Moduli of abelian varieties and p-divisible groups

Ching-Li Chai and Frans Oort

ABSTRACT. This is a set of notes for a course we gave in the second week of August in the 2006 CMI Summer School at Göttingen. Our main topic is geometry and arithmetic of $\mathcal{A}_g \otimes \mathbb{F}_p$, the moduli space of polarized abelian varieties of dimension g in positive characteristic. We illustrate properties of $\mathcal{A}_g \otimes \mathbb{F}_p$, and some of the available techniques by treating two topics: 'Density of ordinary Hecke orbits' and 'A conjecture by Grothendieck on deformations of p-divisible groups'.

CONTENTS

We present proofs of two recent results. The main point is that the *methods* used for these proofs are interesting. The emphasis will be on the various techniques available.

In characteristic zero we have strong tools at our disposal: besides algebraic-geometric theories we can use analytic and topological methods. It would seem that we are at a loss in positive characteristic. However the opposite is true. Phenomena

occurring only in positive characteristic provide us with strong tools to study moduli spaces. And, as it turns out again and again, several results in characteristic zero can be derived using reduction modulo p. The discussion of *tools in positive characteristic* will be the focus of our notes.

Here is a list of some of the central topics:

- Serre-Tate theory.
- Abelian varieties over finite fields.
- Monodromy: ℓ-adic and p-adic, geometric and arithmetic.
- Dieudonné modules and Newton polygons.
- Theory of Dieudonné modules, Cartier modules and displays.
- Cayley-Hamilton and deformations of p-divisible groups.
- Hilbert modular varieties.
- Purity of the Newton polygon stratification in families of p-divisible groups.

The strategy is that we have chosen certain central topics, and for those we took ample time for explanation and for proofs. Besides that we need certain results which we label as "Black Box". These are results which we need for our proofs, which are either fundamental theoretical results (but it would take too much time to explain their proofs), or lemmas which are computational, important for the proof, but not very interesting to explain in a course. We hope that we explain well enough what every relevant statement is. We write:

| BB | A Black Box, please accept that this result is true.
| Th | One of the central results, we will explain it.
| Extra | A result which is interesting but was not discussed in the course.

Notation to be used will be explained in Section 10. In order to be somewhat complete we will gather related interesting results, questions and conjectures in Section 11. Part of our general convention is that K denotes a field of characteristic $p > 0$, unless otherwise specified, and k denotes an algebraically closed field.

We assume that the reader is familiar with the basic theory of abelian varieties at the level of Chapter II of [**54**] and [**55**], Chapter 6; we consider abelian varieties over an arbitrary field, and abelian schemes over a base scheme. Alternative references: [**16**], [**81**]. For the main characters of our play: *abelian varieties, moduli spaces, and p-divisible groups*, we give references and definitions in Section 10.

1. Introduction: Hecke orbits, and the Grothendieck conjecture

In this section we discuss the two theorems we are going to consider.

1.1. An abelian variety A of dimension g over a field $K \supset \mathbb{F}_p$ is said to be *ordinary* if

$$\#\left(A[p](k)\right) = p^g.$$

More generally, the number $f = f(A)$ such that $\#\left(A[p](k)\right) = p^f$ is called the *p-rank* of A. It is a fact that the p-rank of A is at most $\dim(A)$; an abelian variety is ordinary if its p-rank is equal to its dimension. See 10.10 for other equivalent definitions.

An elliptic curve E over a field $K \supset \mathbb{F}_p$ is said to be *supersingular* if it is not ordinary; equivalently, E is supersingular if $E[p](k) = 0$ for any overfield $k \supset K$. This

terminology stems from Deuring: an elliptic curve in characteristic zero is said to determine a *singular j*-value if its endomorphism ring over an algebraically closed field (of characteristic 0) is larger than $\mathbb{Z}$ (therefore of rank 2 over $\mathbb{Z}$), while a *supersingular* elliptic curve E over an algebraically closed field $k \supset \mathbb{F}_p$ has $\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(E)) = 4$. Since an elliptic curve is non-singular, a better terminology would be "an elliptic curve with a singular j-invariant".

We say an abelian variety A of dimension g over a field K is *supersingular* if there exists an isogeny $A \otimes_K k \sim E^g$, where E is a supersingular elliptic curve. An equivalent definition for an abelian variety in characteristic p to be supersingular is that all of its slopes are equal to $1/2$; see 4.38 for the definition of slopes and the Newton polygon. Supersingular abelian varieties have p-rank zero. For $g = 2$ one can show that (supersingular) $\Leftrightarrow$ ($f = 0$), where f is the p-rank. For $g > 2$ there exist abelian varieties of p-rank zero which are not supersingular, see 5.22.

Hecke orbits.

Definition 1.2. Let A and B be abelian varieties over a field K. Let $\Gamma \subset \mathbb{Q}$ be a subring. A Γ-isogeny from A to B is an element ψ of $\mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \Gamma$ which has an inverse in $\mathrm{Hom}(B, A) \otimes_{\mathbb{Z}} \Gamma$, i.e., there exists an element $\psi' \in \mathrm{Hom}(B, A) \otimes_{\mathbb{Z}} \Gamma$ such that $\psi' \psi = \mathrm{id}_A \otimes 1$ in $\mathrm{Hom}(A, A) \otimes_{\mathbb{Z}} \Gamma$ and $\psi \psi' = \mathrm{id}_B \otimes 1$ in $\mathrm{Hom}(B, B) \otimes_{\mathbb{Z}} \Gamma$.

Remark.

(i) When $\Gamma = \mathbb{Q}$ (resp. $\Gamma = \mathbb{Z}_{(p)}$, resp. $\mathbb{Z}[1/\ell]$), we say that ψ is a *quasi-isogeny* (resp. *prime-to-p quasi-isogeny*, resp. an *ℓ-power quasi-isogeny*). A *prime-to-p isogeny* (resp. *ℓ-power isogeny*) is an isogeny which is also a $\mathbb{Z}_{(p)}$-isogeny (resp. a $\mathbb{Z}[1/\ell]$-isogeny). Here $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$ is the localization of $\mathbb{Z}$ at the prime ideal $(p) = p\mathbb{Z}$.

(ii) A $\mathbb{Q}$-isogeny ψ (resp. $\mathbb{Z}_{(p)}$-isogeny, resp. $\mathbb{Z}[1/\ell]$-isogeny) can be realized by a diagram

$$A \xleftarrow{\alpha} C \xrightarrow{\beta} B \,,$$

where α and β are isogenies such that there exists an integer $N \in \Gamma^{\times}$ (resp. an integer N prime to p, resp. an integer $N \in \ell^{\mathbb{N}}$) such that $N \cdot \mathrm{Ker}(\alpha) = N \cdot \mathrm{Ker}(\beta) = 0$.

Definition 1.3. Let $[(A, \lambda)] = x \in \mathcal{A}_g(K)$ be the moduli point of a polarized abelian variety over a field K.

(i) We say that a point $[(B, \mu)] = y$ of $\mathcal{A}_g$ is in the *Hecke orbit* of x if there exists a field Ω and

$$\text{a } \mathbb{Q}\text{-isogeny } \varphi : A_{\Omega} \to B_{\Omega} \text{ such that } \varphi^*(\mu) = \lambda.$$

Notation: $y \in \mathcal{H}(x)$. The set $\mathcal{H}(x)$ is called the *Hecke orbit* of x.

(ii) *Hecke-prime-to-p-orbits.* If in the previous definition moreover φ is a $\mathbb{Z}_{(p)}$-isogeny, we say $[(B, \mu)] = y$ is in the Hecke-prime-to-p-orbit of x.
Notation: $y \in \mathcal{H}^{(p)}(x)$.

(iii) *Hecke-ℓ-orbits.* Fix a prime number ℓ different from p. We say $[(B, \mu)] = y$ is in the Hecke-ℓ-orbit of x if in the previous definition moreover φ is a $\mathbb{Z}[1/\ell]$-isogeny.
Notation: $y \in \mathcal{H}_{\ell}(x)$.

(iv) **Notation:** Suppose that $x = [(A, \lambda)]$ is a point of $\mathcal{A}_{g,1}$, i.e., λ is principal. Write

$$\mathcal{H}^{(p)}_{\mathrm{Sp}}(x) := \mathcal{H}^{(p)}(x) \cap \mathcal{A}_{g,1}, \qquad \mathcal{H}^{\mathrm{Sp}}_\ell(x) := \mathcal{H}_\ell(x) \cap \mathcal{A}_{g,1} \ \ (\ell \neq p).$$

Remark.

(i) Clearly we have $\mathcal{H}_\ell(x) \subseteq \mathcal{H}^{(p)}(x) \subseteq \mathcal{H}(x)$. Similarly we have

$$\mathcal{H}^{\mathrm{Sp}}_\ell(x) \subseteq \mathcal{H}^{(p)}_{\mathrm{Sp}}(x) \quad \text{for} \quad x \in \mathcal{A}_{g,1}.$$

(ii) Note that $y \in \mathcal{H}(x)$ is equivalent to requiring the existence of a diagram

$$(B, \mu) \xleftarrow{\ \psi\ } (C, \zeta) \xrightarrow{\ \varphi\ } (A, \lambda).$$

such that $\psi^* \mu = \zeta = \varphi^* \lambda$, where ϕ and ψ are isogenies, $[(B, \mu)] = y$, $[(A, \lambda)] = x$. If we have such a diagram such that both ψ and φ are $\mathbb{Z}_p$-isogenies (resp. $\mathbb{Z}[1/\ell]$-isogenies), then $y \in \mathcal{H}^{(p)}(x)$ (resp. $y \in \mathcal{H}_\ell(x)$.)

(iii) We have given the definition of the so-called Sp_{2g}-Hecke-orbit. One can also define the (slightly bigger) $\mathrm{CSp}_{2g}(\mathbb{Z})$-Hecke-orbits by the usual Hecke correspondences, see [**28**], VII.3, also see 1.7 below.

(iv) The diagram which defines $\mathcal{H}(x)$ as above gives representable correspondences between components of the moduli scheme; these correspondences could be denoted by Sp-Isog, whereas the correspondences considered in [**28**], VII.3 could be denoted by CSp-Isog.

1.4. Why are Hecke orbits interesting? Here we work first over $\mathbb{Z}$. A short answer is that they are manifestations of the Hecke symmetry on $\mathcal{A}_g$. The Hecke symmetry is a salient feature of the moduli space $\mathcal{A}_g$; methods developed for studying Hecke orbits have been helpful for understanding the Hecke symmetry.

To explain what the Hecke symmetry is, we will focus on $\mathcal{A}_{g,1}$, the moduli space of principally polarized abelian varieties and the prime-to-p power, the projective system of $\mathcal{A}_{g,1,n}$ over $\mathbb{Z}[1/n]$. The group $\mathrm{Sp}_{2g}(\mathbb{A}^{(p)}_f)$ of finite prime-to-p adelic points of the symplectic group Sp_{2g} operates on this tower, and induces finite correspondences on $\mathcal{A}_{g,1}$; these finite correspondences are known as *Hecke correspondences*. By the term Hecke symmetry we refer to both the action on the tower of moduli spaces and the correspondences on $\mathcal{A}_{g,1}$. The prime-to-p Hecke orbit $\mathcal{H}^{(p)}(x) \cap \mathcal{A}_{g,1}$ is exactly the orbit of x under the Hecke correspondences coming from the group $\mathrm{Sp}_{2g}(\mathbb{A}^{(p)}_f)$. In characteristic 0, the moduli space of g-dimensional principally polarized abelian varieties is uniformized by the Siegel upper half space $\mathbb{H}_g$, consisting of all symmetric $g \times g$ matrices in $\mathrm{M}_g(\mathbb{C})$ whose imaginary part is positive definite: $\mathcal{A}_{g,1}(\mathbb{C}) \cong \mathrm{Sp}_{2g}(\mathbb{Z}) \backslash \mathbb{H}_g$. The group $\mathrm{Sp}_{2g}(\mathbb{R})$ operates transitively on $\mathbb{H}_g$, and the action of the rational elements $\mathrm{Sp}_{2g}(\mathbb{Q})$ give a family of algebraic correspondences on $\mathrm{Sp}_{2g}(\mathbb{Z}) \backslash \mathbb{H}_g$. These algebraic correspondences are of fundamental importance for harmonic analysis on arithmetic quotients such as $\mathrm{Sp}_{2g}(\mathbb{Z}) \backslash \mathbb{H}_g$.

Remark/Exercise 1.5. (Characteristic zero.) The Hecke orbit of a point in the moduli space $\mathcal{A}_g \otimes \mathbb{C}$ in *characteristic zero* is dense in that moduli space for both the metric topology and the Zariski topology.

1.6. Hecke orbits of elliptic curves. Consider the moduli point $[E] = j(E) = x \in \mathcal{A}_{1,1} \cong \mathbb{A}^1$ of an elliptic curve in characteristic p. Here $\mathcal{A}_{1,1}$ stands for $\mathcal{A}_{1,1} \otimes \mathbb{F}_p$. Note that every elliptic curve has a unique principal polarization.

(1) *If E is supersingular $\mathcal{H}(x) \cap \mathcal{A}_{1,1}$ is a finite set; we conclude that $\mathcal{H}(x)$ is nowhere dense in $\mathcal{A}_1$.*

Indeed, the supersingular locus in $\mathcal{A}_{1,1}$ is closed, there do exist ordinary elliptic curves, and hence that locus is finite; Deuring and Igusa computed the exact number of geometric points in this locus.

(2) **Remark/Exercise.** *If E is ordinary, its Hecke-ℓ-orbit is dense in $\mathcal{A}_{1,1}$.*

There are several ways to prove this. Easy and direct considerations show that in this case $\mathcal{H}_\ell(x) \cap \mathcal{A}_{1,1}$ is not finite; note that every component of $\mathcal{A}_1$ has dimension one, and conclude $\mathcal{H}(x)$ is dense in $\mathcal{A}_1$.

Remark. For elliptic curves we have defined (supersingular) $\Leftrightarrow$ (non-ordinary). For $g = 2$ one can show that (supersingular) $\Leftrightarrow$ ($f = 0$), where f is the p-rank. For $g > 2$ there exist abelian varieties of p-rank zero which are not supersingular, see 5.22.

1.7. A bigger Hecke orbit. We work over $\mathbb{Z}$. We define the notion of CSp-Hecke orbits on $\mathcal{A}_{g,1}$. Two K-points $[(A, \lambda)]$, $[(B, \mu)]$ of $\mathcal{A}_{g,1}$ are in the same CSp-Hecke orbit (resp. prime-to-p CSp-Hecke orbit, resp. ℓ-power CSp-Hecke orbit) if there exists an isogeny $\varphi : A \otimes k \to B \otimes k$ and a positive integer n (resp. a positive integer n which is relatively prime to p, resp. a positive integer which is a power of ℓ) such that $\varphi^*(\mu) = n \cdot \lambda$. Such Hecke correspondences are representable by a morphism $\mathrm{Isog}_g \to \mathcal{A}_g \times \mathcal{A}_g$ on $\mathcal{A}_g$, also see [**28**], VII.3.

The set of all such (B, μ) for a fixed $x := [(A, \lambda)]$ is called the CSp-Hecke orbit (resp. $\mathrm{CSp}(\mathbb{A}_f^{(p)})$-Hecke orbit, resp. $\mathrm{CSp}(\mathbb{Q}_\ell)$-Hecke orbit) of x, and denoted $\mathcal{H}^{\mathrm{CSp}}(x)$ (resp. $\mathcal{H}_{\mathrm{CSp}}^{(p)}(x)$, resp. $\mathcal{H}_\ell^{\mathrm{CSp}}(x)$). Note that

$$\mathcal{H}^{\mathrm{CSp}}(x) \supset \mathcal{H}_{\mathrm{CSp}}^{(p)}(x) \supset \mathcal{H}_\ell^{\mathrm{CSp}}(x),$$

$\mathcal{H}^{\mathrm{CSp}}(x) \supset \mathcal{H}(x)$, $\mathcal{H}_{\mathrm{CSp}}^{(p)}(x) \supset \mathcal{H}^{(p)}(x)$ and $\mathcal{H}_\ell^{\mathrm{CSp}}(x) \supset \mathcal{H}_\ell(x)$. This slightly bigger Hecke orbit will play no role in this paper. However, it is nice to see the relation between the Hecke orbits defined previously in 1.3, which could be called the Sp-Hecke orbits and Sp-Hecke correspondences, with the CSp-Hecke orbits and CSp-Hecke correspondences.

Theorem 1.8. $\boxed{\text{Th}}$ (Density of ordinary Hecke orbits) *Let $[(A, \lambda)] = x \in \mathcal{A}_g \otimes \mathbb{F}_p$ be the moduli point of a polarized ordinary abelian variety in characteristic p.*

(i) *If the polarization λ is separable, then $\left(\mathcal{H}^{(p)}(x) \cap \mathcal{A}_{g,1}\right)^{\mathrm{Zar}} = \mathcal{A}_{g,1}$. If $\deg(\lambda) \in \ell^{\mathbb{N}}$ for a prime number $\ell \neq p$, then $(\mathcal{H}_\ell(x) \cap \mathcal{A}_{g,1})^{\mathrm{Zar}} = \mathcal{A}_{g,1}$.*

(ii) *From (i) we conclude that $\mathcal{H}(x)$ is dense in $\mathcal{A}_g$, with no restriction on the degree of λ.*

See Theorem 9.1. This theorem was proved by Ching-Li Chai in 1995; see [**9**], Theorem 2 on page 477. Although CSp-Hecke orbits were used in [**9**], the same argument works for Sp-Hecke orbits as well. We present a proof of this theorem; we follow [**9**] partly, but also present a new insight which was necessary for solving the general Hecke orbit problem. This final strategy will provide us with a proof which seems easier than the one given previously. More information on the general Hecke orbit problem can be obtained from [**10**] as long as [**13**] is not yet available.

Exercise 1.9. (Any characteristic.) Let k be any algebraically closed field (of any characteristic). Let E be an elliptic curve over k such that $\mathrm{End}(E) = \mathbb{Z}$. Let

ℓ be a prime number different from the characteristic of k. Let E' be an elliptic curve such that there exists an isomorphism $E'/(\underline{\mathbb{Z}/\ell})_k \cong E$. Let λ be the principal polarization on E, let μ be the pullback of λ to E', hence μ has degree ℓ^2, and let $\mu' = \mu/\ell^2$, hence μ' is a principal polarization on E'. *Note that $[(E', \mu')] \in \mathcal{H}(x)$. Show that $[(E', \mu')] \notin \mathcal{H}^{\mathrm{Sp}}(x)$.*

Exercise 1.10. Let E be an elliptic curve in characteristic p which is not supersingular (hence ordinary); let μ be any polarization on E, and $x := [(E, \mu)]$. Show $\mathcal{H}^{\mathrm{Sp}}(x)$ is dense in $\mathcal{A}_1$.

1.11. (1) Let $\mathrm{Isog}_{\mathrm{g,Sp}}$ be the moduli space which classifies diagrams of polarized g-dimensional abelian schemes

$$(B, \mu) \xleftarrow{\psi} (C, \zeta) \xrightarrow{\varphi} (A, \lambda)$$

in characteristic p such that $\psi^*\mu = \zeta = \varphi^*\lambda$. Consider a component I of $\mathrm{Isog}_{g,\mathrm{Sp}}$ defined by diagrams as in 1.7 with $\deg(\psi) = b$ and $\deg(\varphi) = c$. If b is not divisible by p, the first projection $\mathcal{A}_g \leftarrow I$ is étale; if c is not divisible by p, the second projection $I \to \mathcal{A}_g$ is étale.
(2) Consider $\mathrm{Isog}_{g,\mathrm{Sp}}^{\mathrm{ord}} \subset \mathrm{Isog}_{g,\mathrm{Sp}}$, the largest subscheme (it is locally closed) lying over the ordinary locus (either in the first projection, or in the second projection, which is the same).

Exercise. Show that the two projections $(\mathcal{A}_g)^{\mathrm{ord}} \leftarrow \mathrm{Isog}_{g,\mathrm{Sp}}^{\mathrm{ord}} \to (\mathcal{A}_g)^{\mathrm{ord}}$ are both surjective, finite and flat.

(3) $\boxed{\textbf{Extra}}$ Let Z be an irreducible component of $\mathrm{Isog}_{g,\mathrm{Sp}}$ over which the polarizations μ, λ are principal, and such that ζ is a multiple of a principal polarization. Then the projections $\mathcal{A}_{g,1} \leftarrow Z \to \mathcal{A}_{g,1}$ are both surjective and proper. This follows from [**28**], VII.4. The previous exercise (2) is easy; the fact (3) here is more difficult; it uses the computation in [**56**].

1.12. We explain the reason to focus our attention on $\mathcal{A}_{g,1} \otimes \mathbb{F}_p$, the moduli space of principally polarized abelian varieties in characteristic p.
(1) $\boxed{\textbf{BB}}$ In [**56**] it has been proved that $(\mathcal{A}_g)^{\mathrm{ord}}$ *is dense in* $\mathcal{A}_g = \mathcal{A}_g \otimes \mathbb{F}_p$.
(2) We show that for an ordinary $[(A, \lambda)] = x$ we have

$$(\mathcal{H}_\ell(z) \cap \mathcal{A}_{g,1})^{\mathrm{Zar}} = \mathcal{A}_{g,1} \quad \forall z \in \mathcal{A}_{g,1} \quad \Longrightarrow \quad (\mathcal{H}(x))^{\mathrm{Zar}} = \mathcal{A}_g.$$

Work over k. In fact, consider an irreducible component T of $\mathcal{A}_g$. As proved in [**56**] there is an ordinary point $y = [(B, \mu)] \in T$. By [**54**], Corollary 1 on page 234, we see that there is an isogeny $(B, \mu) \to (A, \lambda)$, where λ is a principal polarization. By 1.11 (2) we see that density of $\mathcal{H}_\ell(x) \cap \mathcal{A}_{g,1}$ in $\mathcal{A}_{g,1}$ implies density of $\mathcal{H}_\ell(x) \cap T$ in T. $\qquad\square$

Therefore, from now on we shall be mainly interested in Hecke orbits in the principally polarized case.

Theorem 1.13. $\boxed{\textbf{Extra}}$ (Ching-Li Chai and Frans Oort) *For any $[(A, \mu)] = x \in \mathcal{A}_g \otimes \mathbb{F}_p$ with $\xi = \mathcal{N}(A)$, the Hecke orbit $\mathcal{H}(x)$ is dense in the Newton polygon stratum $\mathcal{W}_\xi(\mathcal{A}_g \otimes \mathbb{F}_p)$.*

A proof will be presented in [**13**]. For a definition of Newton polygon strata and the fact that they are closed in the moduli space, see 1.19, 1.20. Note that in

case $f(A) \leq g-2$ the ℓ-Hecke orbit is not dense in $\mathcal{W}_\xi(\mathcal{A}_g \otimes \mathbb{F}_p)$. In [**68**], 6.2 we find a precise conjectural description of the Zariski closure of $\mathcal{H}_\ell(x)$; that conjecture has now been proven and it implies 1.13.

Lemma 1.14. $\boxed{\text{BB}}$ (Chai) *Let* $[(A, \lambda)] = x \in \mathcal{A}_{g,1}$. *Suppose that A is super-singular. Then $\mathcal{H}^{(p)}(x) \cap \mathcal{A}_{g,1}$ is finite, therefore $\mathcal{H}_\ell(x) \cap \mathcal{A}_{g,1}$ is finite for every prime number $\ell \neq p$. Conversely if $\mathcal{H}_\ell(x) \cap \mathcal{A}_{g,1}$ is finite for a prime number $\ell \neq p$, then x is supersingular.*

See [**9**], Proposition 1 on page 448 for a proof. Note that $\mathcal{H}(x)$ equals *the whole supersingular Newton polygon stratum: the prime-to-p Hecke orbit is small, but the Hecke orbit including p-power quasi-isogenies is large.* Lemma 1.14 will be used in 3.22.

A conjecture by Grothendieck.

Definition 1.15. *p-divisible groups.* Let $h \in \mathbb{Z}_{>0}$ be a positive integer, and let S be a base scheme. A p-divisible group of height h over S is an inductive system of finite, locally free commutative group scheme G_i over S indexed by $i \in \mathbb{N}$, satisfying the following conditions.

(1) The group scheme $G_i \to S$ is of rank p^{ih} for every $i \geq 0$. In particular G_0 is the constant trivial group scheme over S.

(2) The subgroup scheme $G_{i+1}[p^i]$ of p^i-torsion points in G_{i+1} is equal to G_i for every $i \geq 0$.

(3) For each $i \geq 0$, the endomorphism $[p]_{G_{i+1}} : G_{i+1} \to G_{i+1}$ of G_{i+1} factors as $\iota_{i+1,i} \circ \psi_{i+1,i}$, where $\psi_{i+1,i} : G_{i+1} \to G_i$ is a faithfully flat homomorphism, and $\iota_{i+1,i} : G_i \hookrightarrow G_{i+1}$ is the inclusion.

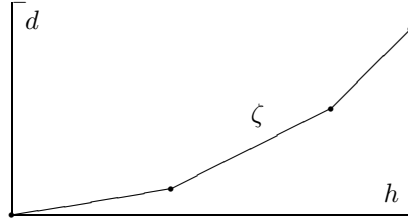Homomorphisms between p-divisible groups are defined by

$$\operatorname{Hom}(\{G_i\}, \{H_j\}) \quad = \varprojlim_i \varinjlim_j \operatorname{Hom}(G_i, H_j).$$

A p-divisible group is also called a Barsotti-Tate group. It is clear that one can generalize the definition of p-divisible groups so that the height is a locally constant function $h : S \to \mathbb{Z}$ on the base scheme S. For more information see [**38**], Section 1. Also see 10.6, and see Section 10 for further information.

In order to being able to handle the isogeny class of $A[p^\infty]$ we need the notion of Newton polygons.

