is* smooth *if for all finite S-algebras R and all square zero ideals I of R, the canonical map from $G(R)$ to $G(R/I)$ is surjective.*
- *A* formal p-group *G over S is a formal S-group such that $G \cong \varinjlim G[p^n]$.*
- *Call a smooth formal p-group G over S p-*faithful *if the "multiplication-by-p" morphism $[p] : G \to G$ is faithfully flat.*

Remark A.6 *The primary example of a p-faithful smooth formal p-group to keep in mind is a Barsotti-Tate group over A' or A'_n.*

Let R be a finite k-algebra. Define the R-valued *Witt covectors*, $CW_k(R)$, to be the set of sequences $(\ldots, a_{-n}, \ldots, a_0)$ of elements $a_{-n} \in R$ indexed by non-positive integers $-n$ with a_{-n} nilpotent for large n. Let $S_m =\in \mathbf{Z}[X_0, \ldots, X_m, Y_0, \ldots, Y_m]$ denote the mth addition polynomial for Witt vectors. Then choosing $\mathbf{a}$ and $\mathbf{b}$ in $CW_k(R)$, the nilpotence condition on elements of $CW_k(R)$ implies that the sequence

$$\{S_m(a_{-n-m}, \ldots, a_{-n}, b_{-n-m}, \ldots, b_{-m})\}_{m \geq 0}$$

is stationary. Denote its limit by c_{-n}. Then $\mathbf{c} := (c_{-n})$ is in $CW_k(R)$. Moreover, defining $\mathbf{a} + \mathbf{b} = \mathbf{c}$ makes $CW_k(R)$ into a commutative group with identity $(\ldots, 0, \ldots, 0)$.

Remark A.7 *For some intuition, think of the Witt covectors as being analogous to* $\mathbf{Q}_p/\mathbf{Z}_p$. *In fact, if* k' *is a finite extension of* k *then* $CW_k(k') = K'/W(k')$ *where* K' *is the field of fractions of* $W(k')$.

There is a natural topology on $CW_k(R)$ coming from viewing it as a subset of the product space $\prod_{n \leq 0} R$ where each factor has the discrete topology. In fact, it admits a unique topological A-module structure such that for all $x \in k$ with Teichmüller lift $[x] \in A$,

$$[x] \cdot \mathbf{a} = (\ldots, x^{p^{-n}} a_{-n}, \ldots, x^{p^{-1}} a_{-1}, a_0).$$

Moreover, $CW_k(R)$ can be made into a topological D_k-module with F and V operators given by

$$F(\mathbf{a}) = (\ldots, a_{-n}^p, \ldots, a_0^p) \text{ and } V(\mathbf{a}) = (\ldots, a_{-n-1}, \ldots, a_{-1}).$$

This means that F and V are additive, continuous with respect to the topological A-module structure, satisfy $FV = VF = p$ and are σ and σ^{-1}-semi-linear respectively where $\sigma : A \to A$ is the Frobenius morphism. Finally, it is important to note that all of this is functorial in R, so CW_k is a functor from k-algebras to topological D_k-modules.

The functor CW_k on finite k-algebras is pro-represented by a group scheme, which we denote by $\widehat{CW}_k$. For complete local noetherian A-algebras, R, define

$$\widehat{CW}_A(R) = \varprojlim CW_k(R/\mathfrak{m}_R^n)$$

where $\mathfrak{m}_R$ is the maximal ideal of R. This is a Hausdorff topological D_k-module and it is functorial in R. As it turns out, if the residue field of such R is a field extension of k then $\widehat{CW}_k(R) = \widehat{CW}_A(R)$.

Remark A.8 *When R is any separated and complete topological A-module with a base of open ideals, one can similarly define $\widehat{CW}_A(R)$. There are, however, some subtleties that arise from the interaction between the product topology and the direct limit topology.*

Definition A.9 *Let G be a formal p-group over k. Then the* Dieudonné module *of G is*

$$\mathcal{M}(G) := \mathrm{Hom}(G, \widehat{CW}_k),$$

the group of formal k-group scheme morphisms $G \to \widehat{CW}_k$.