1.16. Newton polygons. Suppose we are given integers $h, d \in \mathbb{Z}_{\geq 0}$; here h = "height", d = "dimension". In the case of abelian varieties we will choose $h = 2g$, and $d = g$. A Newton polygon γ (related to h and d) is a polygon $\gamma \subset \mathbb{R} \times \mathbb{R}$, such that:

- γ starts at $(0,0)$ and ends at (h, d);
- γ is lower convex;
- every slope β of γ has the property that $0 \leq \beta \leq 1$;
- the breakpoints of γ are in $\mathbb{Z} \times \mathbb{Z}$; hence $\beta \in \mathbb{Q}$.

In the above, γ being lower convex means that the region in $\mathbb{R}^2$ above γ is a convex subset of $\mathbb{R}^2$, or equivalently, γ is the graph of a piecewise linear continuous function $f : [0, h] \to \mathbb{R}$ such that $f(tx + (1-t)y) \leq tf(x) + (1-t)f(y)$ for all $x, y \in [0, h]$.

Note that a Newton polygon determines (and is determined by) its slope sequence

$$\beta_1, \ldots, \beta_h \in \mathbb{Q} \text{ with } 0 \leq \beta_1 \leq \cdots \leq \beta_h \leq 1 \quad \leftrightarrow \quad \zeta.$$

Remark.   (i) The last condition above implies that the multiplicity of any slope β in a Newton polygon is a multiple of the denominator of β.

(ii) We imposed the condition that all slopes are between 0 and 1 because we only consider Newton polygons attached to p-divisible groups or abelian varieties. This condition should be eliminated when one considers Newton polygons attached to general (iso)crystals.

Sometimes we will give a Newton polygon by data of the form $\sum_i (m_i, n_i)$, where $m_i, n_i \in \mathbb{Z}_{\geq 0}$, with $\gcd(m_i, n_i) = 1$, and $m_i/(m_i + n_i) \leq m_j/(m_j + n_j)$ for $i \leq j$. The Newton polygon attached to $\sum_i (m_i, n_i)$ can be described as follows. Its height h is given by the formula $h = \sum_i (m_i + n_i)$, its dimension d is given by the formula $d = \sum_i m_i$, and the multiplicity of any rational number β as a slope is $\sum_{m_i = \beta(m_i + n_i)} (m_i + n_i)$. Conversely it is clear that every Newton polygon can be encoded in a unique way in such a form.

Remark. The Newton polygon of a polynomial. Let $g \in \mathbb{Q}_p[T]$ be a monic polynomial of degree h. We are interested in the p-adic values of its zeroes (in an algebraic closure of $\mathbb{Q}_p$). These can be computed by the Newton polygon of this polynomial. Write $g = \sum_j \gamma_j T^{h-j}$. Plot the pairs $(j, v_p(\gamma_j))$ for $0 \leq j \leq h$, where v_p is the valuation on $\mathbb{Q}_p$ with $v_p(p) = 1$. Consider the lower convex hull of $\{(j, v_p(\gamma_j)) \mid j\}$. This is a Newton polygon according to the definition above. The slopes of the sides of this polygon are precisely the p-adic values of the zeroes of g, ordered in non-decreasing order. (Suggestion: prove this as an exercise.)

Later we will see: *a p-divisible group X over a field of characteristic p determines a Newton polygon.* In Section 4 a correct and precise definition will be given. Isogenous p-divisible groups have the same Newton polygon. Moreover a theorem by Dieudonné and Manin says that the isogeny class of a p-divisible group over an algebraically closed field $k \supset \mathbb{F}_p$ is uniquely determined by its Newton polygon; see [**48**], "Classification Theorem" on page 35 and 4.42.

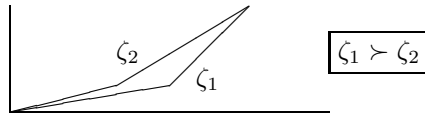(Incorrect.) Here we indicate what the Newton polygon of a p-divisible group is (in a slightly incorrect way...). Consider "the Frobenius endomorphism" of X. This has a "characteristic polynomial". This polynomial determines a Newton polygon, which we write as $\mathcal{N}(X)$, the Newton polygon of X. For an abelian variety A we write $\mathcal{N}(A)$ instead of $\mathcal{N}(A[p^\infty])$.

Well, this "definition" is correct over $\mathbb{F}_p$ as ground field. However, over any other field, $F : X \to X^{(p)}$ is not an endomorphism, and the above "construction" fails. Over a finite field there is a method which repairs this, see 3.8. However we need the Newton polygon of an abelian variety over an arbitrary field. Please accept for the time being the "explanation" given above: $\mathcal{N}(X)$ is the "Newton polygon of the Frobenius on X", which will be made precise later, see Section 4. There is also a more conceptual way of defining the Newton polygon than the definition in Section 4: the slopes measures divisibility properties of tensor constructions of the crystal attached to a p-divisible group; see [**40**].

Examples. (1) The Newton polygon of $\mathbb{G}_m[p^\infty]_{\mathbb{F}_p}$ has one slope (counting multiplicity), which is equal to 1. In fact, on $\mathbb{G}_m$ the Frobenius endomorphism is $[p]$.

(2) The Newton polygon of the constant p-divisible group $\underline{\mathbb{Q}_p/\mathbb{Z}_p}_{\mathbb{F}_p}$ has one slope (counting multiplicity), which is equal to 0.

(3) The Newton polygon of an ordinary elliptic curve has two slopes, equal to 0 and to 1, each with multiplicity one.

(4) The Newton polygon of a supersingular elliptic curve has two slopes, both equal to $1/2$.

1.17. Newton polygons go up under specialization. Grothendieck observed in 1970 that "Newton polygons go up" under specialization. See 1.20, 4.47 for more information. In order to study this and related questions we introduce the notation of a *partial ordering* between Newton polygons.

We write $\zeta_1 \succ \zeta_2$ if ζ_1 is "below" ζ_2, i.e., if no point of ζ_1 is strictly above ζ_2:

Note that we use this notation only if Newton polygons with the same endpoints are considered. A note on convention: we write $\prec$ instead of $\preceq$, so we have $\zeta \succ \zeta$ for any Newton polygon ζ.

This notation may seem unnatural. However if ζ_1 is strictly below ζ_2 the stratum defined by ζ_1 is larger than the stratum defined by ζ_2; this explains the choice for this notation.

1.18. Later in Section 4 we will show that isogenous p-divisible groups have the same Newton polygon. We will also see in 4.40 that if $\mathcal{N}(X)$ is given by $\{\beta_i \mid 1 \leq i \leq h\}$ then $\mathcal{N}(X^t)$ is given by $\{1 - \beta_h, \ldots, 1 - \beta_1\}$.

A Newton polygon ξ, given by the slopes $\beta_1 \leq \cdots \leq \beta_h$ is called *symmetric* if $\beta_i = 1 - \beta_{h+1-i}$ for all i. We see that $X \sim X^t$ implies that $\mathcal{N}(X)$ is symmetric; in particular for an abelian variety A we see that $\mathcal{N}(A)$ is symmetric. This was proved over finite fields by Manin, see [**48**], page 70; for any base field we can use the duality theorem over any base, see [**61**], Th. 19.1, also see 10.11.

1.19. If S is a base scheme over $\mathbb{F}_p$, and $\mathcal{X} \to S$ is a p-divisible group over S and ζ is a Newton polygon we write

$$\mathcal{W}_\zeta(S) := \{s \in S \mid \mathcal{N}(\mathcal{X}_s) \prec \zeta\} \subset S$$

and

$$\mathcal{W}_\zeta^0(S) := \{s \in S \mid \mathcal{N}(\mathcal{X}_s) = \zeta\} \subset S.$$

Theorem 1.20. $\boxed{\text{BB}}$ (Grothendieck and Katz; see [**40**], 2.3.2)

$$\mathcal{W}_\zeta(S) \subset S \quad \text{is a closed set.}$$

Working over $S = \text{Spec}(K)$, where K is a perfect field, $\mathcal{W}_\zeta(S)$ and $\mathcal{W}_\zeta^0(S)$ will be given the induced reduced scheme structure.

As the set of Newton polygons of a given height is finite we conclude:

$$\mathcal{W}_\zeta^0(S) \subset S \quad \text{is a locally closed set.}$$

Notation. Let ξ be a symmetric Newton polygon. We write $W_\xi = \mathcal{W}_\xi(\mathcal{A}_{g,1} \otimes \mathbb{F}_p)$.

1.21. We have seen that "Newton polygons go up under specialization". Does a kind of converse hold? In 1970 Grothendieck conjectured the converse. In the appendix of [**34**] is a letter of Grothendieck to Barsotti, with the following passage on page 150: *"The wishful conjecture I have in mind now is the following: the necessary conditions . . . that G' be a specialization of G are also sufficient. In other words, starting with a BT group $G_0 = G'$, taking its formal modular deformation . . . we want to know if every sequence of rational numbers satisfying . . . these numbers occur as the sequence of slopes of a fiber of G as some point of S."*

Theorem 1.22. $\boxed{\text{Th}}$ (The Grothendieck Conjecture, Montreal 1970) *Let K be a field of characteristic p, and let X_0 be a p-divisible group over K. We write $\mathcal{N}(\mathcal{X}_0) =: \beta$ for its Newton polygon. Given a Newton polygon γ "below" β, i.e., $\beta \prec \gamma$, there exists a deformation X_η of X_0 such that $\mathcal{N}(\mathcal{X}_\eta) = \gamma$.*

See §8. This was proved by Frans Oort in 2001. For a proof see [**20**], [**65**], [**66**].

We say "X_η is a deformation of X_0" if there exists an integral scheme S over K, with generic point $\eta \in S$ and $0 \in S(K)$, and a p-divisible group $\mathcal{X} \to S$ such that $\mathcal{X}_0 = X_0$ and $\mathcal{X}_\eta = X_\eta$.

A (quasi-) polarized version will be given later.

In this paper we record a proof of this theorem, and we will see that this is an important tool in understanding Newton polygon strata in $\mathcal{A}_g$ in characteristic p.

Why is the proof of this theorem difficult? A direct approach seems obvious: write down deformations of X_0, compute Newton polygons of all fibers, and inspect whether all relevant Newton polygons appear in this way. However, computing the Newton polygon of a p-divisible group in general is difficult (but see Section 5 on how to circumvent this in an important special case). Moreover, abstract deformation theory is easy, but in general Newton polygon strata are "very singular"; in Section 7 we describe how to "move out" of a singular point to a non-singular point of a Newton polygon stratum. Then, at non-singular points the deformation theory can be described more easily, see Section 5. By a combination of these two methods we achieve a proof of the Grothendieck conjecture. Later we will formulate and prove the analogous "polarized case" of the Grothendieck conjecture, see Section 8.

We see: a direct approach did not work, but the detour via "deformation to $a \leq 1$" plus the results via Cayley-Hamilton gave the essential ingredients for a proof. Note the analogy of this method with the approach to liftability of abelian varieties to characteristic zero, as proposed by Mumford, and carried out in [**56**].

2. Serre-Tate theory

In this section we explain the deformation theory of abelian varieties and p-divisible groups. The content can be divided into several parts:

(1) In 2.1 we give the formal definitions of deformation functors for abelian varieties and p-divisible groups.

(2) In contrast to the deformation theory for general algebraic varieties, the deformation theory for abelian varieties and p-divisible groups can be efficiently dealt with by linear algebra, as follows from the crystalline deformation theory of Grothendieck-Messing. It says that, over an extension by an ideal with a divided power structure, deforming abelian varieties or p-divisible groups is the same as lifting the Hodge filtration. See Theorem 2.4 for the precise statement, and Theorem 2.11 for the behavior of the theory under duality. The smoothness of the moduli space $\mathcal{A}_{g,1,n}$ follows quickly from this theory.

(3) The Serre-Tate theorem: deforming an abelian variety is the same as deforming its p-divisible group. See Theorem 2.7 for a precise statement. A consequence is that the deformation space of a polarized abelian variety admits an natural action by a large p-adic group, see 2.14. In general this action is poorly understood.

(4) There is one case when the action on the deformation space mentioned in (3) above is linearized and well-understood. This is the case when the abelian variety is ordinary. The theory of Serre-Tate coordinates says that the deformation space of an ordinary abelian variety has a natural structure as a formal torus. See Theorem 2.19 for the statement. In this case the action on the local moduli space mentioned in (3) above preserves the group structure and gives a linear representation on the character group of the Serre-Tate formal torus. This phenomenon has important consequences later. A local rigidity result, Theorem 2.26, is important for the Hecke orbit problem in that it provides an effective linearization of the Hecke orbit problem. Also, computing the deformation using the Serre-Tate coordinates is often easy; the reader is encouraged to try Exercise 2.25.

Here is a list of recommended references.

p-divisible groups: [49], [38].
Crystalline deformation theory: [49], [5].
Serre-Tate Theorem: [49], [41].
Serre-Tate coordinates: [42].

2.1. Deformations of abelian varieties and of p-divisible groups.

Definition. Let K be a perfect field of characteristic p. Denote by $W(K)$ the ring of p-adic Witt vectors with coordinates in K.
(i) Denote by $\mathrm{Art}_{W(K)}$ the category of Artinian local algebras over $W(K)$. An object of $\mathrm{Art}_{W(K)}$ is a pair (R, j), where R is an Artinian local algebra and $j : W(K) \to R$ is a local homomorphism of local rings. A morphism in $\mathrm{Art}_{W(K)}$ from

(R_1, j_1) to (R_2, j_2) is a homomorphism $h : R_1 \to R_2$ between Artinian local rings such that $h \circ j_1 = j_2$.

(ii) Denote by Art_K the category of Artinian local K-algebras. An object in Art_K is a pair (R, j), where R is an Artinian local algebra and $j : K \to R$ is a ring homomorphism. A morphism in Art/K from (R_1, j_1) to (R_2, j_2) is a homomorphism $h : R_1 \to R_2$ between Artinian local rings such that $h \circ j_1 = j_2$. Notice that Art_K is a fully faithful subcategory of $\mathrm{Art}_{W(K)}$.

Definition. Denote by Sets the category whose objects are sets and whose morphisms are maps between sets.

Definition. Let A_0 be an abelian variety over a perfect field $K \supset \mathbb{F}_p$. The deformation functor of A_0 is a functor

$$\mathrm{Def}(A_0/W(K)) : \mathrm{Art}_{W(K)} \to \mathrm{Sets}$$

defined as follows. For every object (R, j) of $\mathrm{Art}_{W(K)}$, $\mathrm{Def}(A_0/W(K))(R, j)$ is the set of isomorphism classes of pairs $(A \to \mathrm{Spec}(R), \epsilon)$, where $A \to \mathrm{Spec}(R)$ is an abelian scheme, and

$$\epsilon : A \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R/\mathfrak{m}_R) \xrightarrow{\sim} A_0 \times_{\mathrm{Spec}(K)} \mathrm{Spec}(R/\mathfrak{m}_R)$$

is an isomorphism of abelian varieties over $R/\mathfrak{m}_R$. Denote by $\mathrm{Def}(A_0/K)$ the restriction of the deformation functor $\mathrm{Def}(A_0/W(K))$ to the faithful subcategory Art_K of $\mathrm{Art}_{W(K)}$.

Definition. Let A_0 be an abelian variety over a perfect field $K \supset \mathbb{F}_p$, and let λ_0 be a polarization on A_0. The deformation functor of (A_0, λ_0) is a functor

$$\mathrm{Def}(A_0/W(K)) : \mathrm{Art}_{W(K)} \to \mathrm{Sets}$$

defined as follows. For every object (R, ϵ) of $\mathrm{Art}_{W(K)}$, $\mathrm{Def}(A_0/W(K))(R, \epsilon)$ is the set of isomorphism classes of pairs $(A, \lambda) \to \mathrm{Spec}(R), \epsilon)$, where $(A, \lambda) \to \mathrm{Spec}(R)$ is a polarized abelian scheme, and

$$\epsilon : (A, \lambda) \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R/\mathfrak{m}_R) \xrightarrow{\sim} (A_0, \lambda_0) \times_{\mathrm{Spec}(K)} \mathrm{Spec}(R/\mathfrak{m}_R)$$

is an isomorphism of polarized abelian varieties over $R/\mathfrak{m}_R$. Let $\mathrm{Def}((A_0, \lambda_0)/K)$ denote the restriction of $\mathrm{Def}(A_0/W(K))$ to the faithful subcategory Art_K of $\mathrm{Art}_{W(K)}$.

Exercise. Let X_0 be a p-divisible group over a perfect field $K \supset \mathbb{F}_p$, and let $\lambda_0 : X_0 \to X_0^t$ be a polarization of X_0. Define the deformation functor $\mathrm{Def}(X_0/W(K))$ for X_0 and the deformation functor $\mathrm{Def}((X_0, \lambda_0)/W(K))$ imitating the above definitions for abelian varieties.

Definition 2.2. Let R be a commutative ring, and let $I \subset R$ be an ideal of I. A *divided power structure* (a DP structure for short) on I is a collection of maps $\gamma_i : I \to R$, $i \in \mathbb{N}$, such that

- $\gamma_0(x) = 1 \quad \forall x \in I$,
- $\gamma_1(x) = x \quad \forall x \in I$,
- $\gamma_i(x) \in I \quad \forall x \in I, \forall i \geq 1$,
- $\gamma_j(x + y) = \sum_{0 \leq i \leq j} \gamma_i(x)\gamma_{j-i}(y) \quad \forall x, y \in I, \forall j \geq 0$,
- $\gamma_i(ax) = a^i \quad \forall a \in R, \forall x \in I, \forall i \geq 1$,
- $\gamma_i(x)\gamma_j(y) = \frac{(i+j)!}{i!j!}\gamma_{i+j}(x) \quad \forall i, j \geq 0, \forall x \in I$,

- $\gamma_i(\gamma_j(x)) = \frac{(ij)!}{i!(j!)^i}\gamma_{ij}(x) \quad \forall i, j \geq 1, \forall x \in I.$

A divided power structure $(R, I, (\gamma_i)_{i \in \mathbb{N}})$ as above is *locally nilpotent* if there exist $n_0 \in \mathbb{N}$ such that $\gamma_i(x) = 0$ for all $i \geq n_0$ and all $x \in I$. A *locally nilpotent* DP *extension* of a commutative ring R_0 is a locally nilpotent DP structure $(R, I, (\gamma_i)_{i \in \mathbb{N}})$ together with an isomorphism $R/I \xrightarrow{\sim} R_0$.

Remark 2.3.

(i) The basic idea for a divided power structure is that $\gamma_i(x)$ should "behave like" $x^i/i!$ and make sense even though dividing by $i!$ is illegitimate. The reader can easily verify that $\gamma_i(x) = x^i/i!$ is the unique divided power structure on (R, I) when $R \supseteq \mathbb{Q}$.

(ii) Given a divided power structure on (R, I) as above, one can define an exponential homomorphism $\exp : I \to 1 + I \subset R^\times$ by

$$\exp(x) = 1 + \sum_{n \geq 1} \gamma_n(x),$$

and a logarithmic homomorphism $\log : (1 + I) \to I$ by

$$\log(1 + x) = \sum_{n \geq 1} (n - 1)! \, (-1)^{n-1} \gamma_n(x).$$

These homomorphisms establish an isomorphism $(1 + I) \xrightarrow{\sim} I$.

(iii) Let R be a commutative ring with 1, and let I be an ideal of R such that $I^2 = (0)$. Define a DP structure on I by requiring that $\gamma_i(x) = 0$ for all $i \geq 2$ and all $x \in I$. This DP structure on a square-zero ideal I will be called the *trivial DP structure* on I.

(iv) The notion of a divided power structure was first introduced in the context of cohomology of Eilenberg-Mac Lane spaces. Grothendieck realized that one can use the divided power structure to define the crystalline first Chern class of line bundles, by analogy with the classical definition in characteristic 0, thanks to the isomorphism $(1 + I) \xrightarrow{\sim} I$ provided by a divided power structure. This observation motivated the definition of the crystalline site based on the notion of divided power structure.

(v) Theorem 2.4 below reduces deformation theory for abelian varieties and p-divisible groups to linear algebra, provided the augmentation ideal I has a divided power structure. An extension of a ring R_0 by a square-zero ideal I constitutes a standard "input data" in deformation theory; on (R, I) we have the trivial divided power structure. So we can feed such input data into the crystalline deformation theory summarized in Theorem 2.4 below to translate the deformation of an abelian scheme $A \to \mathrm{Spec}(R_0)$ over a square-zero extension $R \twoheadrightarrow R_0$ into a question about lifting Hodge filtrations, which is a question in linear algebra.

The statement of the black-boxed Theorem 2.4 below is a bit long. Roughly it says that attached to any DP-extension $(R, I, (\gamma_i)$ of the base of an abelian scheme (or a p-divisible group) over R/I, we can attach a (covariant) Dieudonné crystal, which is canonically isomorphic to the first de Rham homology of any lifting over R of the abelian scheme, if such a lifting exists. Moreover, lifting the abelian scheme to R is equivalent to lifting the Hodge filtration to the Dieudonné crystal. Notice that the first de Rham homology of abelian varieties over base schemes in

characteristic 0 enjoys similar properties, through the Gauss-Manin connection and the Kodaira-Spencer map.

Theorem 2.4. [BB] (Grothendieck-Messing) *Let $X_0 \to \mathrm{Spec}(R_0)$ be an p-divisible group over a commutative ring R_0.*

(i) *To every locally nilpotent DP extension $(R, I, (\gamma_i)_{i \in \mathbb{N}})$ of R_0 there is a functorially attached locally free R-module $\mathbb{D}(X_0)_R = \mathbb{D}(X0)_{(R,I,(\gamma_i))}$ of rank $\mathrm{ht}(X_0)$. The functor $\mathbb{D}(X_0)$ is called the covariant Dieudonné crystal attached to X_0.*

(ii) *Let $(R, I, (\gamma_i)_{i \in \mathbb{N}})$ be a locally nilpotent DP extension of R_0. Suppose that $X \to \mathrm{Spec}(R)$ is a p-divisible group extending $X_0 \to \mathrm{Spec}(R_0)$. Then there is a functorial short exact sequence*

$$0 \to \mathrm{Lie}(X^t/R)^\vee \to \mathbb{D}(X_0)_R \to \mathrm{Lie}(X/R) \to 0\,.$$

Here $\mathrm{Lie}(X/R)$ is the tangent space of the p-divisible group $X \to \mathrm{Spec}(R)$, which is a projective R-module of rank $\dim(X/R)$, and $\mathrm{Lie}(X^t/R)^\vee$ is the R-dual of the tangent space of the Serre dual $X^t \to \mathrm{Spec}(R)$ of $X \to \mathrm{Spec}(R)$.

(iii) *Let $(R, I, (\gamma_i)_{i \in \mathbb{N}})$ be a locally nilpotent DP extension of R_0. Suppose that $A \to \mathrm{Spec}(R)$ is an abelian scheme such that there exists an isomorphism*

$$\beta : A[p^\infty] \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R_0) \xrightarrow{\sim} X_0$$

of p-divisible groups over R_0. Then there exists a natural isomorphism

$$\mathbb{D}(X_0)_R \to \mathrm{H}_1^{\mathrm{DR}}(A/R)\,,$$

where $\mathrm{H}_1^{\mathrm{DR}}(A/R)$ is the first de Rham homology of $A \to \mathrm{Spec}(R)$. Moreover the above isomorphism identifies the short exact sequence

$$0 \to \mathrm{Lie}(A[p^\infty]^t/R)^\vee \to \mathbb{D}(X_0)_R \to \mathrm{Lie}(A[p^\infty]/R) \to 0$$

described in (ii) *with the Hodge filtration*

$$0 \to \mathrm{Lie}(A^t/R)^\vee \to \mathrm{H}_1^{\mathrm{DR}}(A/R) \to \mathrm{Lie}(A/R) \to 0$$

on $\mathrm{H}_1^{\mathrm{DR}}(A/R)$.

(iv) *Let $(R, I, (\gamma_i)_{i \in \mathbb{N}})$ be a locally nilpotent DP extension of R_0. Denote by $\mathfrak{E}$ the category whose objects are short exact sequences*

$$0 \to F \to \mathbb{D}(X_0)_R \to Q \to 0$$

such that F and Q are projective R-modules, plus an isomorphism from the short exact sequence

$$(0 \to F \to \mathbb{D}(X_0)_R \to Q \to 0) \otimes_R R_0$$

of projective R_0-modules to the short exact sequence

$$0 \to \mathrm{Lie}(X_0^t)^\vee \to \mathbb{D}(X_0)_{R_0} \to \mathrm{Lie}(X) \to 0$$

attached to the p-divisible group $X_0 \to \mathrm{Spec}(R_0)$ as a special case of (ii) *above. The morphisms in $\mathfrak{E}$ are maps between diagrams. Then the functor from the category of p-divisible groups over R lifting X_0 to the category $\mathfrak{E}$ described in* (ii) *is an equivalence of categories.*

Theorem 2.4 is a summary of the main results in Chapter IV of [**49**].

Corollary 2.5. *Let X_0 be a p-divisible group over a perfect field $K \supset \mathbb{F}_p$. Let $d = \dim(X_0)$, $c = \dim(X_0^t)$. The deformation functor $\mathrm{Def}(X_0/W(K))$ of X_0 is representable by a smooth formal scheme over $W(K)$ of dimension cd. In other words, $\mathrm{Def}(X_0/W(K))$ is non-canonically isomorphic to the functor represented by the formal spectrum $\mathrm{Spf}\,(W(K)[[x_1, \ldots, x_{cd}]])$.*

Proof. Recall that formal smoothness of $\mathrm{Def}(X_0/W(K))$ means that the natural map

$$\mathrm{Def}(X_0/W(K))(R) \to \mathrm{Def}(X_0/W(K))(R')$$

attached to any surjective ring homomorphism $R \to R'$ is surjective, for any Artinian local rings $R, R' \in \mathrm{Art}_{W(K)}$. To prove this, we may and do assume that the kernel I of the surjective homomorphism $R \to R'$ satisfies $I^2 = (0)$. Apply Theorem 2.4 to the trivial DP structure on pairs (R, I) with $I^2 = (0)$, we see that $\mathrm{Def}(X_0/W(K))$ is formally smooth over $W(K)$. Applying Theorem 2.4 again to the pair $K[t]/(t^2), tK[t]/(t^2)$, we see that the dimension of the tangent space of $\mathrm{Def}(X_0/K)$ is equal to cd. $\qquad\square$

2.6. We set up notation for the Serre-Tate Theorem 2.7, which says that deforming an abelian variety A_0 over a field of characteristic p is the same as deforming the p-divisible group $A_0[p^\infty]$ attached to A_0. Recall that $A_0[p^\infty]$ is the inductive system formed by the p^n-torsion subgroup schemes $A_0[p^n]$ of A_0, where n runs through positive integers. In view of Theorem 2.4 one can regard the p-divisible group $A_0[p^\infty]$ as a refinement of the first homology group of A_0.

Let p be a prime number. Let S be a scheme such that p is locally nilpotent in $\mathcal{O}_S$. Let $I \subset \mathcal{O}_S$ be a coherent sheaf of ideals such that I is locally nilpotent. Let $S_0 = \mathrm{Spec}(\mathcal{O}_S/I)$. Denote by AV_S the category of abelian schemes over S. Denote by $\mathrm{AVBT}_{S_0,S}$ the category whose objects are triples $(A_0 \to S_0, X \to S, \epsilon)$, where $A_0 \to S_0$ is an abelian scheme over S_0, $X \to S$ is a p-divisible group over S, and $\epsilon : X \times_S S_0 \to A_0[p^\infty]$ is an isomorphism of p-divisible groups. A morphism from $(A_0 \to S_0, X \to S, \epsilon)$ to $(A_0' \to S_0, X' \to S, \epsilon')$ is a pair (h, f), where $h_0 : A_0 \to A_0'$ is a homomorphism of abelian schemes over S_0, and $f : X \to X'$ is a homomorphism of p-divisible groups over S, such that $h[p^\infty] \circ \epsilon = \epsilon' \circ (f \times_S S_0)$. Let

$$\mathbb{G}_{S_0,S} : \mathrm{AV}_S \to \mathrm{AVBT}_{S_0,S}$$

be the functor which sends an abelian scheme $A \to S$ to the triple

$$((A \times_S S_0, A[p^\infty], \mathrm{can}),$$

where can is the canonical isomorphism $A[p^\infty] \times_S S_0 \xrightarrow{\sim} (A \times_S S_0)[p^\infty]$.

Theorem 2.7. $\boxed{\textbf{BB}}$ (Serre-Tate) *Notation and assumptions as in the above paragraph. The functor $\mathbb{G}_{S_0,S}$ is an equivalence of categories.*

Remark. See [**46**]. A proof of Theorem 2.7 first appeared in print in [**49**]. See also [**41**].

Corollary 2.8. *Let A_0 be an abelian variety over a perfect field K. Let*

$$\mathbb{G} : \mathrm{Def}(A_0/W(K)) \to \mathrm{Def}(A_0[p^\infty]/W(K))$$

be the functor which sends any object

$$\left(A \to \mathrm{Spec}(R), \epsilon : A \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R/\mathfrak{m}_R) \xrightarrow{\sim} A_0 \times_{\mathrm{Spec}(k)} \mathrm{Spec}(R/\mathfrak{m}_R) \right)$$

in $\mathrm{Def}(A_0/W(K))$ *to the object*

$$(A[p^\infty] \to \mathrm{Spec}(R), \epsilon[p^\infty])$$
$$\epsilon[p^\infty] : A[p^\infty] \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R/\mathfrak{m}_R) \xrightarrow{\sim} A_0[p^\infty] \times_{\mathrm{Spec}(K)} \mathrm{Spec}(R/\mathfrak{m}_R)$$

in $\mathrm{Def}(A_0[p^\infty]/W(K))$. *The functor* $\mathbb{G}$ *is an equivalence of categories.*

Remark. In words, Corollary 2.8 says that deforming an abelian variety is the same as deforming its p-divisible group.

Corollary 2.9. *Let A_0 be a g-dimensional abelian variety over a perfect field $K \supset \mathbb{F}_p$. The deformation functor $\mathrm{Def}(A_0/W(K))$ of A_0 is representable by a smooth formal scheme over $W(K)$ of relative dimension g^2.*

PROOF. We have $\mathrm{Def}(A_0/W(K)) \cong \mathrm{Def}(A_0[p^\infty]/W(K))$ by Theorem 2.7. Corollary 2.9 follows from Corollary 2.5. □

2.10. Let R_0 be a commutative ring. Let $A_0 \to \mathrm{Spec}(R_0)$ be an abelian scheme. Let $\mathbb{D}(A_0) := \mathbb{D}(A_0[p^\infty])$ be the covariant Dieudonné crystal attached to A_0. Let $\mathbb{D}(A_0^t)$ be the covariant Dieudonné crystal attached to the dual abelian scheme A^t. Let $\mathbb{D}(A_0)^\vee$ be the dual of $\mathbb{D}(A_0)$, i.e.,

$$\mathbb{D}(A_0)^\vee_{(R,I,(\gamma_i))} = \mathrm{Hom}_R(\mathbb{D}(A_0)_R, R)$$

for any locally nilpotent DP extension $(R, I, (\gamma_i)_{i\in\mathbb{N}})$ of $R_0 = R/I$.

Theorem 2.11. $\boxed{\text{BB}}$ *We have functorial isomorphisms*

$$\varphi_{A_0} : \mathbb{D}(A_0)^\vee \xrightarrow{\sim} \mathbb{D}(A_0^t)$$

for abelian varieties A_0 over K with the following properties.

(1) *The composition*

$$\mathbb{D}(A_0^t)^\vee \xrightarrow[\sim]{\varphi_{A_0}^\vee} (\mathbb{D}(A_0)^\vee)^\vee = \mathbb{D}(A_0) \xrightarrow[\sim]{j_{A_0}} \mathbb{D}((A_0^t)^t)$$

is equal to

$$-\varphi_{A_0^t} : \mathbb{D}(A_0^t)^\vee \xrightarrow{\sim} \mathbb{D}((A_0^t)^t),$$

where the isomorphism $\mathbb{D}_{A_0} \xrightarrow[\sim]{j_{A_0}} \mathbb{D}((A_0^t)^t)$ *is induced by the canonical isomorphism*

$$A_0 \xrightarrow{\sim} (A_0^t)^t.$$

(2) *For any locally nilpotent DP extension $(R, I, (\gamma_i)_{i\in\mathbb{N}})$ of $R_0 = R/I$ and any lifting $A \to \mathrm{Spec}(R)$ of $A_0 \to \mathrm{Spec}(R_0)$ to R, the following diagram*

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Lie}(A/R)^\vee & \longrightarrow & \mathbb{D}(A_0)^\vee_R & \longrightarrow & (\mathrm{Lie}(A^t/R)^\vee)^\vee & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle\varphi_{A_0}} & & \downarrow{\scriptstyle=} & & \\
0 & \longrightarrow & \mathrm{Lie}((A^t)^t/R)^\vee & \longrightarrow & \mathbb{D}(A_0^t)_R & \longrightarrow & \mathrm{Lie}(A^t/R) & \longrightarrow & 0
\end{array}
$$

commutes. Here the bottom horizontal exact sequence is as in 2.4, the top horizontal sequence is the dual of the short exact sequence in 2.4, and the left vertical isomorphism is induced by the canonical isomorphism $A \xrightarrow{\sim} (A^t)^t$.

Theorem 2.11 is proved in [**5**], Chapter 5, §1.

Below are three applications of Theorem 2.4, Theorem 2.7 and Theorem 2.11; their proofs are left as exercises. The first two, Corollary 2.12 and Corollary 2.13, are basic properties of the moduli space of polarized abelian varieties. The group action in Corollary 2.14 is called the action of the local stabilizer subgroup. This "local symmetry" of the local moduli space will play an important role later in the proof of the density of ordinary Hecke orbits.

Corollary 2.12. *Let (A_0, λ_0) be a g-dimensional principally polarized abelian variety over a perfect field $K \supset \mathbb{F}_p$. The deformation functor $\mathrm{Def}((A_0, \lambda)/W(K))$ of A_0 is representable by a smooth formal scheme over $W(K)$ of dimensional $g(g+1)/2$.*

Remark. Corollary 2.12 can be reformulated as follows. Let η_0 be a K-rational symplectic level-n structure on A_0, $n \geq 3$, $(n, p) = 1$, and let $x_0 = [(A_0, \lambda_0, \eta_0)] \in \mathcal{A}_{g,1,n}(K)$. The formal completion $\mathcal{A}_{g,1,n}^{/x_0}$ of the moduli space $\mathcal{A}_{g,1,n} \to \mathrm{Spec}(W(K))$ is non-canonically isomorphic to $\mathrm{Spf}\left(W(K)[[x_1, \ldots, x_{g(g+1)/2}]]\right)$.

Corollary 2.13. *Let (A_0, λ_0) be a polarized abelian variety over a perfect field $K \supset \mathbb{F}$; let $\deg(\lambda_0) = d^2$.*

   (i) *The natural map $\mathrm{Def}((A_0, \lambda_0)/W(K)) \to \mathrm{Def}(A_0/W(K))$ is represented by a closed embedding of formal schemes.*

   (ii) *Let n be a positive integer, $n \geq 3$, $(n, pd) = 1$. Let η_0 be a K-rational symplectic level-n structure on (A_0, λ_0). Let $x_0 = [(A_0, \lambda_0, \eta_0)] \in \mathcal{A}_{g,d,n}(K)$. The formal completion $\mathcal{A}_{g,d,n}^{/x_0}$ of the moduli space $\mathcal{A}_{g,d,n} \to \mathrm{Spec}(W(K))$ at the closed point x_0 is isomorphic to the local deformation space*

$$\mathrm{Def}((A_0, \lambda_0)/W(K)).$$

Corollary 2.14. (i) *Let A_0 be an variety over a perfect field $K \supset \mathbb{F}$. There is a natural action of the profinite group $\mathrm{Aut}(A_0[p^\infty])$ on the smooth formal scheme $\mathrm{Def}(A_0/W(K))$.*

   (ii) *Let λ_0 be a principal polarization on an abelian variety A_0 over a perfect field K. Denote by $\mathrm{Aut}((A_0, \lambda_0)[p^\infty])$ the closed subgroup of $\mathrm{Aut}(A_0[p^\infty])$ consisting of all automorphisms of $\mathrm{Aut}(A[p^\infty])$ compatible with the quasi-polarization $\lambda_0[p^\infty]$. The natural action in (i) above induces a natural action on the closed formal subscheme $\mathrm{Def}(A_0, \lambda_0)$ of $\mathrm{Def}(A_0)$.*

Remark. In the situation of (ii) above, the group $\mathrm{Aut}(A_0, \lambda_0)$ of polarization-preserving automorphisms of A_0 is finite, while $\mathrm{Aut}((A_0, \lambda_0)[p^\infty])$ is a compact p-adic Lie group of positive dimension of positive dimension if $\dim(A_0) > 0$. The group $\mathrm{Aut}(A_0, \lambda)$ (resp. $\mathrm{Aut}((A_0, \lambda_0)[p^\infty])$) operates on $\mathrm{Def}(A_0, \lambda_0)$ (resp. $\mathrm{Def}((A_0, \lambda_0)[p^\infty])$) by "changing the marking". By Theorem 2.7, we have a natural isomorphism $\mathrm{Def}(A_0, \lambda_0) \xrightarrow{\sim} \mathrm{Def}((A_0, \lambda_0)[p^\infty])$, which is equivariant for the inclusion homomorphism $\mathrm{Aut}(A_0, \lambda_0) \hookrightarrow \mathrm{Aut}((A_0, \lambda_0)[p^\infty])$. In other words, the action of $\mathrm{Aut}(A_0, \lambda)$ on $\mathrm{Def}(A_0, \lambda_0)$ extends to an action by $\mathrm{Aut}((A_0, \lambda_0)[p^\infty])$.

2.15. Étale and toric p-divisible groups: notation. A p-divisible group X over a base scheme S is said to be étale (resp. toric) if and only if $X[p^n]$ is étale (resp. of multiplicative type) for every $n \geq 1$; see the end of 10.6.

Remark. Let $E \to S$ be an étale p-divisible group, where S is a scheme. The p-adic Tate module of E, defined by

$$\mathrm{T}_p(E) := \varprojlim_{n} E[p^n] \,,$$

is representable by a smooth $\mathbb{Z}_p$-sheaf on $S_{\text{ét}}$ whose rank is equal to $\mathrm{ht}(E/S)$. Here the rank of E is a locally constant function on the base scheme S. When S is the spectrum of a field K, $\mathrm{T}_p(E)$ "is" a free $\mathbb{Z}_p$-module with an action by $\mathrm{Gal}(K^{\text{sep}}/K)$; see 10.5.

Remark. Attached to any toric p-divisible group $T \to S$ is its character group

$$X^*(T) := \underline{\mathrm{Hom}}(T, \mathbb{G}_m[p^\infty])$$

and cocharacter group

$$X_*(T) := \underline{\mathrm{Hom}}(\mathbb{G}_m[p^\infty], T) \,.$$

The character group of T can be identified with the p-adic Tate module of the Serre-dual T^t of T, and T^t is an étale p-divisible group over S. Both $X^*(T)$ and $X_*(T)$ are smooth $\mathbb{Z}_p$-sheaves of rank $\dim(T/S)$ on $S_{\text{ét}}$, and they are naturally dual to each other.

Definition 2.16. Let S be either a scheme such that p is locally nilpotent in $\mathcal{O}_S$, or an adic formal scheme such that p is locally topologically nilpotent in $\mathcal{O}_S$. A p-divisible group $X \to S$ is *ordinary* if X sits in the middle of a short exact sequence

$$0 \to T \to X \to E \to 0$$

where T (resp. E) is a multiplicative (resp. étale) p-divisible group. Such an exact sequence is unique up to unique isomorphism.

Remark. Suppose that X is an ordinary p-divisible group over $S = \mathrm{Spec}(K)$, where K is a perfect field $K \supset \mathbb{F}_p$. Then there exists a unique splitting of the short exact sequence $0 \to T \to X \to E \to 0$ over K.

Proposition 2.17. $\boxed{\text{BB}}$ *Suppose that S is a scheme over $W(K)$ and p is locally nilpotent in $\mathcal{O}_S$. Let $S_0 = \underline{\mathrm{Spec}}(\mathcal{O}_S/p\mathcal{O}_S)$, the closed subscheme of S defined by the ideal $p\mathcal{O}_S$ of the structure sheaf $\mathcal{O}_S$. If $X \to S$ is a p-divisible group such that $X \times_S S_0$ is ordinary, then $X \to S$ is ordinary.*

Proposition 2.17 is a consequence of the rigidity of finite étale group schemes and commutative finite group schemes of multiplicative type. See SGA3, Exposé X.

2.18. We set up notation for Theorem 2.19 on the theory of Serre-Tate local coordinates. Let $K \supset \mathbb{F}_p$ be a perfect field and let X_0 be an ordinary p-divisible group over K. This means that there is a natural split short exact sequence

$$0 \to T_0 \to X_0 \to E_0 \to 0$$

where T_0 (resp. E_0) is a multiplicative (resp. étale) p-divisible group over K. Let

$$T_i \to \mathrm{Spec}(W(K)/p^i W(K)) \quad (\text{resp. } E_i \to \mathrm{Spec}(W(K)/p^i W(K)))$$

be the multiplicative (resp. étale) p-divisible group over $\mathrm{Spec}(W(K)/p^i W(K))$ which lifts T_0 (resp. E_0) for each $i \geq 1$. Both T_i and E_i are unique up to unique isomorphism. Taking the limit of $T_i[p^n]$ (resp. $E_i[p^i]$) as $i \to \infty$, we get a multiplicative (resp. étale) BT_n-group $T^\sim \to \mathrm{Spec}(W(K))$ (resp. $E^\sim \to \mathrm{Spec}(W(K))$) over $W(K)$.

Denote by $T^\wedge$ the formal torus over $W(K)$ attached to T_0. More explicitly, it is the scheme theoretic inductive limit of $T_i[p^n]$ as i and n both go to ∞; see also 10.9 (4) and 10.21. Another equivalent description is that $T^\wedge = X_*(T_0) \otimes_{\mathbb{Z}_p} \mathbb{G}_m^\wedge$, where $\mathbb{G}_m^\wedge$ is the formal completion of $\mathbb{G}_m \to \mathrm{Spec}(W(K))$ along its unit section, and $X_*(T_0)$ is the étale smooth free $\mathbb{Z}_p$-sheaf of rank $\dim(T_0)$ on the étale site $\mathrm{Spec}(K)_{\mathrm{\acute{e}t}}$, which is isomorphic to the étale sites $\big(\mathrm{Spec}(W(K)/p^i W(K))\big)_{\mathrm{et}}$ and $(\mathrm{Spec}W(K))_{\mathrm{\acute{e}t}}$ for all i because the étale topology is insensitive to nilpotent extensions.

Theorem 2.19 below says that the deformation space of an ordinary p-divisible group X_0 as above has a natural structure as a formal torus over $W(K)$, whose dimension is equal to the product of the heights of the étale part E_0 and the multiplicative part T_0.

Theorem 2.19. *Notation and assumption as above.*

(i) *Every deformation $X \to \mathrm{Spec}(R)$ of X_0 over an Artinian local $W(K)$-algebra R is an ordinary p-divisible group over R. Therefore X sits in the middle of a short exact sequence*

$$0 \to T^\sim \times_{\mathrm{Spec}(W(K))} \mathrm{Spec}(R) \to X \to E^\sim \times_{\mathrm{Spec}(W(K))} \mathrm{Spec}(R) \to 0\,.$$

(ii) *The deformation functor $\mathrm{Def}(X_0/W(K)$ has a natural structure, via the Baer sum construction, as a functor from $\mathrm{Art}_{W(K)}$ to the category AbG of abelian groups. In particular the unit element in $\mathrm{Def}(X_0/W(K)(R)$ corresponds to the p-divisible group*

$$\big(T^\sim \times_{\mathrm{Spec}(W(K))} E^\sim\big) \times_{\mathrm{Spec}(W(K))} \mathrm{Spec}(R)$$

over R.

(iii) *There is a natural isomorphism of functors*

$$\mathrm{Def}(X_0/W(K)) \xleftarrow{\sim} \underline{\mathrm{Hom}}_{\mathbb{Z}_p}(\mathrm{T}_p(E_0), T^\wedge) = \mathrm{T}_p(E_0)^\vee \otimes_{\mathbb{Z}_p} X_*(T_0) \otimes_{\mathbb{Z}_p} \mathbb{G}_m^\wedge$$
$$= \underline{\mathrm{Hom}}_{\mathbb{Z}_p}\big(\mathrm{T}_p(E_0) \otimes_{\mathbb{Z}_p} X^*(T_0), \mathbb{G}_m^\wedge\big)\,.$$

In other words, the deformation space $\mathrm{Def}(X_0/W(K))$ of X_0 has a natural structure as a formal torus over $W(K)$ whose cocharacter group is isomorphic to the $\mathrm{Gal}(K^{\mathrm{alg}}/K)$-module $\mathrm{T}_p(E)^\vee \otimes_{\mathbb{Z}_p} X_*(T_0)$.

PROOF. The statement (i) is follows from Proposition 2.17, so is (ii). It remains to prove (iii).

By étale descent, we may and do assume that K is algebraically closed. By (i), over any Artinian local $W(K)$-algebra R, we see that $\mathrm{Def}(X_0/W(K))(R)$ is the set of isomorphism classes of extensions of $E^\sim \times_{W(K)} \mathrm{Spec}(R)$ by $T^\sim \times_{W(K)} \mathrm{Spec}(R)$. Write T_0 (resp. E_0) as a product of a finite number of copies of $\mathbb{G}_m[p^\infty]$ (resp. $\mathbb{Q}_p/\mathbb{Z}_p$), we only need to verify the statement (iii) in the case when $T_0 = \mathbb{G}_m[p^\infty]$ and $E_0 = \mathbb{Q}_p/\mathbb{Z}_p$.

Let R be an Artinian local $W(K)$-algebra. We have seen that

$$\mathrm{Def}(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{G}_m[p^\infty])(R)$$

is naturally isomorphic to the inverse limit $\varprojlim_n \mathrm{Ext}^1_{\mathrm{Spec}(R),\mathbb{Z}/p^n\mathbb{Z}}(p^{-n}\mathbb{Z}/\mathbb{Z}, \mu_{p^n})$, where the Ext group is computed in the category of sheaves of $(\mathbb{Z}/p^n\mathbb{Z})$-modules for the flat topology on $\mathrm{Spec}(R)$. By Kummer theory, we have

$$\mathrm{Ext}^1_{\mathrm{Spec}(R),\mathbb{Z}/p^n\mathbb{Z}}(p^{-n}\mathbb{Z}/\mathbb{Z}, \mu_{p^n}) = R^\times/(R^\times)^{p^n} = (1 + \mathfrak{m}_R)/(1 + \mathfrak{m}_R)^{p^n}\,;$$

the second equality follows from the hypothesis that K is perfect. One checks that the map

$$\mathrm{Ext}^1_{\mathrm{Spec}(R),\mathbb{Z}/p^{n+1}\mathbb{Z}}(p^{-n-1}\mathbb{Z}/\mathbb{Z},\mu_{p^{n+1}}) \to \mathrm{Ext}^1_{\mathrm{Spec}(R),\mathbb{Z}/p^n\mathbb{Z}}(p^{-n}\mathbb{Z}/\mathbb{Z},\mu_{p^n})$$

obtained by "restriction to the subgroup of $[p^n]$-torsions" corresponds to the natural surjection

$$(1+\mathfrak{m}_R)/(1+\mathfrak{m}_R)^{p^{n+1}} \twoheadrightarrow (1+\mathfrak{m}_R)/(1+\mathfrak{m}_R)^{p^n}.$$

We know that $p \in \mathfrak{m}_R$ and $\mathfrak{m}_R$ is nilpotent. Hence there exists an n_0 such that $(1+\mathfrak{m}_R)^{p^n} = 1$ for all $n \geq n_0$. Taking the inverse limit as $n \to \infty$, we see that the natural map

$$1+\mathfrak{m}_R \to \varprojlim_n \mathrm{Ext}^1_{\mathrm{Spec}(R),\mathbb{Z}/p^n\mathbb{Z}}(p^{-n}\mathbb{Z}/\mathbb{Z},\mu_{p^n})$$

is an isomorphism. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Corollary 2.20. *Let $K \supset \mathbb{F}_p$ be a perfect field, and let A_0 be an ordinary abelian variety. Let $\mathrm{T}_p(A_0) := \mathrm{T}_p(A_0[p^\infty]_{\mathrm{ét}})$, $\mathrm{T}_p(A_0^t) := \mathrm{T}_p(A_0^t[p^\infty]_{\mathrm{ét}})$. Then*

$$\mathrm{Def}(A_0/W(K)) \cong \underline{\mathrm{Hom}}_{\mathbb{Z}_p}(\mathrm{T}_p(A_0) \otimes_{\mathbb{Z}_p} \mathrm{T}_p(A_0^t), \mathbb{G}_m^\wedge).$$

Exercise 2.21. Let R be a commutative ring with 1. Compute

$$\mathrm{Ext}^1_{\mathrm{Spec}(R),(\mathbb{Z}/n\mathbb{Z})}(n^{-1}\mathbb{Z}/\mathbb{Z},\mu_n),$$

the group of isomorphism classes of extensions of the constant group scheme $n^{-1}\mathbb{Z}/\mathbb{Z}$ by μ_n over $\mathrm{Spec}(R)$ in the category of finite flat group schemes over $\mathrm{Spec}(R)$ which are killed by n.

Notation. Let R be an Artinian local $W(k)$-algebra, where $k \supset \mathbb{F}_p$ is an algebraically closed field. Let $X \to \mathrm{Spec}(R)$ be an ordinary p-divisible group such that the closed fiber $X_0 := X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(k)$ is an ordinary p-divisible group over k. Denote by $q(X/R;\cdot,\cdot)$ the $\mathbb{Z}_p$-bilinear map

$$q(X/R;\cdot,\cdot) : \mathrm{T}_p(X_{0,\mathrm{ét}}) \times \mathrm{T}_p(X_{0,\mathrm{ét}}^t) \to 1+\mathfrak{m}_R$$

correspond to the deformation $X \to \mathrm{Spec}(R)$ of the p-divisible group X_0 as in Corollary 2.20. Here we have used the natural isomorphism $X^*(X_{0,\mathrm{mult}}) \cong \mathrm{T}_p(X_{0,\mathrm{ét}}^t)$, so that the Serre-Tate coordinates for the p-divisible group $X \to \mathrm{Spec}(R)$ is a $\mathbb{Z}_p$-bilinear map $q(X/R;\cdot,\cdot)$ on $\mathrm{T}_p(X_{0,\mathrm{ét}}) \times \mathrm{T}_p(X_{0,\mathrm{ét}}^t)$. The abelian group $1+\mathfrak{m}_R \subset R^\times$ is regarded as a $\mathbb{Z}_p$-module, so "$\mathbb{Z}_p$-bilinear" makes sense. Let $\mathrm{can} : X_0 \xrightarrow{\sim} (X_0^t)^t$ be the canonical isomorphism from X_0 to its double Serre dual, and let $\mathrm{can}_* : \mathrm{T}_p(X_{0,\mathrm{ét}}) \xrightarrow{\sim} \mathrm{T}_p((X_0^t)_{\mathrm{ét}}^t)$ be the isomorphism induced by can.

The relation between the Serre-Tate coordinate $q(X/R;\cdot,\cdot)$ of a deformation of X_0 and the Serre-Tate coordinates $q(X^t/R;\cdot,\cdot)$ of the Serre dual X^t of X is given by 2.22. The proof is left as an exercise.

Lemma 2.22. *Let $X \to \mathrm{Spec}(R)$ be an ordinary p-divisible group over an Artinian local $W(k)$-algebra R. Then we have*

$$q(X;u,v_t) = q(X^t;v_t,\mathrm{can}_*(u)) \qquad \forall u \in \mathrm{T}_p(X_{0,\mathrm{ét}}),\ \forall v \in \mathrm{T}_p(X_{0,\mathrm{ét}}^t).$$

The same statement holds when the ordinary p-divisible group $X \to \mathrm{Spec}(R)$ is replaced by an ordinary abelian scheme $A \to \mathrm{Spec}(R)$.