Remark A.10 *Similar to the construction of CW_k, one can think of the definition of the Dieudonné module of a formal p-group as being analogous to the functor*

$$G \mapsto \mathrm{Hom}(G, \mathbf{C}^\times) \cong \mathrm{Hom}(G, \mathbf{Q}_p/\mathbf{Z}_p)$$

for finite abelian p-groups G.

The D_k-action on CW_k induces a D_k-action on $\mathcal{M}(G)$. Moreover, one can show that, with respect to a suitable topology, $\mathcal{M}(G)$ is a topological D_k-module.

Definition A.11 *An $A[F]$-profinite D_k-module is a (left) D_k-module with a profinite $A[F]$-module structure on which V acts continuously.*

The following generalization of Theorem 2.4 is the main result of this theory. As indicated by Theorem 2.6, however, there are many specializations of this result.

Theorem A.12 *The functor $G \mapsto \mathcal{M}(G)$ is an anti-equivalence between the category of formal p-groups over k and $A[F]$-profinite D_k-modules.*

Remark A.13 *Proofs of the various statements about Witt covectors and Theorem A.12 may be found in chapters 2 and 3 of [13].*

The main result of [13] augments the Dieudonné module theory with additional linear algebra data that classifies formal p-groups over A'. We now describe this enhancement.

Let M be a D_k-module. Let $M^{(1)}$ be the D_k-module whose underlying space is M with A-action given by $a \cdot x = \sigma^{-1}(a)x$ for all $a \in A$ and $x \in M$. The operators F and V act on $M^{(1)}$ as before. Thus we can view F and V as A-linear maps

$$M \xrightarrow{V} M^{(1)} \text{ and } M^{(1)} \xrightarrow{F} M.$$

Definition A.14 *Define $M_{A'}$ to be the direct limit of the diagram*

$$\begin{array}{ccc} \mathfrak{m} \otimes_A M & \xrightarrow{V_1} & p^{-1}\mathfrak{m} \otimes_A M^{(1)} \\ {\scriptstyle \varphi_0}\downarrow & & \uparrow{\scriptstyle \varphi_1} \\ A' \otimes_A M & \xleftarrow{F_1} & A' \otimes_A M^{(1)} \end{array}$$

where the vertical maps are the obvious "inclusions," $V_1(\lambda \otimes x) = p^{-1}\lambda \otimes V(x)$ and $F_1(\lambda \otimes x) = \lambda \otimes F(x)$.

More concretely, $M_{A'}$ is the quotient of $A' \otimes_A M \oplus p^{-1}\mathfrak{m} \otimes_A M^{(1)}$ by the submodule

$$\left\{(\varphi_0(u) - F_1(w), \varphi_1(w) - V_1(u)) : u \in \mathfrak{m} \otimes_A M, w \in A' \otimes_A M^{(1)}\right\}.$$

Furthermore, denoting the image of the projection $p^{-1}\mathfrak{m} \otimes_A M^{(1)} \to M_{A'}$ by $M_{A'}[1]$, Fontained proved that $M_{A'}/M_{A'}[1] \cong M/FM$ as k-vector spaces.

Let G be a formal p-group over A' and let R be its affine algebra. Denote the affine algebra of its closed fiber G_k by $R_k := R \otimes_{A'} k \cong R/\mathfrak{m}R$ and denote the affine algebra of its generic fiber G_K by $R_K := R \otimes_A K \cong R \otimes_{A'} K'$ where K' is the field of fractions of A'. For $s \geq 1$, set $J_s = \sum_{i=1}^{\infty} p^{-i+1}\mathfrak{m}^{is}$ and define $R_K^{an} = \varprojlim R_K/J_s$. Lastly, let $\Omega_{A'}(R)$ be the module of continuous A'-differentials of R and define

$$P(R) = \{\alpha \in R_K^{an} : d(\alpha) \in \Omega_{A'}(R)\}$$

where $d : R_K^{an} \to \Omega_{A'}(R_K^{an})$ is the canonical morphism.

Thinking of R as an A-algebra, Fontaine constructed a continuous A-linear map $\widehat{w}_R : CW_A(R) \to P(R)$ defined by

$$\widehat{w}_R(\ldots, a_{-n}, \ldots, a_0) = \sum_{n=0}^{\infty} p^{-n} a_{-n}^{p^n}.$$

Moreover, $\widehat{w}_R(CW_A(\mathfrak{m}R)) \subset \mathfrak{m}R$ (since $e < p-1$), so we get an induced A-linear continuous map $CW_k(R_k) \to P(R)/\mathfrak{m}R$. Then, by extension of scalars, there is an induced continuous A'-linear homomorphism $A' \otimes_A CW_k(R_k) \to P(R)/\mathfrak{m}R$. Finally, Fontaine uses this to get a continuous A'-linear isomorphism

$$w_R : CW_{k,A'}(R_k) := (CW_k(R_k))_{A'} \to P(R)/\mathfrak{m}R.$$

Denote the comultiplication of R by Δ and, abusing notation, let Δ also denote the comultiplication of R_K^{an}. For $\alpha \in R_K^{an}$, set $\delta(\alpha) = \alpha \widehat{\otimes} 1 + 1 \widehat{\otimes} \alpha - \Delta(\alpha)$. Define

$$\mathcal{L} = \{\alpha \in P(R) : \delta(\alpha) = 0\} \text{ and } \mathcal{L}_1 = \{\alpha \in P(A) : \delta(\alpha) \in \mathfrak{m}R \otimes_{A'} R\}.$$

Note that we can realize $\mathcal{M}(G_k)$ as a subset of $CW_k(R_k)$ by viewing the formal k-group scheme morphisms $G_k \to \widehat{CW}_k$ as just formal k-scheme morphisms. Then Fontaine gives the following result relating $\mathcal{M}(G_k)_{A'}$ and $\mathcal{L}_1$.

Proposition A.15 *There is an injection of A'-modules $\mathcal{M}(G_k)_{A'} \hookrightarrow CW_{k,A'}(R_k)$ induced from the inclusion $\mathcal{M}(G_k) \subset CW_k(R_k)$. Furthermore, w_R gives an A'-linear isomorphism $\mathcal{M}(G_k)_{A'} \to \mathcal{L}_1/\mathfrak{m}R$.*

Definition A.16 *Call a D_k-module that is A-profinite and is such that its open D_k-submodules form a fundamental system of neighborhoods of zero a* profinite D_k*-module.*

We now describe the category $\Lambda_{A'}^{\ell}$.

Definition A.17 *Let $\Lambda_{A'}^{\ell}$ be the category of triples (L, M, ρ) where*

- *M is a profinite D_k-module on which the action of F is injective and such that the quotient M/FM is a finite dimensional k-vector space,*

- *L is a free A'-module of finite rank,*
- *$\rho : L \to M_{A'}$ is an A'-linear homomorphism such that the induced homomorphism $\overline{\rho} : L/\mathfrak{m}L \to M_{A'}/M_{A'}[1] \xrightarrow{\sim} M/FM$ is an isomorphism of k-vector spaces*
- *and the morphisms are the obvious ones.*

For a smooth finite dimensional formal p-group G over A', Fontaine defined an additive functor $\mathcal{L}M_{A'}(G) = (\mathcal{L}, \mathcal{M}(G_k), \rho_G)$ where ρ_G is the composition

$$\mathcal{L} \hookrightarrow \mathcal{L}_1 \to \mathcal{L}_1/\mathfrak{m}R \xrightarrow{\sim} \mathcal{M}(G_k)_{A'}.$$

The next theorem is the main result of [13].