From the functoriality of the construction in 2.19, it is not difficult to verify the following.

Proposition 2.23. *Let X_0, Y_0 be ordinary p-divisible groups over a perfect field $K \supset \mathbb{F}$. Let R be an Artinian local ring over $W(K)$. Let $X \to \mathrm{Spec}(R)$, $Y \to \mathrm{Spec}(R)$ be abelian schemes whose closed fibers are X_0 and Y_0 respectively. Let $q(X/R; \cdot, \cdot)$, $q(Y/R; \cdot, \cdot)$ be the Serre-Tate coordinates for X and Y respectively. Let $\beta : X_0 \to Y_0$ be a homomorphism of abelian varieties over k. Then β extends to a homomorphism from X to Y over $\mathrm{Spec}(R)$ if and only if*

$$q(X/R; u, \beta^t(v_t)) = q(Y/R; \beta(u), v_t) \quad \forall u \in \mathrm{T}_p(X_0),\ \forall v_t \in \mathrm{T}_p(Y_0^t).$$

Corollary 2.24. *Let A_0 be an ordinary abelian variety over a perfect field $K \supset \mathbb{F}_p$. Let $\lambda_0 : A_0 \to A_0^t$ be a polarization on A_0. Then*

$$\mathrm{Def}((A_0, \lambda_0)/W(K)) \cong \underline{\mathrm{Hom}}_{\mathbb{Z}_p}(S, \mathbb{G}_m{}^\wedge),$$

where S is defined as

$$\mathrm{T}_p(A_0[p^\infty]_{\text{ét}}) \otimes_{\mathbb{Z}_p} \mathrm{T}_p(A_0^t[p^\infty]_{\text{ét}}) \Big/ \big(u \otimes \mathrm{T}_p(\lambda_0)(v) - v \otimes \mathrm{T}_p(\lambda_0)(u)\big)_{u,v \in \mathrm{T}_p(A[p^\infty]_{\text{ét}})}.$$

Exercise 2.25. Notation as in 2.24. Let $p^{e_1}, \ldots, p^{e_g}$ be the elementary divisors of the $\mathbb{Z}_p$-linear map $\mathrm{T}_p(\lambda_0) : \mathrm{T}_p(A_0[p^\infty]_{\text{ét}}) \to \mathrm{T}_p(A_0^t[p^\infty]_{\text{ét}})$, $g = \dim(A_0)$, $e_1 \leq e_2 \leq \cdots \leq e_g$. The torsion submodule S_{torsion} of S is isomorphic to $\bigoplus_{1 \leq i < j \leq g} (\mathbb{Z}_p/p^{e_i}\mathbb{Z}_p)$.

Theorem 2.26. $\boxed{\textbf{BB}}$ *(local rigidity) Let $k \supset \mathbb{F}_p$ be an algebraically closed field. Let*

$$T \cong ((\mathbb{G}_m^\wedge)^n = \mathrm{Spf}\, k[[u_1, \ldots, u_n]]$$

be a formal torus, with group law given by

$$u_i \ \mapsto \ u_i \otimes 1 + 1 \otimes u_i + u_i \otimes u_i \qquad i = 1, \ldots n.$$

Let $X = \mathrm{Hom}_k(\mathbb{G}_m^\wedge, T) \cong \mathbb{Z}_p^n$ be the cocharacter group of T; notice that $\mathrm{GL}(X)$ operates naturally on T. Let $G \subset \mathrm{GL}(X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \cong \mathrm{GL}_n$ be a reductive linear algebraic subgroup over $\mathbb{Q}_p$. Let Z be an irreducible closed formal subscheme of T which is stable under the action of an open subgroup U of $G(\mathbb{Q}_p) \cap \mathrm{GL}(X)$. Then Z is a formal subtorus of T.

See Theorem 6.6 of [**7**] for a proof of 2.26; see also [**12**].

Corollary 2.27. *Let $x_0 = [(A_0, \lambda_0, \eta_0)] \in \mathcal{A}_{g,1,n}(\mathbb{F})$ be an $\mathbb{F}$-point of $\mathcal{A}_{g,1,n}$, where $\mathbb{F}$ is the algebraic closure of $\mathbb{F}_p$. Assume that the abelian variety A_0 is ordinary. Let $Z(x_0)$ be the Zariski closure of the prime-to-p Hecke orbit $\mathcal{H}_{\mathrm{Sp2g}}^{(p)}(x_0)$ on $\mathcal{A}_{g,1,n}$. The formal completion $Z(x_0)^{/x_0}$ of $Z(x_0)$ at x_0 is a formal subtorus of the Serre-Tate formal torus $\mathcal{A}_{g,1,n}^{/x_0}$.*

PROOF. This is immediate from 2.26 and the local stabilizer principle; see 9.5 for the statement of the local stabilizer principle. $\qquad\square$

Remark. Corollary 2.27 puts a serious restriction on the Zariski closure $Z(x_0)$ of the Hecke orbit of an ordinary point x_0 in $\mathcal{A}_{g,1,n}(\mathbb{F})$. In fact the argument shows that the formal completion of $Z(x_0)$ at any closed point y_0 of the smooth ordinary locus of Z_{x_0} is a formal subtorus of the Serre-Tate torus at y_0. This constitutes the linearization step toward proving that $Z(x_0) = A_{g,1,n}$. See Proposition 6.14 and Step 4 of the proof of Theorem 9.2, where Theorem 2.26 plays a crucial role.

3. The Tate-conjecture: ℓ-adic and p-adic

Most results of this section will not be used directly in our proofs. However, this is such a beautiful part of mathematics that we wish to tell more than we really need.

Basic references: [**79**] and [**37**]; [**78**], [**19**], [**62**].

3.1. Let A be an abelian variety over a field K of arbitrary characteristic. The ring $\text{End}(A)$ is an algebra over $\mathbb{Z}$, which has no torsion, and which is free of finite rank as $\mathbb{Z}$-module. We write $\text{End}^0(A) = \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Let $\mu : A \to A^t$ be a polarization. An endomorphism $x : A \to A$ defines $x^t : A^t \to A^t$. We define an anti-involution

$$^{\dagger} : \text{End}^0(A) \to \text{End}^0(A), \quad \text{by} \quad x^t \cdot \mu = \mu \cdot x^{\dagger},$$

called the *Rosati involution*; see 10.13. In case μ is a principal polarization the Rosati involution maps $\text{End}(A)$ into itself.

The Rosati involution is *positive definite* on $D := \text{End}^0(A)$, meaning that $x \mapsto \text{Tr}(x \cdot x^{\dagger})$ is a positive definite quadratic form on $\text{End}^0(A)$; for references see Proposition II in 3.10. Such algebras have been classified by Albert, see 10.14.

Definition 3.2. A field L is said to be a CM-field if L is a finite extension of $\mathbb{Q}$ (hence L is a number field), and there is a subfield $L_0 \subset L$ such that $L_0/\mathbb{Q}$ is totally real (i.e., every $\psi_0 : L_0 \to \mathbb{C}$ gives $\psi_0(L_0) \subset \mathbb{R}$) *and* L/L_0 *is quadratic totally imaginary* (i.e., $[L : L_0] = 2$ and for every $\psi : L \to \mathbb{C}$ we have $\psi(L) \not\subset \mathbb{R}$.

Equivalently, L is a CM-field if there exists an element of order 2 in the center of the Galois group $\text{Gal}(M/\mathbb{Q})$ of the Galois closure M of L over $\mathbb{Q}$, which is equal to the complex conjugation for every archimedean place of M.

Remark. The quadratic extension L/L_0 gives an involution $\iota \in \text{Aut}(L/L_0)$. For every embedding $\psi : L \to \mathbb{C}$ this involution corresponds with the restriction of complex conjugation on $\mathbb{C}$ to $\psi(L)$.

Even more is known about the endomorphism algebra of an abelian variety over a finite field. Tate showed that

Theorem 3.3. (Tate) *An abelian variety over a finite field admits* sufficiently many Complex Multiplications.

This is equivalent with: *Let A be a simple abelian variety over a finite field. Then there is a* CM-*field of degree* $2 \cdot \dim(A)$ *contained in* $\text{End}^0(A)$.

A proof can be found in [**78**], [**79**]; also see 10.17 for a stronger statement. See 10.15 for the definition of "abelian varieties with sufficiently many Complex Multiplications". A consequence of this theorem is the following.

Let A be an abelian variety over $\mathbb{F} = \overline{\mathbb{F}_p}$. Suppose that A is simple, and hence that $\text{End}^0(A)$ is a division algebra; this algebra has finite rank over $\mathbb{Q}$; the possible structures of endomorphism algebras of an abelian variety have been classified by Albert, see 10.14. In this case

- either A is a supersingular elliptic curve, and $D := \text{End}^0(A) = \mathbb{Q}_{p,\infty}$, which is the (unique) quaternion algebra central over $\mathbb{Q}$, which is unramified for every finite prime $\ell \neq p$, i.e., $D \otimes \mathbb{Q}_\ell$ is the 2×2 matrix algebra over $\mathbb{Q}_\ell$, and $D/\mathbb{Q}$ is ramified at p and at ∞; here D is of Albert Type III(1);

- or A is not a supersingular elliptic curve; in this case D is of Albert Type IV(e_0, d) with $e_0 \cdot d = g := \dim(A)$.

In particular (to be used later).

Corollary 3.4. *Let A be an abelian variety over $\mathbb{F} := \overline{\mathbb{F}_p}$. There exists $E = F_1 \times \cdots \times F_r$, a product of totally real fields, and an injective homomorphism $E \hookrightarrow \mathrm{End}^0(A)$ such that $\dim_{\mathbb{Q}}(E) = \dim(A)$.*

Examples.   (1) E is a supersingular elliptic curve over $K = \mathbb{F}_q$. Then either $D := \mathrm{End}^0(E)$ is isomorphic with $\mathbb{Q}_{p,\infty}$, or D is an imaginary quadratic field over $\mathbb{Q}$ in which p is not split.

   (2) E is a non-supersingular elliptic curve over $K = \mathbb{F}_q$. Then $D := \mathrm{End}^0(E)$ is an imaginary quadratic field over $\mathbb{Q}$ in which p is split.

   (3) If A is simple over $K = \mathbb{F}_q$ such that $D := \mathrm{End}^0(A)$ is commutative, then $D = L = \mathrm{End}^0(A)$ is a CM-field of degree $2 \cdot \dim(A)$ over $\mathbb{Q}$.

   (4) In characteristic zero the endomorphism algebra of a simple abelian variety which admits smCM is *commutative*. However in positive characteristic an Albert Type IV(e_0, d) with $e_0 > 1$ can appear. For example, see [**79**], page 67: for any prime number $p > 0$, and for any $g > 2$ there exists a simple abelian variety over $\mathbb{F}$ such that $D = \mathrm{End}^0(A)$ is a division algebra of rank g^2 over its center L, which is a quadratic imaginary field over $\mathbb{Q}$.

3.5. Weil numbers and CM-fields.

Definition. Let p be a prime number, $n \in \mathbb{Z}_{>0}$; write $q = p^n$. A Weil q-number is an algebraic integer π such that for every embedding $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have

$$|\psi(\pi)| \quad = \quad \sqrt{q}.$$

We say that π and π' are *conjugated* if there exists an isomorphism $\mathbb{Q}(\pi) \cong \mathbb{Q}(\pi')$ mapping π to π'.
Notation: $\pi \sim \pi'$. We write $W(q)$ for the set of Weil q-numbers and $W(q)/\sim$ for the set of conjugacy classes of Weil q-numbers.

Proposition 3.6. *Let π be a Weil q-number. Then*
(I) *either for at least one $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\pm\sqrt{q} = \psi(\pi) \in \mathbb{R}$; in this case we have:*
(Ie) *n is even, $\sqrt{q} \in \mathbb{Q}$, and $\pi = +p^{n/2}$, or $\pi = -p^{n/2}$; or*
(Io) *n is odd, $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$, and $\psi(\pi) = \pm p^{n/2}$.*
In particular in case (I) we have $\psi(\pi) \in \mathbb{R}$ for every ψ.
(II) *Or for every $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\psi(\pi) \notin \mathbb{R}$ (equivalently: for at least one ψ we have $\psi(\pi) \notin \mathbb{R}$). In case (II) the field $\mathbb{Q}(\pi)$ is a CM-field.*

PROOF. Exercise.

Remark 3.7. We see a characterization of Weil q-numbers. In case (I) we have $\pi = \pm\sqrt{q}$. If $\pi \notin \mathbb{R}$:

$$\beta := \pi + \frac{q}{\pi} \quad \text{is totally real,}$$

and π is a zero of

$$T^2 - \beta \cdot T + q, \quad \text{with} \quad \beta < 2\sqrt{q}.$$

In this way it is easy to construct Weil q-numbers.

3.8. Let A be an abelian variety over a finite field $K = \mathbb{F}_q$ with $q = p^n$. Let $F : A \to A^{(p)}$ be the relative Frobenius morphism for A. Iterating this Frobenius map n times, observing there is a canonical identification $A^{(p^n)} = A$, we obtain $(\pi : A \to A) \in \mathrm{End}(A)$. If A is simple, the subring $\mathbb{Q}(\pi) \subset \mathrm{End}^0(A)$ is a subfield, and we can view π as an algebraic integer.

Theorem 3.9. $\boxed{\textbf{Extra}}$ (Weil) *Let $K = \mathbb{F}_q$ be a finite field, let A be a simple abelian variety over K. Then π is a Weil q-number.*

This is the famous "Weil conjecture" for an abelian variety over a finite field. See [**86**], page 70; [**87**], page 138; [**54**], Theorem 4 on page 206.

Exercise 3.10. Use Propositions I and II below to prove the following statements, thereby proving Theorem 3.9.

  (i) *Suppose that A is a simple abelian variety over a field K, and let $L = \mathrm{Centre}(\mathrm{End}^0(A))$. A Rosati involution on $D := \mathrm{End}^0(A)$ induces the complex conjugation on L (for every embedding $L \hookrightarrow \mathbb{C}$).*
  (ii) *If moreover K is a finite field, $\pi = \pi_A$ is a Weil q-number.*

Proposition. I. *For a simple abelian variety A over $K = \mathbb{F}_q$ we have*

$$\pi_A \cdot (\pi_A)^{\dagger} = q.$$

Here $\dagger : D \to D := \mathrm{End}^0(A)$ is the Rosati involution attached to a polarization of A.

One proof can be found in [**54**], formula (i) on page 206; also see [**16**], Corollary 19.2 on page 144.

Another proof of (I) can be given by duality. We have

$$\left(F_{A/S} : A \to A^{(p)} \right)^t \quad = \quad V_{A^t/S} : (A^{(p)})^t \to A^t,$$

where $V_{A^t/S}$ is the Verschiebung of the abelian scheme A^t/S dual to A/S; see 10.24. From this formula we see that

$$\pi_{A^t} \cdot (\pi_A)^t = (F_{A^t})^n \cdot (V_{A^t})^n = p^n = q,$$

where we use the shorthand notation F^n for the n times iterated relative Frobenius morphism, and the same for V^n. See [GM], 5.21, 7.34 and Section 15. $\square$

Proposition. II. *For any polarized abelian variety A over a field the Rosati involution $\dagger : D \to D := \mathrm{End}^0(A)$ is a positive definite bilinear form on D, i.e., for any non-zero $x \in D$ we have $\mathrm{Tr}(x \cdot x^{\dagger}) > 0$.*

See [**54**], Theorem 1 on page 192, see [**16**], Theorem 17.3 on page 138.

Remark 3.11. Given $\pi = \pi_A$ of a simple abelian variety over $\mathbb{F}_q$ one can determine the structure of the division algebra $\mathrm{End}^0(A)$, see [**79**], Theorem 1. See 10.17.

Theorem 3.12. $\boxed{\textbf{Extra}}$ (Honda and Tate) *By $A \mapsto \pi_A$ we obtain a bijective map*

$$\{abelian\ varieties\ simple\ over\ \mathbb{F}_q\}/\sim_{\mathbb{F}_q} \quad \xrightarrow{\sim} \quad W(q)/\sim$$

between the set of $\mathbb{F}_q$-isogeny classes of abelian varieties simple over $\mathbb{F}_q$ and the set of conjugacy classes of Weil q-numbers.

See [**79**], Theorem 1 on page 96.

3.13. Let π be a Weil q-number. Let $\mathbb{Q} \subset L \subset D$ be the central algebra determined by π. It is known that

$$[L : \mathbb{Q}] =: e, \quad [D : L] =: d^2, \quad 2g := e \cdot d. \qquad \text{See 10.12.}$$

As we have seen in Proposition 3.6 there are three possibilities:

($\mathbb{R}$e) *Either $\pi = \sqrt{q} \in \mathbb{Q}$, and $q = p^n$ with n an **even** positive integer.*

$\boxed{\text{Type III}(1), \quad g = 1}$

In this case $\pi = +p^{n/2}$, or $\pi = -p^{n/2}$. Hence $L = L_0 = \mathbb{Q}$. We see that $D/\mathbb{Q}$ has rank 4, with ramification exactly at ∞ and at p. We obtain $g = 1$, we have that $A = E$ is a supersingular elliptic curve, $\text{End}^0(A)$ is of Type III(1), a definite quaternion algebra over $\mathbb{Q}$. This algebra was denoted by Deuring as $\mathbb{Q}_{p,\infty}$. Note that "all endomorphisms of E are defined over K", i.e., for any

$$\forall \quad K \subset K' \quad \text{we have} \quad \text{End}(A) = \text{End}(A \otimes K').$$

($\mathbb{R}$o) *Or $q = p^n$ with n an **odd** positive integer, $\pi = \sqrt{q} \in \mathbb{R} \notin \mathbb{Q}$.*

$\boxed{\text{Type III}(2), \quad g = 2}$

In this case $L_0 = L = \mathbb{Q}(\sqrt{p})$, a real quadratic field. We see that D ramifies exactly at the two infinite places with invariants equal to $(n/2) \cdot 2/(2n) = 1/2$. Hence D/L_0 is a definite quaternion algebra over L_0; it is of Type III(2). We conclude $g = 2$. If $K \subset K'$ is an extension of odd degree we have $\text{End}(A) = \text{End}(A \otimes K')$. If $K \subset K'$ is an extension of even degree, $A \otimes K'$ is non-simple, it is K'-isogenous to a product of two supersingular elliptic curves, and $\text{End}^0(A \otimes K')$ is a 2×2 matrix algebra over $\mathbb{Q}_{p,\infty}$, and

$$\forall K' \quad \text{with} \quad 2 \mid [K' : K] \quad \text{we have} \quad \text{End}(A) \neq \text{End}(A \otimes K').$$

($\mathbb{C}$) *For at least one embedding $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\psi(\pi) \notin \mathbb{R}$.*

$\boxed{\text{Type IV}(e_0, d), \quad g := e_0 \cdot d}$

In this case all conjugates of $\psi(\pi)$ are non-real. We can determine $[D : L]$ knowing all $v(\pi)$ by 10.17 (3); here d is the greatest common divisor of all denominators of $[L_v : \mathbb{Q}_p] \cdot v(\pi)/v(q)$, for all $v \mid p$. This determines $2g := e \cdot d$. The endomorphism algebra is of Type IV(e_0, d). For $K = \mathbb{F}_q \subset K' = \mathbb{F}_{q^m}$ we have

$$\text{End}(A) = \text{End}(A \otimes K') \quad \Longleftrightarrow \quad \mathbb{Q}(\pi) = \mathbb{Q}(\pi^m).$$

Exercise 3.14. Let $m, n \in \mathbb{Z}$ with $m > n > 0$; write $g = m + n$ and $q = p^g$. Consider the polynomial $T^2 + p^n T + p^g$, and let π be a zero of this polynomial.

(a) *Show that π is a p^g-Weil number; compute the p-adic values of all conjugates of π.*

(b) By the previous theorem we see that π defines the isogeny class of an abelian variety A over $\mathbb{F}_q$. It can be shown that A has dimension g, and that $\mathcal{N}(A) = (m, n) + (n, m)$, see [**79**], page 98. *This gives a proof of a conjecture of Manin,* see 5.21.

3.15. ℓ-adic monodromy. (Any characteristic.) Let K be a base field, of any characteristic. Write $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Let ℓ be a prime number, not equal to $\mathrm{char}(K)$. Note that this implies that $T_\ell(A) = \varprojlim_j A[\ell^j](K^{\mathrm{sep}})$ can be considered as a group isomorphic with $(\mathbb{Z}_\ell)^{2g}$ with a continuous G_K-action. See 10.5, 10.8.

Theorem 3.16. $\boxed{\text{Extra}}$ (Tate, Faltings, and many others) *Suppose K is of finite type over its prime field. (Any characteristic.) The canonical map*

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \quad \xrightarrow{\sim} \quad \mathrm{End}(T_\ell(A)) \cong \mathrm{End}_{G_K}((\mathbb{Z}_\ell)^{2g})$$

is an isomorphism.

This was conjectured by Tate. In 1966 Tate proved this in case K is a finite field, see [**78**]. The case of function fields in characteristic p was proved by Zarhin and by Mori, see [**90**], [**91**], [**52**]; also see [**51**], pp. 9/10 and VI.5 (pp. 154-161).

The case K is a number field was open for a long time; it was finally proved by Faltings in 1983, see [**26**]. For the case of a function field in characteristic zero, see [**29**], Theorem 1 on page 204.

Remark 3.17. $\boxed{\text{Extra}}$ The previous result holds over a number field, but the Tate map need not be an isomorphism for an abelian variety over a local field.

Example. Lubin and Tate, see [**47**], 3.5; see [**63**], 14.9. *There exists a finite extension $L \supset \mathbb{Q}_p$ and an abelian variety over L such that*

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \quad \subsetneq \quad \mathrm{End}(T_\ell(A)).$$

We give details of a proof of this fact (slightly more general than in the paper by Lubin and Tate). Choose a prime number p, and choose a supersingular elliptic curve E_0 over $K = \mathbb{F}_q$ such that the endomorphism ring $R := \mathrm{End}(E_0)$ has rank 4 over $\mathbb{Z}$. In that case R is a maximal order in the endomorphism algebra $D := \mathrm{End}^0(E_0)$, which is a quaternion division algebra central over $\mathbb{Q}$. Let I be the index set of all subfields L_i of D, and let

$$\Lambda := \bigcup_{i \in I} (L_i \otimes \mathbb{Q}_p) \subset D \otimes \mathbb{Q}_p.$$

CLAIM.

$$\Lambda \subsetneq D_p := D \otimes \mathbb{Q}_p.$$

Indeed, the set I is countable, and $[L_i : \mathbb{Q}] \leq 2$ for every i. Hence Λ is a countable union of 2-dimensional $\mathbb{Q}_p$-vector spaces inside $D_p \cong (\mathbb{Q}_p)^4$. The claim follows.

Hence we can choose $\psi_0 \in R_p := R \otimes \mathbb{Z}_p$ such that $\psi_0 \notin \Lambda$: first choose ψ_0' in D_p outside Λ, then multiply with a power of p in order to make $\psi_0 = p^n \cdot \psi_0'$ integral.

Consider $X_0 := E_0[p^\infty]$. The pair (X_0, ψ_0) can be lifted to characteristic zero, see [**63**], Lemma 14.7, hence to (X, ψ) defined over an order in a finite extension L of $\mathbb{Q}_p$. We see that $\mathrm{End}^0(X) = \mathbb{Q}_p(\psi)$, which is a quadratic extension of $\mathbb{Q}_p$. By the theorem of Serre and Tate, see 2.7, we derive an elliptic curve E, which is a lifting of E_0, such that $E[p^\infty] = X$. Clearly $\mathrm{End}(E) \otimes \mathbb{Z}_p \subset \mathrm{End}(X)$.

CLAIM. $\mathrm{End}(E) = \mathbb{Z}$.
In fact, if $\mathrm{End}(E)$ were bigger, we would have $\mathrm{End}(E) \otimes \mathbb{Z}_p = \mathrm{End}(X)$. Hence

$\psi \in \mathrm{End}^0(E) \subset \Lambda$, which is a contradiction. This finishes the proof of the example:

$$\mathrm{End}(E) = \mathbb{Z} \quad \text{and} \quad \dim_{\mathbb{Q}_p} \mathrm{End}^0(X) = 2 \quad \text{and} \quad \mathrm{End}(E) \otimes \mathbb{Z}_p \subsetneqq \mathrm{End}(X).$$

However, surprise, in the "anabelian situation" of a hyperbolic curve over a p-adic field, the analogous situation, gives an isomorphism for fundamental groups, see [50]. We see: the Tate conjecture as in 3.16 does not hold over p-adic fields but the Grothendieck "anabelian conjecture" is true for hyperbolic curves over p-adic fields. Grothendieck took care to formulate his conjecture with a number field as base field, see [75], page 19; we see that this care is necessary for the original Tate conjecture for abelian varieties, but for hyperbolic curves this condition can be relaxed.

3.18. We would like to have a p-adic analogue of 3.16. For this purpose it is convenient to have p-divisible groups instead of Tate ℓ-groups, and in fact the following theorem now has been proved to be true.

Theorem 3.19. ⃞BB⃞ (Tate and De Jong) *Let R be an integrally closed, Noetherian integral domain with field of fractions K (any characteristic). Let X, Y be p-divisible groups over $\mathrm{Spec}(R)$. Let $\beta_K : X_K \to Y_K$ be a homomorphism. There exists (a unique) $\beta : X \to Y$ over $\mathrm{Spec}(R)$ extending β_K.*

This was proved by Tate, under the extra assumption that the characteristic of K is zero. For the case $\mathrm{char}(K) = p$, see [19], 1.2 and [18], Theorem 2 on page 261.