Theorem A.18 *The functor $\mathcal{L}M_{A'}$ is an anti-equivalence of categories between $\Lambda^{\ell}_{A'}$ and the category of smooth finite dimensional formal p-groups over A'.*

Let $H^d_{A'}$ denote the category of pairs (L, M) where

- M is as in Definition A.17 and, is moreover, a free A-module of finite rank,
- L is a free A'-submodule of $M_{A'}$ such that $L/\mathfrak{m}L \cong M_{A'}/M_{A'}[1] \cong M/FM$.

Such a pair is called a *smooth Honda system* over A'. For a Barsottie-Tate group G over A', Fontaine showed that $LM_{A'}(G) = (L(G), \mathcal{M}(G_k))$ where $L(G) = \rho_G(\mathcal{L})$ defines an additive functor into $H^d_{A'}$. Then restricting to the subcategory of Barsotti-Tate groups over A', we have the following corollary.

Corollary A.19 *The functor $LM_{A'}$ is an anti-equivalence of categories between $H^d_{A'}$ and the category of Barsotti-Tate groups over A'.*

Remark A.20 *We use the term anti-equivalence in the same sense as Fontaine. That is, $\mathcal{L}M_{A'}$ and $LM_{A'}$ are essentially surjective and fully faithful. We repeat this usage in Theorem A.21 and Corollary A.22.*

Analogous to Fontaine's work, Berbec defined a category $\Lambda^f_{A'_n}$ of triples (L_n, M, ρ) where

- M is a profinite D_k-module on which the action of F is injective, the "multiplication by p" map on M is injective, and such that the quotient M/FM is a finite dimensional k-vector space,
- L_n is a free A'_{n-1}-module,
- $\rho : L_n \to M_{A'}/\mathfrak{m}^{n-1}M_{A'}$ is an A'_{n-1}-linear homomorphism such that the induced homomorphism

$$\overline{\rho} : L_n/\mathfrak{m}L_n \to M_{A'}/\mathfrak{m}M_{A'} \to M_{A'}/M_{A'}[1] \xrightarrow{\sim} M/FM$$

  is an isomorphism of k-vector spaces.

Let G be a smooth finite dimensional formal p-faithful groups over A'_n and let R be its affine algebra. Let $\mathcal{R}$ be a smooth A'-lift of R (which is unique up to non-unique isomorphism). Berbec generalizes Fontaine's $\mathcal{L}M_{A'}$ by defining a functor $\mathcal{L}M_n$ from the category of smooth formal p-groups over A'_n to $\Lambda^f_{A'_n}$ as follows. Define the submodule $\mathcal{L}_n := \{\alpha \in P(\mathcal{R}) : \delta(\alpha) \in \mathfrak{m}^n\mathcal{R}\widehat{\otimes}_{A'}\mathcal{R}\}$. Then he uses the composition

$$\mathcal{L}_n \hookrightarrow \mathcal{L}_1 \to \mathcal{L}_1/\mathfrak{m}\mathcal{R} \xrightarrow{\sim} M_{A'} \tag{A.1}$$

to construct an injective map

$$\varphi_n : \mathcal{L}_n/\mathfrak{m}^{n-1}\mathcal{L}_1 \to A'\widehat{\otimes}_A CW_A(R)/\mathcal{K}$$

where $\mathcal{K}$ is the kernel of a surjective map $A'\widehat{\otimes}_A CW_A(R) \to P(\mathcal{R})/\mathfrak{m}^{n-1}P(\mathcal{R})$. In fact, he shows that $\mathcal{K}$ is independent of the lift $\mathcal{R}$, so that the image L_n of φ_n is functorial. Moreover, from the composition (A.1), there is an induced map $\rho : L_n \to M_{A'}/\mathfrak{m}^{n-1}M_{A'}$.