Theorem 3.20. ⃞BB⃞ (Tate and De Jong) *Let K be a field finitely generated over $\mathbb{F}_p$. Let A and B be abelian varieties over K. The natural map*

$$\mathrm{Hom}(A, B) \otimes \mathbb{Z}_p \quad \xrightarrow{\sim} \quad \mathrm{Hom}(A[p^\infty], B[p^\infty])$$

is an isomorphism.

This was proved by Tate in case K is a finite field; a proof was written up in [85]. The case of a function field over $\mathbb{F}_p$ was proved by Johan de Jong, see [19], Theorem 2.6. This case follows from the result by Tate and from the proceeding result 3.19 on extending homomorphisms.

3.21. Ekedahl-Oort strata. ⃞BB⃞ In [67] a new technique is developed, which will be used below. We sketch some of the details of that method. We will only indicate details relevant for the polarized case (and we leave aside the much easier unpolarized case).

A finite group scheme N (say over a perfect field) for which $N[V] = \mathrm{Im}(F_N)$ and $N[F] = \mathrm{Im}(V_N)$ is called a BT_1 group scheme (a p-divisible group scheme truncated at level 1). By a theorem of Kraft, independently observed by Oort, for a given rank over an algebraically closed field k the number of isomorphism classes of BT_1 group schemes is finite, see [43]. For any abelian variety A, the group scheme $A[p]$ is a BT_1 group scheme. A principal polarization λ on A induces a form on $A[p]$, and the pair $(A, \lambda)[p]$ is a polarized BT_1 group scheme, see [67], Section 9 (there are subtleties in case $p = 2$: the form has to be taken, over a perfect field, on the Dieudonné module of $A[p]$).

3.21.1. *The number of isomorphism classes of polarized BT_1 group schemes* $(N, \langle, \rangle)$ *over k of a given rank is finite; see the classification in* [**67**], *9.4.*

Let φ be the isomorphism type of a polarized BT_1 group scheme. Consider $S_\varphi \subset \mathcal{A}_{g,1}$, the set of all $[(A, \lambda)]$ such that $(A, \lambda)[p]$ geometrically belongs to the isomorphism class φ.

3.21.2. *It can be shown that S_φ is a locally closed set*; it is called an EO-stratum. We obtain $\mathcal{A}_{g,1} = \bigsqcup_\varphi S_\varphi$, a disjoint union of locally closed sets. *This is a stratification*, in the sense that *the boundary of a stratum is a union of lower dimensional strata.*

One of the main theorems of this theory is that

3.21.3. *The set S_φ is quasi-affine* (i.e., open in an affine scheme) *for every φ*, see [**67**], 1.2.

The finite set Φ_g of such isomorphism types has two partial orderings, see [**67**], 14.3. One of these, denoted by $\varphi \subset \varphi'$, is defined by the property that S_φ is contained in the Zariski closure of $S_{\varphi'}$.

3.22. An application. *Let $x \in \mathcal{A}_{g,1}$. Let*

$$\left(\mathcal{H}_\ell^{\mathrm{Sp}}(x) \right)^{\mathrm{Zar}} = (\mathcal{H}_\ell(x) \cap \mathcal{A}_{g,1})^{\mathrm{Zar}} \quad \subset \quad \mathcal{A}_{g,1}$$

be the Zariski closure of the ℓ-power Hecke orbit of x in $\mathcal{A}_{g,1}$. This closed set in $\mathcal{A}_{g,1}$ contains a supersingular point.

Use 3.21 and the second part of 1.14.   □

4. Dieudonné modules and Cartier modules

In this section we explain the theory of Cartier modules and Dieudonné modules. These theories provide equivalence of categories of geometric objects such as commutative smooth formal groups or p-divisible groups on the one side, and modules over certain non-commutative rings on the other side. As a result, questions on commutative smooth formal groups or p-divisible groups, which are apparently non-linear in nature, are translated into questions in linear algebra over rings. Such results are essential for any serious computation.

There are many versions and flavors of Dieudonné theory. We explain the Cartier theory for commutative smooth formal groups over general commutative rings, and the covariant Dieudonné modules for p-divisible groups over perfect fields of characteristic $p > 0$. Since the Cartier theory works over general commutative rings, one can "write down" explicit deformations over complete rings such as $k[[x_1, \ldots, x_n]]$ or $W(k)[[x_1, \ldots, x_n]]$, something rarely feasible in algebraic geometry. For our purpose it is those commutative formal groups which are formal completions of p-divisible groups that are really relevant; see 10.9 for the relation between such p-divisible formal groups and the connected p-divisible groups.

Remarks on notation:

    (i) In the first part of this section, on Cartier theory, R denotes a commutative ring with 1, or a commutative $\mathbb{Z}_{(p)}$-algebra with 1.

   (ii) In this section, we used V and F as elements in the Cartier ring $\mathrm{Cart}_p(R)$ or the smaller Dieudonné ring $R_K \subset \mathrm{Cart}_p(R)$ for a perfect field K. In the rest of this article, the notations $\mathcal{V}$ and $\mathcal{F}$ are used; $\mathcal{V}$ corresponds to

the relative Frobenius morphism and $\mathcal{F}$ corresponds to the Verschiebung morphisms for commutative smooth formal groups or p-divisible groups over K.

A synopsis of Cartier theory. The main theorem of Cartier theory says that there is an equivalence between the category of commutative smooth formal groups over R and the category of left modules over a non-commutative ring $\mathrm{Cart}_p(R)$ satisfying certain conditions. See 4.27 for a precise statement.

The Cartier ring $\mathrm{Cart}_p(R)$ plays a crucial role. This is a topological ring which contains elements V, F and $\{\langle a \rangle \mid a \in R\}$. These elements form a set of topological generators, in the sense that every element of $\mathrm{Cart}_p(R)$ has a unique expression as a convergent sum in the following form

$$\sum_{m,n \geq 0} V^m \langle a_{mn} \rangle F^n \,,$$

with $a_{mn} \in R$ for all $m, n \geq 0$; moreover for each $m \in \mathbb{N}$, there exists a constant $C_m > 0$ such that $a_{mn} = 0$ for all $n \geq C_m$. Every convergent sum as above is an element of $\mathrm{Cart}_p(R)$. These topological generators satisfy the following commutation relations:

- $F \langle a \rangle = \langle a^p \rangle F$ for all $a \in R$;
- $\langle a \rangle V = V \langle a^p \rangle$ for all $a \in R$;
- $\langle a \rangle \langle b \rangle = \langle ab \rangle$ for all $a, b \in R$;
- $FV = p$;
- $V^m \langle a \rangle F^m V^n \langle b \rangle F^n = p^r V^{m+n-r} \langle a^{p^{n-r}} b^{p^{m-r}} \rangle F^{m+n-r}$ for all $a, b \in R$ and all $m, n \in \mathbb{N}$, where $r = \min\{m, n\}$.

Moreover, the ring of p-adic Witt vectors $W_p(R)$ is embedded in $\mathrm{Cart}_p(R)$ by the formula

$$W_p(R) \ni \underline{c} = (c_0, c_1, c_2, \ldots) \longmapsto \sum_{n \geq 0} V^n \langle c_n \rangle F^n \in \mathrm{Cart}_p(R) \,.$$

The topology of $\mathrm{Cart}_p(R)$ is given by the decreasing filtration

$$\mathrm{Fil}^n \left(\mathrm{Cart}_p(R) \right) := V^n \cdot \mathrm{Cart}_p(R) \,,$$

making $\mathrm{Cart}_p(R)$ a complete and separated topological ring. Under the equivalence of categories mentioned above, a left $\mathrm{Cart}_p(R)$ module corresponds to a finite dimensional smooth commutative formal group G over R if and only if

- $V : M \to M$ is injective,
- $M \xrightarrow{\sim} \varprojlim_n M/V^n M$, and
- M/VM is a projective R-module of finite type.

If so, then $\mathrm{Lie}(G/R) \cong M/VM$, and M is a finitely generated $\mathrm{Cart}_p(R)$-module. See 4.18 for the definition of $\mathrm{Cart}_p(R)$, 4.19 for the commutation relations in $\mathrm{Cart}_p(R)$, and 4.23 for some other properties of R.

References for Cartier theory. We highly recommend [**93**], where the approach in §2 of [**73**] is fully developed. Other references for Cartier theory are [**44**] and [**36**].

Remarks on Dieudonné theories.

(1) As already mentioned, the effect of a Dieudonné theory for p-divisible groups (and/or formal groups) is to translate questions for p-divisible groups (and/or formal groups) into questions in linear algebra for modules over suitable rings. A survey of Dieudonné theories can be found in [**6**]. The book [**24**] is a good introduction to the classical contravariant Dieudonné theory over a perfect field $K \supset \mathbb{F}_p$.

(2) The covariant Dieudonné theory described in this section is the dual version of the classical contravariant theory. For a p-divisible group X over a perfect field $K \supset \mathbb{F}_p$, the covariant Dieudonné module $\mathbb{D}(X)$ described in Theorem 4.33 is functorially isomorphic to $\mathbb{D}_{\mathrm{classical}}(X^t)$, the classical contravariant Dieudonné module of the Serre dual X^t of X as defined in [**48**] and [**24**].

(3) The Cartier theory is a Dieudonné theory for commutative formal groups. As explained in 10.9, a p-divisible group X over an Artinian local ring R with residue characteristic p whose maximal étale quotient is trivial can be recovered from the formal completion $X^\wedge$ of X. Such p-divisible groups are called p-*divisible formal groups*. Given a p-divisible formal group X over an Artinian local ring R with residue characteristic p, the formal completion $X^\wedge$ is a smooth commutative formal group over R, and the Cartier theory provides us with a module V-flat V-reduced left $\mathrm{Cart}_p(R)$-module $M_p(X^\wedge)$.

(4) The Cartier module attached to a p-divisible formal group X over a perfect field $K \supset \mathbb{F}_p$ is canonically isomorphic to the Dieudonné module $\mathbb{D}(X)$; see Theorem 4.33 (2). See also 4.34 for the relation with the Dieudonné crystal attached to X.

(5) Let $(R, \mathfrak{m})$ be a complete Noetherian local ring with residue characteristic p. Suppose that X is a p-divisible group over R such that $X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R/\mathfrak{m})$ is a p-divisible formal group. Let $X^\wedge$ be the formal completion of X, defined as the scheme-theoretic inductive limit of the finite flat group schemes $X[p^n] \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R/\mathfrak{m}^i)$ over $\mathrm{Spec}(R/m^i)$ as m and i go to ∞. Then $X^\wedge$ is a commutative smooth formal group over R, whose closed fiber is a p-divisible formal group. Conversely, suppose that X' is a commutative smooth formal group over R whose closed fiber X_0 is the formal completion of a p-divisible formal group X_0 over the residue field $R/\mathfrak{m}$. Then for each $i > 0$, the formal group $X' \times_{\mathrm{Spec}R} \mathrm{Spec}(R/\mathfrak{m}^i)$ is the formal completion of a p-divisible formal group $X_i \to \mathrm{Spec}(R/\mathfrak{m}^i)$, uniquely determined up to unique isomorphism. The projective limit of the p-divisible groups $X_i \to \mathrm{Spec}(R/\mathfrak{m}^i)$ "is" a p-divisible group X over R whose closed fiber is the p-divisible formal group X_0 over $R/\mathfrak{m}$; see 10.21 and 10.9. Notice that the fibers of $X \to \mathrm{Spec}(R/pR)$) may not be p-divisible formal groups; the universal p-divisible group over the equi-characteristic deformation space of a supersingular elliptic curve provides an example.

The upshot of the previous paragraph is that we can apply the Cartier theory to construct and study deformation of p-divisible formal groups. Suppose that R is a complete Noetherian local ring whose residue field $R/\mathfrak{m}$ has characteristic p. In order to produce a deformation over R of a p-divisible formal group X_0 over $R/\mathfrak{m}$, it suffices to "write down" a V-flat V-reduced left $\mathrm{Cart}_p(R)$-module M such that the tensor product $\mathrm{Cart}_p(R/\mathfrak{m}) \otimes_{\mathrm{Cart}_p(R)} M$ is isomorphic to the Cartier module

$M_p(X_0)$ attached to X_0. This way of explicitly constructing deformations over rings such as $K[[x_1, \ldots, x_N]]$ and $W(K)[[x_1, \ldots, x_N]]$ whose analog in deformation theory for general algebraic varieties is often intractable, becomes manageable. This method is essential for Sections 5, 7, 8.

We strongly advise readers with no prior experience with Cartier theory to accept the synopsis above as a "big black box" and use the materials in 4.1–4.27 as a dictionary only when necessary. Instead, we suggest such readers start with 4.28–4.52, get familiar with the ring $\mathrm{Cart}_p(K)$ in the case when $R = K$, a perfect field of characteristic p, play with some examples of finitely generated modules over $\mathrm{Cart}_p(K)$ in conjunction with the theory of covariant Dieudonné modules over perfect fields in characteristic p and do some of the exercises. See the Lemma/Exercise after Def. 4.28 for a concrete definition of the Cartier ring $\mathrm{Cart}_p(K)$ as the V-adic completion of the Dieudonné ring R_K.

Cartier theory

Definition 4.1. Let R be a commutative ring with 1.

(1) Let Nilp_R be the category of all nilpotent R-algebras, consisting of all commutative R-algebras N without unit such that $N^n = (0)$ for some positive integer n.

(2) A *commutative smooth formal group* over R is a covariant functor $G : \mathrm{Nilp}_R \to \mathrm{Ab}$ from Nilp_R to the category of all abelian groups such that the following properties are satisfied:
   - G commutes with finite inverse limits;
   - G is formally smooth, i.e., every surjection $N_1 \to N_2$ in Nilp_R induces a surjection $G(N_1) \to G(N_2)$;
   - G commutes with arbitrary direct limits.

(3) The *Lie algebra* of a commutative smooth formal group G is defined to be $G(N_0)$, where N_0 is the object in Nilp_R whose underlying R-module is R, and $N_0^2 = (0)$.

Remark. Let G be a commutative smooth formal group over R, then G extends uniquely to a functor $G^\sim$ on the category $\mathrm{ProNilp}_R$ of all filtered projective system of nilpotent R-algebras which commutes with filtered projective limits. This functor $G^\sim$ is often denoted G by abuse of notation.

Example. Let A be a commutative smooth group scheme of finite presentation over R. For every nilpotent R-algebra N, denote by $R \oplus N$ the commutative R-algebra with multiplication given by

$$(u_1, n_1) \cdot (u_2, n_2) = (u_1 u_2, u_1 n_2 + u_2 n_1 + n_1 n_2) \qquad \forall u_1, u_2 \in R \ \ \forall n_1, n_2 \in N \,.$$

The functor which sends an object N in Nilp_R to the abelian group

$$\mathrm{Ker}\,(A(R \oplus N) \to A(R))$$

is a commutative smooth formal group over R, denoted by $A^\wedge$. Note that the functor $A^\wedge$ commutes with arbitrary inductive limits because A does.

Here are two special cases: we have

$$\mathbb{G}_a^\wedge(N) = N \qquad \text{and} \qquad \mathbb{G}_m^\wedge(N) = 1 + N \subset (R \oplus N)^\times$$

for all $N \in \mathrm{Ob}(\mathrm{Nilp}_R)$.

Definition 4.2. We define a *restricted version* of the smooth formal group attached to the universal Witt vector group over R, denoted by Λ_R, or Λ when the base ring R is understood.

$$\Lambda_R(N) = 1 + t\, R[t] \otimes_R N \subset ((R \oplus N)[t])^\times \qquad \forall\, N \in \mathrm{Ob}(\mathrm{Nilp}_R)\,.$$

In other words, the elements of $\Lambda(N)$ consists of all polynomials of the form $1 + u_1 t + u_2 t^2 + \cdots + u_r t^r$ for some $r \geq 0$, where $u_i \in N$ for $i = 1, \ldots, r$. The group law of $\Lambda(N)$ comes from multiplication in the polynomial ring $(R \oplus N)[t]$ in one variable t.

Remarks.

(i) The formal group Λ plays the role of a free generator in the category of (smooth) formal groups; see Theorem 4.4.

(ii) When we want to emphasize that the polynomial $1 + \sum_{i \geq 1} u_i t^i$ is regarded as an element of $\Lambda(N)$, we denote it by $\lambda(1 + \sum_{i \geq 1} u_i t^i)$.

(iii) Note that the functor $N \mapsto 1 + N\, t\, R[[t]] \subset (R \oplus N)[[t]]^\times$ is not a commutative smooth formal group because it does not commute with arbitrary direct limits.

Exercise 4.3. Let $R[[X]]^+ = X\, R[[X]]$ be the set of all formal power series over R with constant term 0; it is an object in $\mathrm{ProNilp}_R$. Show that $\Lambda(R[[X]]^+)$ equals

$$\left\{ \prod_{m,n \geq 1} (1 - a_{mn}\, X^m\, t^n) \;\middle|\; a_{m,n} \in R,\ \forall\, m\, \exists\, C_m > 0 \text{ s.t. } a_{mn} = 0\ \forall\, n \geq C_m \right\}.$$

Theorem 4.4. $\boxed{\text{BB}}$ *Let $H : \mathrm{Nilp}_R \to \mathrm{Ab}$ be a commutative smooth formal group over R. Let $\Lambda = \Lambda_R$ be the functor defined in 4.2. Then the map*

$$Y_H : \mathrm{Hom}(\Lambda_R, H) \to H(R[[X]]^+)$$

which sends each homomorphism $\alpha : \Lambda \to H$ of group-valued functors to the element

$$\alpha_{R[[X]]^+}(1 - Xt) \in H(R[[X]]^+)$$

is a bijection.

Remark. The formal group Λ is in some sense a free generator of the additive category of commutative smooth formal groups, a phenomenon reflected in Theorem 4.4.

Definition 4.5. (i) Define $\mathrm{Cart}(R)$ to be $(\mathrm{End}(\Lambda_R))^{\mathrm{op}}$, the opposite ring of the endomorphism ring of the smooth formal group Λ_R. According to Theorem 4.4, for every commutative smooth formal group $H : \mathrm{Nilp}_R \to \mathrm{Ab}$, the abelian group $H(R[[X]]^+) = \mathrm{Hom}(\Lambda_R, H)$ is a *left* module over $\mathrm{Cart}(R)$.

(ii) We define some special elements of the Cartier ring $\mathrm{Cart}(R)$, naturally identified with $\Lambda(R[[X]])$ via the bijection $Y = Y_\Lambda : \mathrm{End}(\Lambda) \xrightarrow{\sim} \Lambda(R[[X]]^+)$ in Theorem 4.4.

- $V_n := Y^{-1}(1 - X^n t)\,, n \geq 1,$
- $F_n := Y^{-1}(1 - X\, t^n)\,, n \geq 1,$
- $[c] := Y^{-1}(1 - c\, X\, t)\,, c \in R.$

Corollary. For every commutative ring with 1 we have

$$\mathrm{Cart}(R) = \left\{ \sum_{m,n \geq 1} V_m\,[c_{mn}]\,F_n \;\middle|\; c_{mn} \in R,\; \forall\, m\, \exists\, C_m > 0 \text{ s.t. } c_{mn} = 0 \;\forall\, n \geq C_m \right\}.$$

Proposition 4.6. $\boxed{\text{BB}}$ *The following identities hold in* $\mathrm{Cart}(R)$.

    (1) $V_1 = F_1 = 1$, $F_n\,V_n = n$.
    (2) $[a]\,[b] = [ab]$ *for all* $a, b \in R$
    (3) $[c]\,V_n = V_n\,[c^n]$, $F_n\,[c] = [c^n]\,F_n$ *for all* $c \in R$, *all* $n \geq 1$.
    (4) $V_m\,V_n = V_n\,V_m = V_{mn}$, $F_m\,F_n = F_n\,F_m = F_{mn}$ *for all* $m, n \geq 1$.
    (5) $F_n\,V_m = V_m\,F_n$ *if* $(m, n) = 1$.
    (6) $(V_n[a]F_n) \cdot (V_m[b]F_m) = r\,V_{\frac{mn}{r}}\left[a^{\frac{m}{r}} b^{\frac{n}{r}}\right] F_{\frac{mn}{r}}$, $r = (m, n)$, *for all* $a, b \in R$,
       $m, n \geq 1$.

Definition 4.7. The ring $\mathrm{Cart}(R)$ has a natural filtration $\mathrm{Fil}^\bullet\mathrm{Cart}(R)$ by right ideals, where $\mathrm{Fil}^j\mathrm{Cart}(R)$ is defined by

$$\left\{ \sum_{m \geq j} \sum_{n \geq 1} V_m[a_{mn}]F_n \;\middle|\; a_{mn} \in R,\; \forall\, m \geq j,\; \exists\, C_m > 0 \text{ s.t. } a_{mn} = 0 \text{ if } n \geq C_m \right\}$$

for every integer $j \geq 1$. The Cartier ring $\mathrm{Cart}(R)$ is complete with respect to the topology given by the above filtration. Moreover each right ideal $\mathrm{Fil}^j\mathrm{Cart}(R)$ is open and closed in $\mathrm{Cart}(R)$.

Remark. The definition of the Cartier ring gives a functor

$$R \longmapsto \mathrm{Cart}(R)$$

from the category of commutative rings with 1 to the category of complete filtered rings with 1.

Definition 4.8. Let R be a commutative ring with 1.

    (1) A *V-reduced* left $\mathrm{Cart}(R)$-module is a left $\mathrm{Cart}(R)$-module M together with a separated decreasing filtration of M

$$M = \mathrm{Fil}^1 M \supset \mathrm{Fil}^2 M \supset \cdots \supset \mathrm{Fil}^n M \supset \mathrm{Fil}^{n+1} \supset \cdots$$

        such that each $\mathrm{Fil}^n M$ is an abelian subgroup of M and
      (i) $(M, \mathrm{Fil}^\bullet M)$ is complete with respect to the topology given by the filtration $\mathrm{Fil}^\bullet M$. In other words, the natural map

$$\mathrm{Fil}^n M \to \varprojlim_{m \geq n} (\mathrm{Fil}^n M / \mathrm{Fil}^m M)$$

        is a bijection for all $n \geq 1$.
      (ii) $V_m \cdot \mathrm{Fil}^n M \subset \mathrm{Fil}^{mn} M$ for all $m, n \geq 1$.
      (iii) The map V_n induces a bijection $V_n : M/\mathrm{Fil}^2 M \xrightarrow{\sim} \mathrm{Fil}^n M / \mathrm{Fil}^{n+1} M$ for every $n \geq 1$.
      (iv) $[c] \cdot \mathrm{Fil}^n M \subset \mathrm{Fil}^n M$ for all $c \in R$ and all $n \geq 1$.
      (v) For every $m, n \geq 1$, there exists an $r \geq 1$ such that $F_m \cdot \mathrm{Fil}^r M \subset \mathrm{Fil}^n M$.
    (2) A V-reduced left $\mathrm{Cart}(R)$-module $(M, \mathrm{Fil}^\bullet M)$ is *V-flat* if $M/\mathrm{Fil}^2 M$ is a flat R-module. The R-module $M/\mathrm{Fil}^2 M$ is called the *tangent space* of $(M, \mathrm{Fil}^\bullet M)$.

Definition 4.9. Let $H : \mathrm{Nilp}_R \to \mathrm{Ab}$ be a commutative smooth formal group over R. The abelian group $\mathrm{M}(H) := H(R[[X]]^+)$ has a natural structure as a left $\mathrm{Cart}(R)$-module according to Theorem 4.4 The $\mathrm{Cart}(R)$-module $\mathrm{M}(H)$ has a natural filtration, with

$$\mathrm{Fil}^n\mathrm{M}(H) := \mathrm{Ker}(H(R[[X]]^+) \to H(R[[X]]^+/X^n R[[X]])) \,.$$

We call the pair $(\mathrm{M}(H), \mathrm{Fil}^\bullet \mathrm{M}(H))$ the *Cartier module attached to* H.

Definition 4.10. Let M be a V-reduced left $\mathrm{Cart}(R)$-module and let Q be a right $\mathrm{Cart}(R)$-module.

(i) For every integer $m \geq 1$, let $Q_m := \mathrm{Ann}_Q(\mathrm{Fil}^m\mathrm{Cart}(R))$ be the subgroup of Q consisting of all elements $x \in Q$ such that $x \cdot \mathrm{Fil}^m\mathrm{Cart}(R) = (0)$. Clearly we have $Q_1 \subseteq Q_2 \subseteq Q_3 \subseteq \cdots$.

(ii) For each $m, r \geq 1$, define $Q_m \odot M^r$ to be the image of $Q_m \otimes \mathrm{Fil}^r M$ in $Q \otimes_{\mathrm{Cart}(R)} M$.

Notice that if $r \geq m$ and $s \geq m$, then $Q_m \odot M^r = Q_m \odot M^s$. Hence $Q_m \odot M^m \subseteq Q_n \odot M^n$ if $m \leq n$.

(iii) Define the *reduced tensor product* $Q\overline{\otimes}_{\mathrm{Cart}(R)}M$ by

$$Q\overline{\otimes}_{\mathrm{Cart}(R)}M = Q \otimes_{\mathrm{Cart}(R)} M \,\Big/\, \Big(\bigcup_m (Q_m \odot M^m)\Big) \,.$$

Remark. The reduced tensor product is used to construct the arrow in the "reverse direction" in the equivalence of category in 4.11 below.

Theorem 4.11. $\boxed{\mathrm{BB}}$ *Let R be a commutative ring with 1. There is a canonical equivalence of categories between the category of smooth commutative formal groups over R as defined in* 4.1 *and the category of V-flat V-reduced left $\mathrm{Cart}(R)$-modules, defined as follows.*

$$\{\text{smooth formal groups over } R\} \quad \xrightarrow{\ \sim\ } \quad \{V\text{-flat } V\text{-reduced left } \mathrm{Cart}(R)\text{-mod}\}$$

$$G \qquad\qquad\longmapsto\qquad\qquad \mathrm{M}(G) = \mathrm{Hom}(\Lambda, G)$$

$$\Lambda\overline{\otimes}_{\mathrm{Cart}(R)}M \qquad\qquad\longleftarrow\!\!\!| \qquad\qquad M$$

Recall that $\mathrm{M}(G) = \mathrm{Hom}(\Lambda, G)$ *is canonically isomorphic to* $G(X\,R[[X]])$, *the group of all formal curves in the smooth formal group G. The reduced tensor product* $\Lambda\overline{\otimes}_{\mathrm{Cart}(R)}M$ *is the functor whose value at any nilpotent R-algebra N is* $\Lambda(N)\overline{\otimes}_{\mathrm{Cart}(R)}M$.

The Cartier ring $\mathrm{Cart}(R)$ contains the ring of universal Witt vectors $W^\sim(R)$ as a subring which contains the unit element of $\mathrm{Cart}(R)$.

Definition 4.12.

(1) The *universal Witt vector group* $W^\sim$ is defined as the functor from the category of all commutative algebras with 1 to the category of abelian groups such that

$$W^\sim(R) = 1 + T\,R[[T]] \subset R[[T]]^\times$$

for every commutative ring R with 1.

When we regard a formal power series $1 + \sum_{m\geq 1} u_m\,T^m$ in $R[[T]]$ as an element of $W^\sim(R)$, we use the notation $\omega(1 + \sum_{m\geq 1} u_m\,T^m)$. It is

easy to see that every element of $W^\sim(R)$ has a unique expression as

$$\omega\left(\prod_{m\geq 1}(1 - a_m\,T^m)\right).$$

Hence $W^\sim$ is isomorphic to $\operatorname{Spec}\mathbb{Z}[x_1, x_2, x_3, \ldots]$ as a scheme; the R-valued point such that $x_i \mapsto a_i$ is denoted by $\omega(\underline{a})$, where $\underline{a}$ is short for $(a_1, a_2, a_3, \ldots)$, and $\omega(\underline{a}) = \omega(\prod_{m\geq 1}(1 - a_m\,T^m))$.

(2) The group scheme $W^\sim$ has a natural structure as a ring scheme, such that multiplication on $W^\sim$ is determined by the formula

$$\omega(1 - a\,T^m)\cdot\omega(1 - b\,T^n) = \omega\left(\left(1 - a^{\frac{n}{r}}\,b^{\frac{m}{r}}\,T^{\frac{mn}{r}}\right)^r\right), \quad \text{where } r = \gcd(m, n)\,.$$

(3) There are two families of endomorphisms of the group scheme $W^\sim$: V_n and F_n, $n \in \mathbb{N}_{\geq 1}$. Also, for each commutative ring R with 1 and each element $c \in R$ we have an endomorphism $[c]$ of $W^\sim \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec} R$. These operators make $W^\sim(R)$ a left $\operatorname{Cart}(R)$-module; they are defined as follows

$$V_n \;:\; \omega(f(T)) \;\mapsto\; \omega(f(T^n)),$$

$$F_n \;:\; \omega(f(T)) \;\mapsto\; \sum_{\zeta\in\mu_n}\omega(f(\zeta\,T^{\frac{1}{n}})), \qquad (\,\text{formally}\,)$$

$$[c] \;:\; \omega(f(T)) \;\mapsto\; \omega(f(cT)).$$

The formula for $F_n(\omega(f(T)))$ means that $F_n(\omega(f(T)))$ is defined as the unique element such that $V_n(F_n(\omega(f(T)))) = \sum_{\zeta\in\mu_n}\omega(f(\zeta\,T))$.

Exercise 4.13. Show that the Cartier module of $\mathbb{G}_m^\wedge$ over R is naturally isomorphic to $W^\sim(R)$ as a module over $\operatorname{Cart}(R)$.

Proposition 4.14. $\boxed{\text{BB}}$ *Let R be a commutative ring with 1.*

(i) *The subset S of $\operatorname{Cart}(R)$ consisting of all elements of the form*

$$\sum_{n\geq 1} V_n[a_n]F_n\,, \quad a_n \in R \;\forall\, n \geq 1$$

forms a subring of $\operatorname{Cart}(R)$.

(ii) *The injective map*

$$W^\sim(R) \hookrightarrow \operatorname{Cart}(R), \qquad \omega(\underline{a}) \mapsto \sum_{n\geq 1} V_n\,[a_n]\,F_n$$

is an injective homomorphism of rings which sends 1 to 1; its image is the subring S defined in (i).

Definition 4.15. It is a fact that every prime number $\ell \neq p$ is invertible in $\operatorname{Cart}(\mathbb{Z}_{(p)})$. Define elements ϵ_p and $\epsilon_{p,n}$ of the Cartier ring $\operatorname{Cart}(\mathbb{Z}_{(p)})$ for $n \in \mathbb{N}$, $(n, p) = 1$ by

$$\epsilon_p = \epsilon_{p,1} \;=\; \sum_{\substack{(n,p)=1\\ n\geq 1}} \frac{\mu(n)}{n} V_n F_n \;=\; \prod_{\substack{\ell\neq p\\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell} V_\ell F_\ell\right)$$

$$\epsilon_{p,n} \;=\; \frac{1}{n} V_n \epsilon_p F_n$$

where μ is the Möbius function on $\mathbb{N}_{\geq 1}$, characterized by the following properties: $\mu(mn) = \mu(m)\,\mu(n)$ if $(m, n) = 1$, and for every prime number ℓ we have $\mu(\ell) = -1$,

$\mu(\ell^i) = 0$ if $i \geq 2$. For every commutative with 1 over $\mathbb{Z}_{(p)}$, the image of ϵ_p in $\mathrm{Cart}(R)$ under the canonical ring homomorphism $\mathrm{Cart}(\mathbb{Z}_{(p)}) \to \mathrm{Cart}(R)$ is also denoted by ϵ_p.

Exercise 4.16. Let R be a $\mathbb{Z}_{(p)}$-algebra, and let $(a_m)_{m \geq 0}$ be a sequence in R. Prove the equality

$$\epsilon_p \left(\omega \left(\prod_{m \geq 1} (1 - a_m\, T^m) \right) \right) = \epsilon_p \left(\omega \left(\prod_{n \geq 0} (1 - a_{p^n}\, T^{p^n}) \right) \right)$$

$$= \omega \left(\prod_{n \geq 0} E(a_{p^n}\, T^{p^n}) \right),$$

in $W^{\sim}(R)$, where

$$E(X) = \prod_{(n,p)=1} (1 - X^n)^{\frac{\mu(n)}{n}} = \exp\left(-\sum_{n \geq 0} \frac{X^{p^n}}{p^n} \right) \in 1 + X\mathbb{Z}_{(p)}[[X]]$$

is the inverse of the classical Artin-Hasse exponential.

Proposition 4.17. $\boxed{\textbf{BB}}$ *Let R be a commutative $\mathbb{Z}_{(p)}$-algebra with 1. The following equalities hold in $\mathrm{Cart}(R)$.*

    (i) $\epsilon_p{}^2 = \epsilon_p$.

    (ii) $\displaystyle\sum_{p \nmid n,\, n \geq 1} \epsilon_{p,n} = 1$.

    (iii) $\epsilon_p V_n = 0$, $F_n \epsilon_p = 0$ *for all n with $p \nmid n$.*

    (iv) $\epsilon_{p,n}{}^2 = \epsilon_{p,n}$ *for all $n \geq 1$ with $p \nmid n$.*

    (v) $\epsilon_{p,n}\, \epsilon_{p,m} = 0$ *for all $m \neq n$ with $p \nmid mn$.*

    (vi) $[c]\, \epsilon_p = \epsilon_p\, [c]$ *and* $[c]\, \epsilon_{p,n} = \epsilon_{p,n}\, [c]$ *for all $c \in R$ and all n with $p \nmid n$.*

    (vii) $F_p \epsilon_{p,n} = \epsilon_{p,n} F_p$, $V_p \epsilon_{p,n} = \epsilon_{p,n} V_p$ *for all n with $p \nmid n$.*

Definition 4.18. Let R be a commutative ring with 1 over $\mathbb{Z}_{(p)}$.

    (i) Denote by $\mathrm{Cart}_p(R)$ the subring $\epsilon_p \mathrm{Cart}(R)\epsilon_p$ of $\mathrm{Cart}(R)$. Note that ϵ_p is the unit element of $\mathrm{Cart}_p(R)$.

    (ii) Define elements $F, V \in \mathrm{Cart}_p(R)$ by

$$F = \epsilon_p F_p = F_p \epsilon_p = \epsilon_p F_p \epsilon_p, \quad V = \epsilon_p V_p = V_p \epsilon_p = \epsilon_p V_p \epsilon_p.$$

    (iii) For every element $c \in R$, denote by $\langle c \rangle$ the element

$$\epsilon_p[c]\epsilon_p = \epsilon_p[c] = [c]\epsilon_p \in \mathrm{Cart}_p(R).$$

Exercise 4.19. Prove the following identities in $\mathrm{Cart}_p(R)$.

    (1) $F \langle a \rangle = \langle a^p \rangle F$ for all $a \in R$.

    (2) $\langle a \rangle V = V \langle a^p \rangle$ for all $a \in R$.

    (3) $\langle a \rangle \langle b \rangle = \langle ab \rangle$ for all $a, b \in R$.

    (4) $FV = p$.

    (5) $VF = p$ if and only if $p = 0$ in R.

    (6) Every prime number $\ell \neq p$ is invertible in $\mathrm{Cart}_p(R)$. The prime number p is invertible in $\mathrm{Cart}_p(R)$ if and only if p is invertible in R.

    (7) $V^m \langle a \rangle F^m\, V^n \langle b \rangle F^n = p^r\, V^{m+n-r} \langle a^{p^{n-r}} b^{p^{m-r}} \rangle F^{m+n-r}$ for all $a, b \in R$ and all $m, n \in \mathbb{N}$, where $r = \min\{m, n\}$.

Definition 4.20. Let R be a commutative $\mathbb{Z}_{(p)}$-algebra with 1. Denote by Λ_p the image of ϵ_p in Λ. In other words, Λ_p is the functor from the category Nilp_R of nilpotent commutative R-algebras to the category Ab of abelian groups such that

$$\Lambda_p(N) = \Lambda(N) \cdot \epsilon_p$$

for any nilpotent R-algebra N.

Definition 4.21.

(1) Denote by W_p the image of ϵ_p, i.e., $W_p(R) := \epsilon_p(W^\sim(R))$ for every $\mathbb{Z}_{(p)}$-algebra R. Equivalently, $W_p(R)$ is the intersection of the kernels $\mathrm{Ker}(F_\ell)$ of the operators F_ℓ on $W^\sim(R)$, where ℓ runs through all prime numbers different from p.

(2) Denote the element

$$\omega(\prod_{n=0}^{\infty} E(c_n\, T^{p^n})) \in W_p(R)$$

by $\omega_p(\underline{c})$.

(3) The endomorphism V_p, F_p of the group scheme $W^\sim$ induces endomorphisms of the group scheme W_p, denoted by V and F respectively.

Remark. The functor W_p has a natural structure as a ring-valued functor induced from that of $W^\sim$; it is represented by the scheme $\mathrm{Spec}\,\mathbb{Z}_{(p)}[y_0, y_1, y_2, \ldots, y_n, \ldots]$ such that the element $\omega_p(\underline{c})$ has coordinates $\underline{c} = (c_0, c_1, c_2, \ldots)$.

Exercise 4.22. Let R be a commutative $\mathbb{Z}_{(p)}$-algebra with 1. Let $E(T) \in \mathbb{Z}_{(p)}[[T]]$ be the inverse of the Artin-Hasse exponential as in Exer. 4.16.

(i) Prove that for any nilpotent R-algebra N, every element of $\Lambda_p(N)$ has a unique expression as a finite product

$$\prod_{i=0}^{m} E(u_i\, t^{p^i})$$

for some $m \in \mathbb{N}$, and $u_i \in N$ for $i = 0, 1, \ldots, m$.

(ii) Prove that Λ_p is a smooth commutative formal group over R.

(iii) Prove that every element of $W_p(R)$ can be uniquely expressed as an infinite product

$$\omega(\prod_{n=0}^{\infty} E(c_n\, T^{p^n})) \in W_p(R) =: \omega_p(\underline{c})\,.$$

(iv) Show that the map from $W_p(R)$ to the product ring $\prod_0^{\infty} R$ defined by

$$\omega_p(\underline{c}) \;\longmapsto\; \big(w_n(\underline{c})\big)_{n \geq 0} \qquad \text{where} \quad w_n(\underline{c}) := \sum_{i=0}^{n} p^{n-i}\, c_{n-i}^{p^i}\,,$$

is a ring homomorphism.

Proposition 4.23.

(i) *The local Cartier ring* $\mathrm{Cart}_p(R)$ *is complete with respect to the decreasing sequence of right ideals* $V^i\mathrm{Cart}_p(R)$.

(ii) *Every element of* $\mathrm{Cart}_p(R)$ *can be expressed in a unique way as a convergent sum in the form*

$$\sum_{m,n\geq 0} V^m \langle a_{mn} \rangle F^n$$

with all $a_{mn} \in R$, *and for each* m *there exists a constant* C_m *such that* $a_{mn} = 0$ *for all* $n \geq C_m$.

(iii) *The set of all elements of* $\mathrm{Cart}_p(R)$ *which can be represented as a convergent sum of the form*

$$\sum_{m\geq 0} V^m \langle a_m \rangle F^m\,, \quad a_m \in R$$

is a subring of $\mathrm{Cart}_p(R)$. *The map*

$$w_p(\underline{a}) \;\mapsto\; \sum_{m\geq 0} V^m \langle a_m \rangle F^m \quad \underline{a} = (a_0, a_1, a_2, \ldots),\ a_i \in R\ \forall\, i \geq 0$$

establishes an isomorphism from the ring of p-*adic Witt vectors* $W_p(R)$ *to the above subring of* $\mathrm{Cart}_p(R)$.

Exercise 4.24. Prove that $\mathrm{Cart}_p(R)$ is naturally isomorphic to $\mathrm{End}(\Lambda_p)^{\mathrm{op}}$, the opposite ring of the endomorphism ring of $\mathrm{End}(\Lambda_p)$.

Definition 4.25. Let R be a commutative $\mathbb{Z}_{(p)}$-algebra.

(i) A *V-reduced* left $\mathrm{Cart}_p(R)$-module M is a left $\mathrm{Cart}_p(R)$-module such that the map $V : M \to M$ is injective and the canonical map $M \to \varprojlim_n (M/V^n M)$ is an isomorphism.

(ii) A *V*-reduced left $\mathrm{Cart}_p(R)$-module M is *V-flat* if M/VM is a flat R-module.

Theorem 4.26. *Let* R *be a commutative* $\mathbb{Z}_{(p)}$-*algebra with* 1.

(i) *There is an equivalence of categories between the category of V-reduced left* $\mathrm{Cart}(R)$-*modules and the category of V-reduced left* $\mathrm{Cart}_p(R)$-*modules, defined as follows.*

$$\{\ V\text{-reduced left } \mathrm{Cart}(R)\text{-mod}\ \} \;\xrightarrow{\ \sim\ }\; \{\ V\text{-reduced left } \mathrm{Cart}_p(R)\text{-mod}\ \}$$

$$M \longmapsto \epsilon_p M$$

$$\mathrm{Cart}(R)\epsilon_p \widehat{\otimes}_{\mathrm{Cart}_p(R)} M_p \longleftarrow\!\shortmid\ M_p$$

(ii) *Let* M *be a V-reduced left* $\mathrm{Cart}(R)$-*module* M, *and let* M_p *be the V-reduced let* $\mathrm{Cart}_p(R)$-*module* M_p *attached to* M *as in* (i) *above. There is a canonical isomorphism* $M/\mathrm{Fil}^2 M \cong M_p/VM_p$. *In particular* M *is V-flat if and only if* M_p *is V-flat. Similarly* M *is a finitely generated* $\mathrm{Cart}(R)$-*module if and only if* M_p *is a finitely generated* $\mathrm{Cart}_p(R)$-*module.*

Theorem 4.27. *Let* R *be a commutative* $\mathbb{Z}_{(p)}$-*algebra with* 1. *There is a canonical equivalence of categories between the category of smooth commutative formal groups over* R *as defined in* 4.1 *and the category of V-flat V-reduced left* $\mathrm{Cart}_p(R)$-*modules,*

defined as follows.

$$\{\text{smooth formal groups over } R\} \quad \xrightarrow{\;\sim\;} \quad \{V\text{-flat } V\text{-reduced left } \mathrm{Cart}_p(R)\text{-mod}\}$$

$$G \quad\longmapsto\quad \mathrm{M}_p(G) = \epsilon_p \mathrm{Hom}(\Lambda, G)$$

$$\Lambda_p \otimes_{\mathrm{Cart}_p(R)} M \quad\longleftarrow\!\shortmid\quad M$$

Dieudonné modules.

In the rest of this section, K stands for a perfect field of characteristic $p > 0$. We have $FV = VF = p$ in $\mathrm{Cart}_p(K)$. It is well known that the ring of p-adic Witt vectors $W(K)$ is a complete discrete valuation ring with residue field K, whose maximal ideal is generated by p. Denote by $\sigma : W(K) \to W(K)$ the Teichmüller lift of the automorphism $x \mapsto x^p$ of K. With the Witt coordinates we have $\sigma : (c_0, c_1, c_2, \ldots) \mapsto (c_0^p, c_1^p, c_2^p, \ldots)$. Denote by $L = B(K)$ the field of fractions of $W(K)$.

Definition 4.28. Denote by R_K the (non-commutative) ring generated by $W(K)$, F and V, subject to the following relations

$$F \cdot V = V \cdot F = p, \quad F \cdot x = {}^{\sigma}x \cdot F, \quad x \cdot V = V \cdot {}^{\sigma}x \qquad \forall x \in W(K)\,.$$

Remark. There is a natural embedding $R_K \hookrightarrow \mathrm{Cart}_p(K)$; we use it to identify R_K as a dense subring of the Cartier ring $\mathrm{Cart}_p(K)$. For every continuous left $\mathrm{Cart}_p(K)$-module M, the $\mathrm{Cart}_p(K)$-module structure on M is determined by the induced left R_K-module structure on M.

Lemma/Exercise.

(i) The ring R_K is naturally identified with the ring

$$W(K)[V, F] := \left(\bigoplus_{i<0} p^{-i} V^i W(K) \right) \bigoplus \left(\bigoplus_{i \geq 0} V^i W(K) \right),$$

i.e., elements of $W(K)[V, F]$ are sums of the form $\sum_{i \in \mathbb{Z}} a_i V^i$, where $a_i \in L$ for all $i \in \mathbb{Z}$, $\mathrm{ord}_p(a_i) \geq \max(0, -i)$ $\forall i \in \mathbb{Z}$, and $a_i = 0$ for all but finitely many i's. The commutation relation between $W(K)$ and V^i is

$$x \cdot V^i = V^i \cdot {}^{\sigma^i}x \quad \text{for all } x \in W(K) \text{ and all } i \in \mathbb{Z}\,.$$

(ii) The ring $\mathrm{Cart}_p(K)$ is naturally identified with the set $W(K)[[V, F\rangle\rangle$, consisting of all non-commutative formal power series of the form $\sum_{i \in \mathbb{Z}} a_i V^i$ such that $a_i \in L$ $\forall i \in \mathbb{Z}$, $\mathrm{ord}_p(a_i) \geq \max(0, -i)$ $\forall i \in \mathbb{Z}$, and $\mathrm{ord}_p(a_i) + i \to \infty$ as $|i| \to \infty$.

(iii) Check that the ring structure on $W(K)[V, F]$ extends to $W(K)[[V, F\rangle\rangle$ by continuity. In other words, the inclusion $W(K)[V, F] \hookrightarrow W(K)[[V, F\rangle\rangle$ is a ring homomorphism, and $W(K)[V, F]$ is dense in $W(K)[[V, F\rangle\rangle$ with respect to the V-adic topology on $W(K)[[V, F\rangle\rangle \cong \mathrm{Cart}_p(K)$. The latter topology on $W(K)[[V, F\rangle\rangle$ is equivalent to the topology given by the discrete valuation v on $W(K)[[V, F\rangle\rangle$ defined by

$$v \left(\sum_{i \in \mathbb{Z}} a_i V^i \right) = \mathrm{Min} \left\{ \mathrm{ord}_p(a_i) + i \,|\, i \in \mathbb{Z} \right\}\,.$$

Definition 4.29.

(1) A *Dieudonné module* is a left R_K-module M such that M is a free $W(K)$-module of finite rank.

(2) Let M be a Dieudonné module over K. Define the α-rank of M to be the natural number $a(M) = \dim_K(M/(VM + FM))$.

Compare with $a(G)$ as defined in 5.4.

Definition 4.30.

(i) For any natural number $n \geq 1$ and any scheme S, denote by $\underline{(\mathbb{Z}/n\mathbb{Z})}_S$ the constant group scheme over S attached to the finite group $\mathbb{Z}/n\mathbb{Z}$. The scheme underlying $\underline{(\mathbb{Z}/n\mathbb{Z})}_S$ is the disjoint union of n copies of S, indexed by the finite group $\mathbb{Z}/n\mathbb{Z}$, see 10.22.

(ii) For any natural number $n \geq 1$ and any scheme S, denote by $\mu_{n,S}$ the kernel of $[n] : \mathbb{G}_{m/S} \to \mathbb{G}_{m/S}$. The group scheme $\mu_{n,S}$ is finite and locally free over S of rank n; it is the Cartier dual of $\underline{(\mathbb{Z}/n\mathbb{Z})}_S$.

(iii) For any field $K \supset \mathbb{F}_p$, define a finite group scheme α_p over K to be the kernel of the endomorphism

$$\mathrm{Fr}_p : \mathbb{G}_{a/K} = \mathrm{Spec}(K[X]) \to \mathbb{G}_{a/K} = \mathrm{Spec}(K[X])$$

of $\mathbb{G}_a$ over K defined by the K-homomorphism from the K-algebra $K[X]$ to itself which sends X to X^p. We have $\alpha_p = \mathrm{Spec}(K[X]/(X^p))$ as a scheme. The comultiplication on the coordinate ring of α_p is induced by $X \mapsto X \otimes X$.

Proposition 4.31. $\boxed{\text{BB}}$ *Let X be a p-divisible group over a perfect field $K \supset \mathbb{F}_p$. Then there exists a canonical splitting*

$$X \cong X_{\mathrm{tor}} \times_{\mathrm{Spec}(K)} X_{\ell\ell} \times_{\mathrm{Spec}(K)} X_{\mathrm{ét}}$$

where $X_{\mathrm{ét}}$ is the maximal étale quotient of X, X_{mult} is the maximal toric p-divisible subgroup of X, and $X_{\ell\ell}$ is a p-divisible group with no non-trivial étale quotient nor non-trivial multiplicative p-divisible subgroup.

Remark.

(i) The analogous statement for finite group schemes over K can be found in [**48**, Chapter 1], from which 4.31 follows. See also [**24**], [**25**].

(ii) See 10.9 for a similar statement for p-divisible groups over an Artinian local ring.

Definition 4.32. Let m, n be non-negative integers such that $\gcd(m, n) = 1$. Let $k \supset \mathbb{F}_p$ be an algebraically closed field. Let $G_{m,n}$ be the p-divisible group whose Dieudonné module is

$$\mathbb{D}(G_{m,n}) = R_K/R_K \cdot (V^n - F^m).$$

Theorem 4.33. $\boxed{\text{BB}}$

(1) *There is an equivalence of categories between the category of p-divisible groups over K and the category of Dieudonné modules over R_K. Denote by $\mathbb{D}(X)$ the covariant Dieudonné module attached to a p-divisible group over K. This equivalence is compatible with direct product and exactness, i.e., short exact sequences correspond under the above equivalence of categories.*

(2) *Let X be a p-divisible group over K such that X is a p-divisible formal group in the sense that the maximal étale quotient of X is trivial. Denote by $X^\wedge$ the formal group attached to X, i.e., $X^\wedge$ is the formal completion of X along the zero section of X. Then there is a canonical isomorphism*

$\mathbb{D}(X) \xrightarrow{\sim} \mathrm{M}_p(X^\wedge)$ *between the Dieudonné module of X and the Cartier module of $X^\wedge$ which is compatible with the actions by F, V and elements of $W(K)$.*

(3) *Let X be a p-divisible group over K and $\mathbb{D}(X)$ the covariant Dieudonné module of X. Then $\mathrm{ht}(X) = \mathrm{rank}_{W(K)}(\mathbb{D}(X))$, and we have a functorial isomorphism $\mathrm{Lie}(X) \cong \mathbb{D}(X)/V \cdot \mathbb{D}(X)$.*

(4) *Let X^t be the Serre-dual of the p-divisible group of X. Then the Dieudonné module $\mathbb{D}(X^t)$ can be described in terms of $\mathbb{D}(X)$ as follows. The underlying $W(K)$-module is the linear dual $\mathbb{D}(X)^\vee := \mathrm{Hom}_{W(K)}(\mathbb{D}(X), W(K))$ of $\mathbb{D}(X)$. The actions of V and F on $\mathbb{D}(X)^\vee$ are defined as follows:*

$$(V \cdot h)(m) = {}^{\sigma^{-1}}(h(Fm)), \quad (F \cdot h)(m) = {}^{\sigma}(h(Vm))$$

for all $h \in \mathbb{D}(X)^\vee = \mathrm{Hom}_{W(K)}(\mathbb{D}(X), W(K))$ and all $m \in \mathbb{D}(X)$.

(5) *A p-divisible group X over K is étale if and only if $V : \mathbb{D}(X) \to \mathbb{D}(X)$ is bijective, or equivalently, $F : \mathbb{D}(X) \to \mathbb{D}(X)$ is divisible by p. A p-divisible group X over K is multiplicative if and only if $V : \mathbb{D}(X) \to \mathbb{D}(X)$ is divisible by p, or equivalently, $F : \mathbb{D}(X) \to \mathbb{D}(X)$ is bijective. A p-divisible group X over K has no non-trivial étale quotient nor non-trivial multiplicative p-divisible subgroup if and only if both F and V are topologically nilpotent on $\mathbb{D}(X)$.*

Remark 4.34.

(1) See [**57**] for Theorem 4.33.