Let $\mathcal{L}M^f_n(G) := (L_n, \mathcal{M}(G_k), \rho)$ where L_n and ρ are as we just discussed and $\mathcal{M}(G_k)$ is the Dieudonné module of the closed fiber G_k of G. Then the main result of [2] is the following theorem.

Theorem A.21 *The functor $\mathcal{L}M_n^f$ is an anti-equivalence of categories between $\Lambda^f_{A'_n}$ and the category of smooth finite dimensional formal p-faithful groups over A'_n.*

As with Barsotti-Tate groups over A', we also have a corollary about classifying Barsotti-Tate groups over A'_n. Let $H^d_{A'_n}$ denote the full subcategory of $\Lambda^f_{A'_n}$ whose objects are pairs (L_n, M) where M and L_n are as in the definition of $\Lambda^f_{A'_n}$ and additionally satisfy the conditions that

- M is a free A-module,
- $L_n \subset M_{A'}/\mathfrak{m}^{n-1}M_{A'}$.

Call objects of $H^d_{A'_n}$ *smooth Honda systems* over A'_n. Then, for a Barsotti-Tate group G over A'_n, defining $LM^d_n(G) := (\rho(L_n), \mathcal{M}(G_k))$ gives a functor into $H^d_{A'_n}$. Furthermore, Theorem A.21 shows that LM^d_n classifies Barsotti-Tate groups over A'_n.

Corollary A.22 *The functor LM^d_n gives an anti-equivalence of categories between $H^d_{A'_n}$ and the category of Barsotti-Tate groups over A'_n.*

BIBLIOGRAPHY

[1] E. Bachmat and E.Z. Goren, *On the non ordinary locus in Hilbert-Blumenthal surfaces*, Math. Ann. **313** (1999), 475 - 506.

[2] I. Berbec, *Group schemes over artinian rings and applications*, Ann. de L'Institut Fourier **59**, 6 (2009), 2371 - 2427.

[3] P. Berthelot, L. Breen, W. Messing, *Theorie de Dieudonné cristalline II*, Lecture Notes in Mathematics **930**, Springer Verlag, 1982.

[4] P. Berthelot, W. Messing, *Theorie de Dieudonné cristalline III: theoremes d'equivalence et pleine fidelite*, in Grothendieck Festschrift, vol I, 173 - 247, Progress in Mathematics **86**, Birkhäuser Verlag, 1990.

[5] L. Breen, *Rapport sur la theorie de Dieudonne*, Asterisque, **63** (1979), 39 - 66.

[6] B. Conrad, *The flat deformation functor* in *Modular forms and Fermat's last theorem*, Springer-Verlag, 1997.

[7] B. Conrad, *Finite group schemes over bases with low ramification*, Compositio Math. **119** (1999), no. 3, 239 - 320.

[8] C. David and T. Weston, *Local torsion on elliptic curves and the deformation theory of Galois representations*, Mathematical Research Letters, **15** (2008), 599 - 611.

[9] M. Demazure, *Lectures on p-divisible groups*, Lecture Notes in Mathematics **302**, Springer-Verlag, Berlin, 1972. MR 0344261 (49 #9000)

[10] M. Demazure and P. Gabriel, *Groupes algebriques*, Tome I: Géométrie algébrique, généralités, groupes commutatifs, Masson & Cie, Éditeur, Paris, 1970, Avec un appendice t Corps de classes local par Michiel Hazewinkel. MR 0302656 (46 #1800)

[11] F. Diamond, M. Flach, L. Guo, *Adjoint motives of modular forms and the Tamagawa number conjecture*, preprint.

[12] M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, Invent. Math. **109** (1992), 307 - 327.

[13] J-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Astérisque **47 - 48**, Soc. Math. de France, 1977.

[14] F. Q. Gouvea, *Deformations of Galois representations* in *Arithmetic Algebraic Geometry*, American Mathematical Society, 2001.

[15] A. Grothendieck, *Groupes de Barsotti-Tate et cristaux*, Actes du Congrés International des Mathèmaticiens **1** (1970) 431-436. Gauthier-Villars, Paris, 1971.

[16] A. Grothendieck. *Groupes de Barsotti-Tate et Cristaux de Dieudonné*. Les Presses de l'Universite de Montreal, 1974.

[17] F. Hirzebruch, *The ring of Hilbert modular forms for real quadratic fields of small discriminant*, in Modular Functions of One Variable VI, J.-P. Serre and D. B. Zagier, ed., Springer-Verlag, Berlin, Heidelberg, (1977) 287 - 323.

[18] F. Hirzebruch and G. van der Geer, *Lectures on Hilbert modular surfaces*, Les Presses de l'Universite de Montreal, 1981.

[19] N. Katz, *Serre-Tate local moduli*, in *Surfaces algébriques (Orsay, 1976-78)*, Lecture Notes in Math. **868**, Springer-Verlag, Berlin-New York, 1981.

[20] J. Manoharmayum, *Abelian surfaces with level* $\sqrt{5}$ *structure*, Asian J. Math. **3** (1999), 677 - 688.

[21] B. Mazur, *Deforming Galois representations*, in: *Galois Groups over* **Q** *(Berkeley, 1987)*, MSRI Publ. **16**, Springer, New York, 1989.

[22] B. Mazur, *An "infinite fern" in the universal deformation space of Galois representations*, Collect. Math. **48** (1997), 155 - 193.

[23] B. Mazur and W. Messing, *Universal Extensions and One Dimensional Cristalline Cohomology*, Springer Lecture Notes in Math. **370** (1974).

[24] W. Messing, *The Crystals Associated to Barsotti-Tate Groups: with applications to abelian schemes*, Springer Lecture Notes in Math. **264** (1972).

[25] D. Mumford, J. Fogarty, *Geometric Invariant Theory*, Springer-Verlag, Berlin, 1989.

[26] J.S. Milne, *Abelian varieties*, in *Arithmetic Geometry*, ed. G. Cornell and J. Silverman, Springer-Verlag (1986), 103 - 150.

[27] M-H. Nicole, *Cris is for Crystalline*, online seminar notes: www.math.mcgill.ca/goren/SeminarOnCohomology/Seminairecohomologie.pdf.

[28] J. Pottharst, *Minor Thesis: Basic Dieudonné Theory*, Harvard 2004. www.math.bu.edu/people/potthars/writings/minorthesis.pdf

[29] K. Ribet, *Galois action on division points of abelian varieties with real multiplication*, American J. of Math. **98**, No. 3, (1976), 751 - 804.

[30] S. Schanuel, *Heights in number fields*, Bulletin del S. M. F. **107** (1979), 433 - 449.

[31] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its application to number theory*, Math. Soc. Japan, Tokyo, 1961.

[32] J. Silverman, *Arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[33] J. Tate, *p-divisible groups*, Proceed. Conf. on Local Fields, Springer-Verlag, Berlin, 1967.

[34] G. van der Geer. *Hilbert modular surfaces*. Springer-Verlag, 1988.

[35] T. Weston, An overview of a theorem of Flach, appendix to *Deformations of Galois representations* by F.Q. Gouvea in *Arithmetic algebraic geometry*, American Mathematical Society, 2001.

[36] T. Weston, *Unobstructed modular deformation problems*, American J. Math. **126** (2004), 1237 - 1252.

[37] J. Wilson, *Curves of genus 2 with real multiplication by a square root of 5*. Ph.D. Thesis, University of Oxford (1998).

[38] L. Xiao, *Notes on p-divisible groups*. Unpublished online notes: math.uchicago.edu/ lxiao/files/notes/p-Divisble%20Groups.pdf.

[39] A. Yamagami, *On the unobstructedness of the deformation problems of residual modular representations*, Tokyo J. Math. **27**, No. 2 (2004), 443 - 455.