(2) When $p > 2$, the Dieudonné module $\mathbb{D}(X)$ attached to a p-divisible group over K can also be defined in terms of the covariant Dieudonné crystal attached to X described in 2.4. In short, $\mathbb{D}(X)$ "is" $\mathbb{D}(X/W(K))_{W(K)}$, the limit of the "values" of the Dieudonné crystal at the divided power structures

$$(W(K)/p^m W(K), pW(K)/p^m W(K), \gamma)$$

as $m \to \infty$, where these are the reductions modulo p^m of the natural DP-structure on $(W(K), pW(K))$. Recall that the natural DP-structure on $(W(K), pW(K))$ is given by $\gamma_i(x) = \frac{x^i}{i!} \quad \forall x \in pW(K)$; the condition that $p > 2$ implies that the induced DP structure on

$$(W(K)/p^m W(K), pW(K)/p^m W(K))$$

is nilpotent.

Proposition 4.35. $\boxed{\text{BB}}$ *Let X be a p-divisible group over K. We have a natural isomorphism*

$$\mathrm{Hom}_K(\alpha_p, X[p]) \cong \mathrm{Hom}_{W(K)}\left(\mathbb{D}(X)^\vee/(V\mathbb{D}(X)^\vee + F\mathbb{D}(X)^\vee), B(K)/W(K)\right),$$

where $B(K) = \mathrm{frac}(W(K))$ is the fraction field of $W(K)$. In particular we have

$$\dim_K(\mathrm{Hom}_K(\alpha_p, X[p])) = a(\mathbb{D}(X)).$$

The natural number $a(\mathbb{D}(X))$ of a p-divisible group X over K is zero if and only if X is an extension of an étale p-divisible group by a multiplicative p-divisible group.

For the notation $a(M)$ see 4.29, and for $a(G)$ see 5.4.

Exercise 4.36.

(i) Prove that $\mathrm{ht}(G_{m,n}) = m + n$.

(ii) Prove that $\dim(G_{m,n}) = m$.

(iii) Show that $G_{0,1}$ is isomorphic to the étale p-divisible group $\mathbb{Q}_p/\mathbb{Z}_p$, and $G_{1,0}$ is isomorphic to the multiplicative p-divisible group $\mu_\infty = \mathbb{G}_m[p^\infty]$.

(iv) Show that $\mathrm{End}(G_{m,n}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a central division algebra over $\mathbb{Q}_p$ of dimension $(m+n)^2$, and compute the Brauer invariant of this central division algebra.

(iv) Relate $G_{m,n}$ to $G_{n,m}$.

(v) Determine all pairs (m,n) such that $\mathrm{End}(G_{m,n})$ is the maximal order of the division algebra $\mathrm{End}(G_{m,n}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Theorem 4.37. $\boxed{\text{BB}}$ *Let $k \supset \mathbb{F}_p$ be an algebraically closed field. Let X be a simple p-divisible group over k, i.e., X has no non-trivial quotient p-divisible groups. Then X is isogenous to $G_{m,n}$ for a uniquely determined pair of natural numbers m, n with $\gcd(m, n) = 1$, i.e., there exists a surjective homomorphism $X \to G_{m,n}$ with finite kernel.*

Definition 4.38.

(i) The slope of $G_{m,n}$ is $m/(m+n)$ with multiplicity $m+n$. The Newton polygon of $G_{m,n}$ is the line segment in the plane from $(0,0)$ to $(m+n, m)$. The slope sequence of $G_{m,n}$ is the sequence $(m/(m+n), \ldots, m/(m+n))$ with $m+n$ entries.

(ii) Let X be a p-divisible group over a field $K \supset \mathbb{F}_p$, and let k be an algebraically closed field containing K. Suppose that X is isogenous to

$$G_{m_1,n_1} \times_{\mathrm{Spec}(k)} \cdots \times_{\mathrm{Spec}(k)} G_{m_r,n_r}$$

$\gcd(m_i, n_i) = 1$ for $i = 1, \ldots, r$, and $m_i/(m_i + n_i) \leq m_{i+1}/(m_{i+1} + n_{i+1})$ for $i = 1, \ldots, r-1$. Then the Newton polygon of X is defined by the data $\sum_{i=1}^r (m_i, n_i)$. Its slope sequence is the concatenation of the slope sequence for $G_{m_1,n_1}, \ldots, G_{m_r,n_r}$.

Example. A p-divisible group X over K is étale (resp. multiplicative) if and only if all of its slopes are equal to 0 (resp. 1).

Exercise 4.39. Suppose that X is a p-divisible group over K such that X is isogenous to $G_{1,n}$ (resp. $G_{m,1}$). Show that X is isomorphic to $G_{1,n}$ (resp. $G_{m,1}$).

Exercise 4.40. Let $\beta_1 \leq \cdots \leq \beta_h$ be the slope sequence of a p-divisible group over K of height h. Prove that the slope sequence of the Serre dual X^t of X is $1 - \beta_h, \ldots, 1 - \beta_1$. (HINT: First show that $G_{m,n}^t \cong G_{n,m}$.)

Conclusion 4.41. Let $K \supset \mathbb{F}_p$ be a field, and let k be an algebraically closed field containing K.

- Any p-divisible group X over K admits an isogeny $X \otimes k \sim \prod_i G_{m_i,n_i}$.
- The Newton polygon $\mathcal{N}(G_{m,n})$ is isoclinic (all slopes are the same) of height $m+n$ and slope $m/(m+n)$.
- In this way the Newton polygon $\mathcal{N}(X)$ is determined. Write $h = h(X)$ for the height of X and $d = \dim(X)$ for the dimension of X. The Newton polygon $\mathcal{N}(X)$ ends at $(h(X), \dim(X))$.
- The isogeny class of a p-divisible group over any algebraically closed field k uniquely determines (and is uniquely determined by) its Newton polygon:

Theorem 4.42. (Dieudonné and Manin, see [**48**], "Classification theorem" on page 35)

$$\{p\text{-divisible groups } X \text{ over } k\}/\sim_k \quad \xrightarrow{\sim} \quad \{\text{Newton polygon}\}$$

In words, p-divisible groups over an algebraically closed field $k \supset \mathbb{F}_p$ are classified up to isogeny by their Newton polygons.

Exercise 4.43. Show that there are infinitely many non-isomorphic p-divisible groups with slope sequence $(1/2, 1/2, 1/2, 1/2)$ (resp. $(1/3, 1/3, 1/3, 2/3, 2/3, 2/3)$) over any infinite perfect field $K \supset \mathbb{F}_p$.

Exercise 4.44. Determine all Newton polygons attached to a p-divisible group of height 6, and the symmetric Newton polygons among them.

Exercise 4.45. Recall that the set of all Newton polygons is partially ordered; $\zeta_1 \prec \zeta_2$ if and only if ζ_1, ζ_2 have the same end points, and ζ_2 lies below ζ_1. Show that this poset is *ranked*, i.e., any two maximal chains between two elements of this poset have the same length.

Exercise 4.46. Prove the equivalence of the statements in 10.10 that characterize ordinary abelian varieties.

Theorem 4.47. $\boxed{\text{BB}}$ *Let S be a scheme such that p is locally nilpotent in $\mathcal{O}_S$. Let $X \to S$ be a p-divisible group over S. Suppose that a point s is a specialization of a point $s' \in S$. Let $\mathcal{N}(X_s)$ and $\mathcal{N}(X_{s'})$ be the Newton polygon of the fibers X_s and $X_{s'}$ of X, respectively. Then $\mathcal{N}(X_s) \prec \mathcal{N}(X_{s'})$, i.e., the Newton polygon $\mathcal{N}(X_s)$ of the specialization lies above (or is equal to) the Newton polygon $\mathcal{N}(X_{s'})$.*

This result first appeared in a letter from Grothendieck to Barsotti dated May 11, 1970; see the Appendix in [**34**]. See [**40**], 2.3.2 for the proof of a stronger result, that the locus in the base scheme S with Newton polygon $\prec \xi$ is closed for any Newton polygon ξ; see 1.19, 1.20.

Exercise 4.48.

(i) Construct an example of a specialization of ordinary p-divisible group of dimension 3 and height 6 to a p-divisible group with slopes $1/3$ and $2/3$, using the theory of Cartier modules.

(ii) Construct an example of a non-constant p-divisible group with constant slope.

4.49. Here is an explicit description of the Newton polygon of an abelian variety A over a finite field $\mathbb{F}_q \supset \mathbb{F}_p$. We may and do assume that A is simple over $\mathbb{F}_q$. By Tate's Theorem 10.17, we know that the abelian variety A is determined by its q-Frobenius π_A up to $\mathbb{F}_q$-rational isogeny. Then the slopes of A are determined by the p-adic valuations of π_A as follows. For every rational number $\lambda \in [0, 1]$, the multiplicity of the slope λ in the Newton polygon of A is

$$\sum_{v \in \varphi_{p,\lambda}} [\mathbb{Q}(\pi_A)_v : \mathbb{Q}_p]$$

where $\varphi_{p,\lambda}$ is the finite set consisting of all places v of $\mathbb{Q}(\pi_A)$ above p such that $v(\pi_A) = \lambda \cdot v(q)$.

Exercise 4.50. Let E be an ordinary elliptic curve over $\mathbb{F}$. Let $L = \mathrm{End}(E)^0$. Show that L is an imaginary quadratic field which is split at p and $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Exercise 4.51. Let L be an imaginary quadratic field which is split at p. Let r, s be positive rational numbers such that $\gcd(r, s) = 1$ and $2r < s$. Use Tate's

Theorem 10.17 to show that there exists a simple s-dimensional abelian variety A over a finite field $\mathbb{F}_q \supset \mathbb{F}_p$ such that $\mathrm{End}(A)^0 = L$ and the slopes of the Newton polygon of A are $\frac{r}{s}$ and $\frac{s-r}{s}$.

Exercise 4.52. Let m, n be positive integers with $\gcd(m, n) = 1$, and let $h = m + n$. Let D be a central division algebra over $\mathbb{Q}_p$ of dimension h^2 with Brauer invariant n/h. This means that there exists a homomorphism $j : \mathrm{frac}(W(\mathbb{F}_{p^h})) \to D$ of $\mathbb{Q}_p$-algebras and an element $u \in D^\times$ with $\frac{\mathrm{ord}(u)}{\mathrm{ord}(p)} \equiv \frac{n}{h} \pmod{\mathbb{Z}}$ such that

$$u \cdot j(x) \cdot u^{-1} = j(\sigma(x)) \quad \forall x \in W(\mathbb{F}_{p^h}).$$

Here ord denotes the normalized valuation on D, and σ is the canonical lifting of Frobenius on $W(\mathbb{F}_{p^h})$. Changing u by a suitable power of p, we may and do assume that $u, pu^{-1} \in \mathcal{O}_D$, where $\mathcal{O}_D$ is the maximal order of D.

Let M be the left $W(\mathbb{F}_{p^h})$-module underlying $\mathcal{O}_D$, where the left $W(\mathbb{F}_{p^h})$-module structure is given by left multiplication with elements of $j(W(\mathbb{F}_{p^h}))$. Let $F : M \to M$ be the operator $z \mapsto u \cdot z$, and let $V : M \to M$ be the operator $z \mapsto pu^{-1} \cdot z$. This makes M a module over the Dieudonné ring $R_{\mathbb{F}_{p^h}}$.

(1) Show that right multiplication by elements of $\mathcal{O}_D$ induces an isomorphism

$$\mathcal{O}_D^{\mathrm{opp}} \xrightarrow{\sim} \mathrm{End}^0_{R_{\mathbb{F}_{p^h}}}(M).$$

(2) Show that $\mathcal{O}_D^{\mathrm{opp}} \xrightarrow{\sim} \mathrm{End}^0_{R_K}(W(K) \otimes_{W(\mathbb{F}_{p^h})} M)$ for every perfect field $K \supset \mathbb{F}_{p^h}$.

(3) Show that there exists a $W(\mathbb{F}_{p^h})$-basis of M $e_0, e_1, \ldots, e_{h-1}$ such that if we extend $e_0, e_1, \ldots, e_{h-1}$ to a cyclic sequence $(e_i)_{i \in \mathbb{Z}}$ by the condition that $e_{i+h} = p \cdot e_i$ for all $i \in \mathbb{Z}$, we have

$$F \cdot e_i = e_{i+n}, \quad V \cdot e_i = e_{i+m}, \quad p \cdot e_i = e_{i+m+n}, \quad M_{m,n} := \oplus_{0 \le i < m+n} W \cdot e_i.$$

(4) Show that the p-divisible group $H_{m,n}$ corresponding to the Dieudonné module M has dimension m and slope m/h.

(5) Suppose that X is a p-divisible group over a perfect field $K \supset \mathbb{F}_p$ such that $\mathrm{End}^0(X)$ is isomorphic to $\mathcal{O}_D^{\mathrm{opp}}$. Show that $K \supset \mathbb{F}_{p^h}$ and X is isomorphic to $H_{m,n} \times_{\mathrm{Spec}(\mathbb{F}_{p^h})} \mathrm{Spec}(K)$.

Proposition 4.53. $\boxed{\text{BB}}$

(i) *There is an equivalence of categories between the category of finite group schemes over the perfect base field K and the category of left R_K-modules which are $W(K)$-modules of finite length. Denote by $\mathbb{D}(G)$ the left R_K-module attached to a finite group scheme G over K.*

(ii) *Suppose that $0 \to G \to X \xrightarrow{\beta} Y \to 0$ is a short exact sequence, where G is a finite group scheme over K, and $\beta : X \to Y$ is an isogeny between p-divisible groups over K. Then we have a natural isomorphism*

$$\mathbb{D}(G) \xrightarrow{\sim} \mathrm{Ker}\left(\mathbb{D}(X) \otimes_{W(K)} B(K)/W(K) \xrightarrow{\beta} \mathbb{D}(Y) \otimes_{W(K)} B(K)/W(K)\right)$$

of left R_K-modules.

Remark.

(i) We say that $\mathbb{D}(G)$ is the covariant Dieudonné module of G, abusing the terminology, because $\mathbb{D}(G)$ is not a free $W(K)$-module.

(ii) Proposition 4.53 is a covariant version of the classical contravariant Dieudonné theory in [**24**] and [**48**]. See also [**60**].

4.54. Remarks on the operators F and V. For group schemes in characteristic p we have the Frobenius homomorphism, and for commutative group schemes the Verschiebung; see 10.23, 10.24. Also for Dieudonné modules such homomorphisms are studied. However, some care has to be taken. In the *covariant* Dieudonné module theory the Frobenius homomorphism on commutative group schemes corresponds to the operator V on the related modules, and the Verschiebung homomorphism on commutative flat group schemes gives the operator F on modules; for details see [**67**], 15.3. In case confusion is possible we write F (resp. V) for the Frobenius (resp. Verschiebung) homomorphism on group schemes and $\mathcal{V} = \mathbb{D}(F)$ (resp. $\mathcal{F} = \mathbb{D}(V)$) for the corresponding operator on modules,

5. Cayley-Hamilton: a conjecture by Manin and the weak Grothendieck conjecture

Main reference: [**65**].

5.1. In this section we develop non-commutative generalizations of the Cayley Hamilton theorem: a matrix $\mathcal{F}$ is a zero of its own characteristic polynomial.

Exercise 5.2. Prove the classical Cayley-Hamilton theorem for a matrix over a commutative ring R: let X be an $n \times n$ matrix with entries in R with characteristic polynomial $g(T) = \mathrm{Det}(X - T \cdot \mathbf{1}_n) \in R[T]$; then the matrix $g(X)$ is the zero matrix.

Here are some suggestions for a proof:

(a) For any commutative ring R, and an $n \times n$ matrix X with entries in R there exists a ring homomorphism $h : \mathbb{Z}[t_{1,1}, \cdots, t_{i,j}, \cdots, t_{n,n}] \to R$ such that the matrix $(t) = (t_{i,j} \mid 1 \leq i, j \leq n)$ is mapped to X.

(b) Let $h^\sim : R[T] \to \mathbb{Z}[t_{ij}][T]$ be the ring homomorphism induced by h. Let $G(T) = \mathrm{Det}((t) - T \cdot \mathbf{1}_n) \in \mathbb{Z}[t_{ij}][T]$, so that $h^\sim(G) = g$. Conclude that it suffices to prove the statement for a commutative ring that contains $\mathbb{Z}[t_{1,1}, \ldots, t_{i,j}, \ldots, t_{n,n}]$.

(c) Construct $\mathbb{Z}[t_{i,j} \mid 1 \leq i, j \leq n] \hookrightarrow \mathbb{C}$, and apply the classical Cayley-Hamilton theorem for $\mathbb{C}$ (which is a consequence of the theorem of canonical forms). Alternatively, show that the matrix (t) considered over $\mathbb{C}$ has mutually different eigenvalues.

Here are suggestions for a different proof:

(1) Show it suffices to prove this for an algebraically closed field of characteristic zero.

(2) Show that the classical Cayley-Hamilton theorem holds for a matrix which is in diagonal form with all diagonal elements mutually different.

(3) Show that the set of all conjugates of matrices as in (2) is Zariski dense in $\mathrm{Mat}(n \times n)$. Finish the proof.

5.3. We will develop a useful analog of this Cayley-Hamilton theorem over the Dieudonné ring. Note that over a non-commutative ring there is no reason that any straightforward analog of Cayley-Hamilton should be true. However, given a specific element in a special situation, we construct an operator $g(\mathcal{F})$ which annihilates that specific element in the Dieudonné module. Warning: In general $g(\mathcal{F})$ does not annihilate all elements of the Dieudonné module.

Notation 5.4. Let G be a group scheme over a field $K \supset \mathbb{F}_p$. Consider $\alpha_p = \mathrm{Ker}(F : \mathbb{G}_a \to \mathbb{G}_a)$. Choose a perfect field L containing K. Note that $\mathrm{Hom}(\alpha_p, G_L)$ is a right module over $\mathrm{End}(\alpha_p \otimes_{\mathbb{F}_p} L) = L$. We define

$$a(G) = \dim_L (\mathrm{Hom}(\alpha_p, G_L)).$$

Remarks. For any field L we write α_p instead of $\alpha_p \otimes_{\mathbb{F}_p} L$ if no confusion is likely.

The group scheme $\alpha_{p,K}$ over a field K corresponds under 5.7 (in any case) or by Dieudonné theory (in case K is perfect) to the module K^+ with operators $\mathcal{F} = 0$ and $\mathcal{V} = 0$.

If K is not perfect it might happen that

$$\dim_K (\mathrm{Hom}(\alpha_p, G)) < \dim_L (\mathrm{Hom}(\alpha_p, G_L));$$

see the Exercise 5.8 below.

However, if L is perfect and $L \subset L'$ is any field extension then

$$\dim_L (\mathrm{Hom}(\alpha_p, G_L)) = \dim_{L'} (\mathrm{Hom}(\alpha_p, G_{L'})).$$

Hence the definition of $a(G)$ is independent of the chosen perfect extension L.

Exercise 5.5.

    (i) Let N be a finite group scheme over a perfect field K. Assume that F and V on N are nilpotent on N, and suppose that $a(N) = 1$. *Show that the Dieudonné module $\mathbb{D}(N)$ is generated by one element over the Dieudonné ring.*

    (ii) Let A be an abelian variety over a perfect field K. Assume that the p-rank of A is zero, and that $a(A) = 1$. *Show that the Dieudonné module $\mathbb{D}(A[p^\infty])$ is generated by one element over the Dieudonné ring.*

Remark. We will see that if $a(X_0) = 1$, then the Newton polygon stratum $\mathcal{W}_{\mathcal{N}(X_0)}(\mathrm{Def}(X_0))$ in $\mathcal{D}(X_0)$ *is non-singular.* See 1.19 and 5.11. Similarly, let (A, λ) be a principally polarized abelian variety, $\xi = \mathcal{N}(A)$. The Newton polygon stratum $\mathcal{W}_\xi(\mathcal{A}_{g,1,n})$ will be shown to be regular at the point (A, λ) (here we work with a fine moduli scheme: assume $n \geq 3$). In the above $\mathcal{W}_\xi(\mathcal{A}_{g,1,n})$ denotes the locus in $\mathcal{A}_{g,1,n}$ with Newton polygon $\prec \xi$ (i.e., lying above ξ); similarly for $\mathcal{W}_{\mathcal{N}(X_0)}(\mathcal{D}(X_0))$; see 1.19, 5.11.

We see that we can a priori consider a set of points where the Newton polygon stratum is guaranteed to be non-singular. That is the main result of this section. Then, in Section 7 we show that such points are dense in both cases considered, p-divisible groups and *principally* polarized abelian varieties.

We give an example, with K non-perfect, where $\dim_K (\mathrm{Hom}(\alpha_p, G)) < a(G)$; we see that the condition "L is perfect" is necessary in 5.4 .

5.6. "Dieudonné modules" over non-perfect fields? This is a difficult topic. However, in one special case statements and results are easy.

p-Lie algebras. Basic reference [**25**]. We will need this theory only in the commutative case. For more general statements see [**25**], II.7.

Let $K \supset \mathbb{F}_p$ be a field. A commutative finite group scheme of *height one* over K is a finite commutative group scheme N over K such that $(F : N \to N^{(p)}) = 0$, the zero map. Denote the category of such objects by GF_K.

A commutative finite dimensional p-Lie algebra M over K is a pair (M, g), where M is a finite dimensional vector space over K, and $g : M \to M$ is a homomorphism of additive groups with the property

$$g(b \cdot x) \quad = \quad b^p \cdot g(x).$$

Denote the category of such objects by Liep_K.

Theorem 5.7. $\boxed{\mathrm{BB}}$ *There is an equivalence of categories*

$$\mathcal{D}_K : \mathrm{GF}_K \xrightarrow{\sim} \mathrm{Liep}_K.$$

This equivalence commutes with base change. If K is a perfect field this functor coincides with the Dieudonné module functor: $\mathcal{D}_K = \mathbb{D}$, and the operator g on $\mathcal{D}_K(N)$ corresponds to the operator F on $\mathbb{D}(N)$ for every $N \in \mathrm{Ob(GF)}_K$.

See [**25**], II.7.4

Exercise.
(i) Classify all commutative group schemes of rank p over k, an algebraically closed field of characteristic p.
(ii) Classify all commutative group schemes of rank p over a perfect field $K \supset \mathbb{F}_p$.

Remark/Exercise 5.8.
(1) Let K be a non-perfect field, with $b \in K$ and $\sqrt[p]{b} \notin K$. Let (M, g) be the commutative finite dimensional p-Lie algebra defined by:

$$M = K \cdot x \oplus K \cdot y \oplus K \cdot z, \quad g(x) = bz, \ g(y) = z, \ g(z) = 0.$$

Let N be the finite group scheme of height one defined by this p-Lie algebra, i.e., such that $\mathcal{D}_K(N) = (M, g)$, see 5.6. *Show:*

$$\dim_K \left(\mathrm{Hom}(\alpha_p, N) \right) = 1, \quad \dim_k \left(\mathrm{Hom}(\alpha_p, N \times_{\mathrm{Spec}(K)} \mathrm{Spec}(k)) \right) = 2,$$

where $k = k^{\mathrm{alg}} \supset K$.

(2) Let $N_2 = W_2[F]$ be the kernel of $F : W_2 \to W_2$ over $\mathbb{F}_p$; here W_2 is the 2-dimensional group scheme of Witt vectors of length 2. In fact one can define N_2 by $\mathbb{D}(N_2) = \mathbb{F}_p \cdot r \oplus \mathbb{F}_p \cdot s$, $\mathcal{V}(r) = 0 = \mathcal{V}(s) = \mathcal{F}(s)$ and $\mathcal{F}(r) = s$. Let $L = K(\sqrt[p]{b})$. *Show that*

$$N \ncong_K (\alpha_p \oplus W_2[F]) \otimes K \quad \text{and} \quad N \otimes L \cong_L (\alpha_p \oplus W_2[F]) \otimes L.$$

Remark. In [**45**], I.5 Definition (1.5.1) should be given over a perfect field K. We thank Chia-Fu Yu for drawing our attention to this flaw.

5.9. We fix integers $h \geq d \geq 0$, and we write $c := h - d$. We consider Newton polygons ending at (h, d). For such a Newton polygon β we write
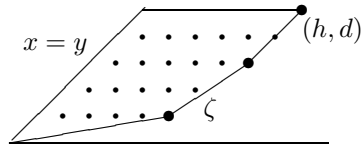
$$\diamondsuit(\beta) := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y < d, \ y < x, \ (x, y) \prec \beta\};$$

here we denote by $(x, y) \prec \beta$ the property "(x, y) is on or above β"; we write

$$\boxed{\dim(\zeta) := \#(\diamondsuit(\zeta)).}$$

Let $\diamondsuit = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 0 \leq y < d, \ y < x \leq y + d\}$.

Example.

$$\zeta = 2 \times (1,0) + (2,1) + (1,5) =$$

$$= 6 \times \tfrac{1}{6} + 3 \times \tfrac{2}{3} + 2 \times \tfrac{1}{1}; \quad h = 11.$$

Here $\dim(\zeta) = \#(\Diamond(\zeta)) = 22$.

Note that for $\rho = d \cdot (1,0) + c \cdot (0,1)$ we have $\dim(\rho) = dc$.

Theorem 5.10. (Newton polygon strata for p-divisible groups) *Suppose $a(X_0) \leq 1$. Write $D = \mathcal{D}(X_0)$. (For notation see 10.21.) For every $\beta \succ \gamma = \mathcal{N}(X_0)$, the Newton polygon stratum: $\mathcal{W}_\beta(D)$ is formally smooth and $\dim(\mathcal{W}_\beta(D)) = \dim(\beta)$. The strata $\mathcal{W}_\beta(D)$ are nested as given by the partial ordering on Newton polygons, i.e.,*

$$\mathcal{W}_\beta(D) \subset \mathcal{W}_\delta(D) \quad \Longleftrightarrow \quad \Diamond(\beta) \subset \Diamond(\delta) \quad \Longleftrightarrow \quad \beta \prec \delta.$$

Generically on $\mathcal{W}_\beta(D)$ the fibers have Newton polygon equal to β.

For the notion "generic" for a p-divisible group over a formal scheme, see 10.21.

5.11. In fact, this can be visualized and made more precise as follows. Choose variables $T_{r,s}$, with $1 \leq r \leq d = \dim(X_0)$, $1 \leq s \leq h = \mathrm{height}(X_0)$ and write these in a diagram

$$
\begin{array}{ccccccc}
& & & & 0 & \cdots & 0 & -1 \\
& & & T_{d,h} & \cdot & & \cdots & T_{1,h} \\
& & \cdot & \vdots & \vdots & & \vdots & \cdot \\
& T_{d,d+2} & \cdots & T_{i,d+2} & \cdots & T_{2,d+2} & T_{1,d+2} & \\
T_{d,d+1} & \cdots & & T_{i,d+1} & \cdots & & T_{1,d+1} &
\end{array}
$$

We show that

$$\mathcal{D}^\wedge = \mathrm{Def}(X_0) = \mathrm{Spf}(k[[Z_{(x,y)} \mid (x,y) \in \Diamond]]), \qquad T_{r,s} = Z_{(s-r,s-1-d)}.$$

Moreover, for any $\beta \succ \mathcal{N}(G_0)$ we write

$$R_\beta = \frac{k[[Z_{(x,y)} \mid (x,y) \in \Diamond]]}{(Z_{(x,y)} \quad \forall (x,y) \notin \Diamond(\beta))} \quad \cong \quad k[[Z_{(x,y)} \mid (x,y) \in \Diamond(\beta)]].$$

CLAIM.

$$(\mathrm{Spec}(R_\beta) \subset \mathrm{Spec}(R)) \quad = \quad (\mathcal{W}_\beta(D) \subset \mathcal{D}).$$

Clearly this claim proves the theorem. We will give a proof of the claim, and hence of this theorem by using the theory of displays and the following tools.

Convention. Let d, c be non-negative integers, and let $h = c + d$. For any $h \times h$ matrix

$$(a) = \left(\begin{array}{cc} A & B \\ C & D \end{array} \right),$$

its associated F-matrix is

$$(\mathcal{F}) = (pa) := \left(\begin{array}{cc} A & pB \\ C & pD \end{array} \right),$$

where A is a $d \times d$ matrix, B is a $d \times c$ matrix, C is a $c \times d$ matrix and D is a $c \times c$ matrix.

Definition 5.12. We consider matrices which can appear as F-matrices associated with a display. Let $d, c \in \mathbb{Z}_{\geq 0}$, and $h = d + c$. Let W be a ring. We say that a display matrix $(a_{i,j})$ of size $h \times h$ is in *normal form* form over W if the F-matrix is of the following form:

$$
\begin{pmatrix}
0 & 0 & \cdots & 0 & a_{1d} & pa_{1,d+1} & \cdots & & \cdots & & \cdots & pa_{1,h} \\
1 & 0 & \cdots & 0 & a_{2d} & \cdots & & & pa_{i,j} & & \cdots & \\
0 & 1 & \cdots & 0 & a_{3d} & & & & 1 \leq i \leq d & & & \\
\vdots & \vdots & \ddots & \ddots & \vdots & & & & d \leq j \leq h & & & \\
0 & 0 & \cdots & 1 & a_{dd} & pa_{d,d+1} & \cdots & & \cdots & & \cdots & pa_{d,h} \\
\\
0 & \cdots & \cdots & 0 & 1 & 0 & & \cdots & & \cdots & \cdots & 0 \\
0 & \cdots & & \cdots & 0 & p & & 0 & & \cdots & \cdots & 0 \\
0 & \cdots & & \cdots & 0 & 0 & & p & & 0 & \cdots & 0 \\
\\
0 & \cdots & & \cdots & 0 & 0 & & 0 & & \ddots & & 0 & 0 \\
0 & \cdots & & \cdots & 0 & 0 & & & \cdots & & & p & 0
\end{pmatrix}
\qquad (\mathcal{F})
$$

with $a_{i,j} \in W$, $a_{1,h} \in W^{*}$; i.e., it consists of blocks of sizes $(d \text{ or } c) \times (d \text{ or } c)$; in the left hand upper corner, which is of size $d \times d$, there are entries in the last column, named $a_{i,d}$, and the entries immediately below the diagonal are equal to 1; the left and lower block has only one element not equal to zero, and it is 1; the right hand upper corner is unspecified and its entries are written $pa_{i,j}$; the right hand lower corner, which is of size $c \times c$, has only entries immediately below the diagonal, and they are all equal to p.

Note that if a Dieudonné module M is defined by a matrix in displayed normal form, then either its p-rank $f(M)$ is maximal, $f = d$, and this happens if and only if $a_{1,d}$ is not divisible by p, or $f(M) < d$, and in that case $a(M) = 1$. The p-rank is zero if and only if $a_{i,d} \equiv 0 \pmod{p}$, $\forall 1 \leq i \leq d$.

Lemma 5.13. $\boxed{\text{BB}}$ *Let M be the Dieudonné module of a p-divisible group G over k with $f(G) = 0$. Suppose $a(G) = 1$. Then there exists a W-basis for M on which $\mathcal{F}$ has a matrix which is in normal form. In this case the entries $a_{1,d}, \ldots, a_{d,d}$ are divisible by p, they can be chosen to be equal to zero.*

Lemma 5.14. (of Cayley-Hamilton type) *Let L be a field of characteristic p, let $W = W_{\infty}(L)$ be its ring of infinite Witt vectors. Let X be a p-divisible group, with $\dim(G) = d$, and $\mathrm{height}(G) = h$, with Dieudonné module $\mathbb{D}(X) = M$. Suppose there is a W-basis of M, such that the display matrix $(a_{i,j})$ on this base gives an $\mathcal{F}$-matrix in normal form as in 5.12. We write $e = X_1 = e_1$ for the first base vector. Then for the expression*

$$
P := \sum_{i=1}^{d} \sum_{j=d}^{h} p^{j-d} a_{i,j}^{\sigma^{h-j}} \mathcal{F}^{h+i-j-1}
$$

we have

$$
\mathcal{F}^{h} \cdot e = P \cdot e \, .
$$

Note that we take powers of $\mathcal{F}$ in the σ-linear sense, i.e., if the display matrix is

$$(a) = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \text{ whose associated } F\text{-matrix is } (\mathcal{F}) = (pa) = \begin{pmatrix} A & pB \\ C & pD \end{pmatrix}$$

then $\mathcal{F}^n$ is given by the matrix

$$(\mathcal{F}^n) = (pa) \cdot (pa^\sigma) \cdot \cdots \cdot (pa^{\sigma^{n-1}}).$$

The exponent $h + i - j - 1$ runs from $0 = h + 1 - h - 1$ to $h - 1 = h + d - d - 1$.

Note that we do not claim that P and $\mathcal{F}^h$ have the same effect on all elements of M.

PROOF. Note that $\mathcal{F}^{i-1}e_1 = e_i$ for $i \leq d$.

CLAIM. *For $d \leq s < h$ we have:*

$$\mathcal{F}^s X = \left(\sum_{i=1}^{d} \sum_{j=d}^{s} \mathcal{F}^{s-j} p^{j-d} a_{i,j} \mathcal{F}^{i-1} \right) X + p^{s-d} e_{s+1}.$$

This is correct for $s = d$. The induction step from s to $s + 1 < h$ follows from

$$\mathcal{F}e_{s+1} = \left(\sum_{i=1}^{d} p \, a_{i,s+1} F^{i-1} \right) X + p e_{s+2}.$$

This proves the claim. Computing $\mathcal{F}(\mathcal{F}^{h-1}X)$ gives the desired formula. □

Proposition 5.15. *Let k be an algebraically closed field of characteristic p, let $W = W_\infty(K)$ be its ring of infinite Witt vectors. Suppose G is a p-divisible group over k such that for its Dieudonné module the map $\mathcal{F}$ is given by a matrix in normal form. Let P be the polynomial given in the previous proposition. The Newton polygon $\mathcal{N}(G)$ of this p-divisible group equals the Newton polygon given by the polynomial P.*

PROOF. Consider the $W[F]$-submodule $M' \subset M$ generated by $X = e_1$. Note that M' contains $X = e_1, e_2, \ldots, e_d$. Also, it contains $\mathcal{F}e_d$, which equals e_{d+1} plus a linear combination of the previous ones; hence $e_{d+1} \in M'$. In the same way we see: $pe_{d+2} \in M'$, and $p^2 e_{d+3} \in M'$ and so on. This shows that $M' \subset M = \bigoplus_{i \leq h} W \cdot e_i$ is of finite index. We see that $M' = W[F]/W[F] \cdot (F^h - P)$. From this we see by the classification of p-divisible groups up to isogeny, that the result follows by [**48**], II.1; also see [**24**], pp. 82-84. By [**24**], page 82, Lemma 2 we conclude that the Newton polygon of M' in case of the monic polynomial $\mathcal{F}^h - \sum_0^m b_i \mathcal{F}^{m-i}$ is given by the lower convex hull of the pairs $\{(i, v(b_i)) \mid i\}$. Hence the proposition is proved. □

Corollary 5.16. *We take the notation as above. Suppose that every element $a_{i,j}$, $1 \leq i \leq c$, $c \leq j \leq h$, is either equal to zero, or is a unit in $W(k)$. Let S be the set of pairs (i, j) with $0 \leq i \leq c$ and $c \leq j \leq h$ for which the corresponding element is non-zero:*
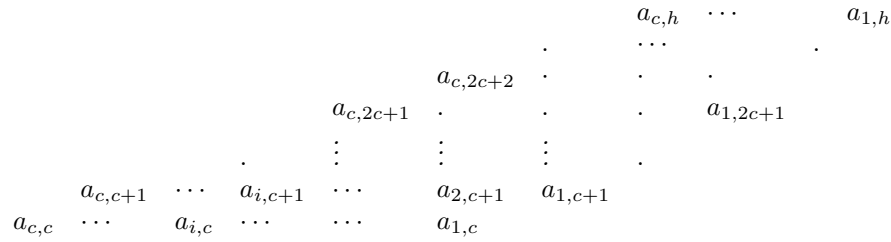
$$(i, j) \in S \quad \Longleftrightarrow \quad a_{i,j} \neq 0.$$

Consider the image T under

$$S \to T \subset \mathbb{Z} \times \mathbb{Z} \quad \text{given by} \quad (i, j) \mapsto (j + 1 - i, j - c).$$

Then $\mathcal{N}(X)$ is the lower convex hull of the set $T \subset \mathbb{Z} \times \mathbb{Z}$ and the point $(0, 0)$; note that $a_{1,h} \in W^*$, hence $(h, h - c = d) \in T$. This can be visualized in the following

diagram (we have pictured the case $d \leq h - d$):

$$
\begin{array}{ccccccccc}
 & & & & & & a_{c,h} & \cdots & & & a_{1,h} \\
 & & & & & & & \cdots & & & \\
 & & & & a_{c,2c+2} & \cdot & & \cdot & & \cdot & \\
 & & & a_{c,2c+1} & \cdot & & \cdot & & \cdot & a_{1,2c+1} & \\
 & & & \vdots & & \vdots & & \vdots & \cdot & & \\
 & a_{c,c+1} & \cdots & a_{i,c+1} & \cdots & & a_{2,c+1} & a_{1,c+1} & & & \\
a_{c,c} & \cdots & & a_{i,c} & \cdots & \cdots & a_{1,c} & & & &
\end{array}
$$

Here the element $a_{c,c}$ is in the plane with coordinates $(x = 1, y = 0)$ and $a_{1,h}$ has coordinates $(x = h, y = h - c = d)$. One erases the spots where $a_{i,j} = 0$, and one leaves the places where $a_{i,j}$ is as unit. The lower convex hull of these points and $(0,0)$ (and $(h, h - c)$) equals $\mathcal{N}(X)$.

Theorem 5.10 proves the following statement:

Conjecture. (The weak Grothendieck conjecture) *Given Newton polygons $\beta \prec \delta$ there exists a family of p-divisible groups over an integral base having δ as Newton polygon for the generic fiber, and β as Newton polygon for a closed fiber.*

However, we will prove a much stronger result later.

5.17. For principally quasi-polarized p-divisible groups and for principally polarized abelian varieties we have an analogous method.

5.18. We fix an integer g. For every *symmetric* Newton polygon ξ of height $2g$ we define

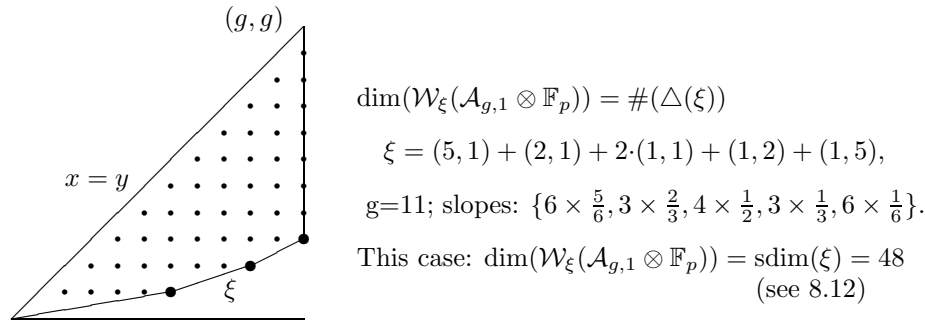$$\triangle(\xi) = \{\, (x,y) \in \mathbb{Z} \times \mathbb{Z} \mid y < x \leq g, \ (x,y) \prec \xi \,\},$$

and we write

$$\boxed{\operatorname{sdim}(\xi) := \#(\triangle(\xi)).}$$

Define $\triangle$ by

$$\triangle = \{\, (x,y) \in \mathbb{Z} \times \mathbb{Z} \mid 0 \leq y < x \leq g \,\}.$$

Example.

$$\dim(\mathcal{W}_\xi(\mathcal{A}_{g,1} \otimes \mathbb{F}_p)) = \#(\triangle(\xi))$$

$$\xi = (5,1) + (2,1) + 2{\cdot}(1,1) + (1,2) + (1,5),$$

$$\text{g=11; slopes: } \{6 \times \tfrac{5}{6}, 3 \times \tfrac{2}{3}, 4 \times \tfrac{1}{2}, 3 \times \tfrac{1}{3}, 6 \times \tfrac{1}{6}\}.$$

This case: $\dim(\mathcal{W}_\xi(\mathcal{A}_{g,1} \otimes \mathbb{F}_p)) = \operatorname{sdim}(\xi) = 48$
(see 8.12)

Suppose given a p-divisible group X_0 over k of dimension g with a principal quasi-polarization λ. We write $\mathcal{N}(X_0) = \gamma$; this is a symmetric Newton polygon. We write $D = \mathcal{D}(X_0, \lambda)$ for the universal deformation space; in particular $D = \operatorname{Spec}(R)$, where $\operatorname{Def}(X_0, \lambda) = \operatorname{Spf}(R)$; see 10.21. For every symmetric Newton polygon ξ with $\xi \succ \gamma$ we define $W_\xi(D) \subset D$ as the maximal closed, reduced subscheme of D carrying all fibers with Newton polygon equal to or above ξ; this

space exists and is closed in D by Grothendieck-Katz, see [40], Theorem 2.3.1 on page 143. Note that $W_\rho = D$, where $\rho = g \cdot ((1,0) + (0,1))$.

Theorem 5.19. (NP-strata for principally quasi-polarized formal groups) *Suppose* $a(X_0) \leq 1$. *Write* $D = \mathcal{D}(X_0, \lambda)$. *For every symmetric* $\xi \succ \gamma := \mathcal{N}(X_0)$ *we have:* $\mathcal{W}_\xi(D)$ *is formally smooth, with* $\dim(\mathcal{W}_\xi(D)) = \mathrm{sdim}(\xi)$. *The strata* $W'_\xi := \mathcal{W}_\xi(D) \subset \mathcal{D}(X_0, \lambda)$ *are nested as given by the partial ordering on symmetric Newton polygons, i.e.,*

$$W'_\xi \quad \subset \quad W'_\delta \quad \Longleftrightarrow \quad \triangle(\xi) \subset \triangle(\delta) \quad \Longleftrightarrow \quad \xi \prec \delta.$$

Generically on W'_ξ *the fibers have Newton polygon equal to* ξ. *We can choose a coordinate system on* $\mathcal{D}(X_0, \lambda)$ *in which all* W'_ξ *are given by linear equations.*

Corollary 5.20. *Suppose given a principally polarized abelian variety* (A_0, λ_0) *over* k *with* $a(A_0) \leq 1$. *Strata in* $\mathcal{D}(X_0, \lambda_0)$ *according to Newton polygons are exactly as in 5.19. In particular, the fiber above the generic point of* W'_ξ *is a principally polarized abelian scheme over* $\mathrm{Spec}(B_\xi)$ *having Newton polygon equal to* ξ.

PROOF. (of 5.20, assuming 5.19) We write $(A_0, \lambda_0)[p^\infty] =: (X_0, \lambda_0)$. By Serre-Tate theory, see [42], Section 1, the formal deformation spaces of (A_0, λ_0) and of (X_0, λ_0) are canonically isomorphic, say $(A', \lambda) \to \mathrm{Spf}(R)$ and $(\mathcal{X}', \lambda) \to \mathrm{Spf}(R)$ and $(A', \lambda)[p^\infty] \cong (\mathcal{X}', \lambda)$. By Chow-Grothendieck, see [32], III^1.5.4 (this is also called a theorem of "GAGA-type"), the formal polarized abelian scheme is algebraizable, and we obtain the universal deformation as a polarized abelian scheme $(A, \lambda) \to \mathrm{Spec}(R)$; see 10.21. We consider the generic point of $W_\xi \subset \mathcal{D}(X_0, \lambda_0) = \mathrm{Spec}(R)$. The Newton polygon of fibers can be read off from the fibers in $(\mathcal{X}, \lambda) \to \mathrm{Spec}(R)$. This proves that 5.20 follows from 5.19. □

PROOF. (of 5.19) The proof of this theorem is analogous to the proof of 5.10. We use the diagram

$$
\begin{pmatrix}
 & & & & & -1 \\
 & & T_{g,g} & \cdots & T_{1,g} & \\
 & & & \vdots & & \\
1 & & T_{g,1} & \cdots & T_{1,1} &
\end{pmatrix}
$$

Here $T_{i,j}$, $1 \leq i, j \leq g$, is written on the place with coordinates $(g - i + j, j - 1)$. We use the ring

$$B := \frac{k[[T_{i,j}; 1 \leq i, j \leq g]]}{(T_{k\ell} - T_{\ell k})}, \quad T_{i,j} = Z_{(g-i+j, j-1)}, \quad (g - i + j, j - 1) \in \triangle.$$

Note that $B = k[[T_{i,j} \mid 1 \leq i \leq j \leq g]] = k[[Z_{x,y} \mid (x,y) \in \triangle]]$. For a symmetric ξ with $\xi \succ \mathcal{N}(X_0)$ we consider

$$B_\xi = \frac{k[[T_{i,j}; 1 \leq i, j \leq g]]}{(T_{k\ell} - T_{\ell k}, \quad \text{and} \quad Z_{(x,y)} \ \forall (x,y) \notin \triangle(\xi))} \quad \cong \quad k[[Z_{(x,y)} \mid (x,y) \in \triangle(\xi)]].$$

With these notations, applying 5.14 and 5.16 we finish the proof of 5.19 as we did in the proof of 5.10 above. □

　　　If the condition $a(A_0) \leq 1$ in the theorem and corollary above is replaced by $a(A_0) = 0$ all fibers above this deformation space are ordinary.

5.21. A conjecture by Manin. Let A be an abelian variety. The Newton polygon $\mathcal{N}(A)$ is symmetric (see 1.18). A conjecture by Manin expects the converse to hold:

Conjecture. (see [**48**], page 76, Conjecture 2) *For any symmetric Newton polygon ξ there exists an abelian variety A such that $\mathcal{N}(A) = \xi$.*

This was proved in the Honda-Tate theory, see 3.12, 3.14. *We sketch a pure characteristic p proof,* see [**65**], Section 5. It is not difficult to show that there exists a principally polarized supersingular abelian variety (A_0, λ_0) with $a(A_0) = 1$, see [**65**], Section 4; this also follows from [**45**], 4.9. By 5.19 it follows that $\mathcal{W}^0_\xi(\mathcal{D}(A_0, \lambda_0))$ is non-empty, *which proves the Manin conjecture.* □

5.22. Let $g \in \mathbb{Z}_{\geq 3}$. There exists an abelian variety in characteristic p which has p-rank equal to zero, and which is not supersingular. In fact choose $\xi = \sum(m_i, n_i)$, a symmetric Newton polygon with $m_i > 0$ and $n_i > 0$ for every i and $(m_i, n_i) \neq (1, 1))$ for at least one i. For example $\xi = (1, g-1) + (g-1, 1)$ or $\xi = (2, 1) + (g-3)(1, 1) + (1, 2)$. By the Manin conjecture there exists an abelian variety A with $\mathcal{N}(A) = \xi$. We see that A is not supersingular, and that the p-rank $f(A)$ equals zero.

6. Hilbert modular varieties

We discuss Hilbert modular varieties over $\mathbb{F}$ in this section. (Recall that $\mathbb{F}$ is the algebraic closure of $\mathbb{F}_p$.) A Hilbert modular variety attached to a totally real number field F classifies "abelian varieties with real multiplication by $\mathcal{O}_F$". An abelian variety A is said to have "real multiplication by $\mathcal{O}_F$" if $\dim(A) = [F : \mathbb{Q}]$ and there is an embedding $\mathcal{O}_F \hookrightarrow \operatorname{End}(A)$; the terminology "fake elliptic curve" was used by some authors. The moduli space of such objects behaves very much like the modular curve, except that its dimension is equal to $[F : \mathbb{Q}]$. Similar to the modular curve, a Hilbert modular variety attached to a totally real number field F has a family of Hecke correspondences coming from the group $\operatorname{SL}_2(F \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)})$ or $\operatorname{GL}_2(\mathbb{A}_f^{(p)})$ depending on the definition one uses. Hilbert modular varieties are closely related to modular forms for GL_2 over totally real fields and the arithmetic of totally real fields.

Besides their intrinsic interest, Hilbert modular varieties play an essential role in the Hecke orbit problem for Siegel modular varieties. This connection results from a special property of $\mathcal{A}_{g,1,n}$ which is not shared by all modular varieties of PEL type: For every $\mathbb{F}$-point x_0 of $\mathcal{A}_{g,1,n}$, there exists a Hilbert modular variety $\mathcal{M}$ and an isogeny correspondence R on $\mathcal{A}_{g,1,n}$ such that x_0 is contained in the image of $\mathcal{M}$ under the isogeny correspondence R. See 9.10 for a precise formulation, and also the beginning of §8.

References. [**71**], [**22**], [**80**] Chap X, [**23**], [**31**], [**88**].

Let $F_1, \ldots, F_r$ be totally real number fields, and let $E := F_1 \times \cdots \times F_r$. Let $\mathcal{O}_E = \mathcal{O}_{F_1} \times \cdots \times \mathcal{O}_{F_r}$ be the product of the rings of integers of $F_1, \ldots, F_r$. Let $\mathcal{L}_i$ be an invertible $\mathcal{O}_{F_i}$-module, and let $\mathcal{L}$ be the invertible $\mathcal{O}_E$-module $\mathcal{L} = \mathcal{L}_1 \times \cdots \times \mathcal{L}_r$.

Definition 6.1. Notation as above. A *notion of positivity* on an invertible $\mathcal{O}_E$-module $\mathcal{L}$ is a union $\mathcal{L}^+$ of connected components of $\mathcal{L} \otimes_{\mathbb{Q}} \mathbb{R}$ such that $\mathcal{L} \otimes_{\mathbb{Q}} \mathbb{R}$ is the disjoint union of $\mathcal{L}^+$ and $-\mathcal{L}^+$.

Definition 6.2.

    (i) An $\mathcal{O}_E$-linear abelian scheme is a pair $(A \to S, \iota)$, where $A \to S$ is an abelian scheme, and $\iota : \mathcal{O}_E \to \mathrm{End}_S(A)$ is an injective ring homomorphism such that $\iota(1) = \mathrm{Id}_A$. Note that every $\mathcal{O}_E$-linear abelian scheme $(A \to S, \iota)$ as above decomposes as a product $(A_1 \to S, \iota_1) \times \cdots \times (A_r \to S, \iota_r)$. Here (A_i, ι_i) is an $\mathcal{O}_{F_i}$-linear abelian scheme for $i = 1, \ldots, r$, and $A = A_1 \times_S \cdots \times_S A_r$.

    (ii) An $\mathcal{O}_E$-linear abelian scheme $(A \to S, \iota)$ is said to be of HB-type if $\dim(A/S) = \dim_{\mathbb{Q}}(E)$.

    (iii) An $\mathcal{O}_E$-linear polarization of an $\mathcal{O}_E$-linear abelian scheme is a polarization $\lambda : A \to A^t$ such that $\lambda \circ \iota(u) = \iota(u)^t \circ \lambda$ for all $u \in \mathcal{O}_E$.

Exercise 6.3. Suppose that $(A \to S, \iota)$ is an $\mathcal{O}_E$-linear abelian scheme, and

$$(A \to S, \iota) = (A_1 \to S, \iota_1) \times \cdots \times (A_r \to S, \iota_r)$$

as in (i). Show that $(A_1 \to S, \iota_1)$ is an $\mathcal{O}_{F_i}$-linear abelian scheme of HB-type for $i = 1, \ldots, r$.

Exercise 6.4. Show that every $\mathcal{O}_E$-linear abelian variety of HB-type over a field admits an $\mathcal{O}_E$-linear polarization.

Definition 6.5. Let $E_p = \prod_{j=1}^s F_{v_j}$ be a product of finite extension fields F_{v_j} of $\mathbb{Q}_p$. Let $\mathcal{O}_{E_p} = \prod_{j=1}^s \mathcal{O}_{F_{v_j}}$ be the product of the rings of elements in F_{v_j} which are integral over $\mathbb{Z}_p$.

    (i) An $\mathcal{O}_{E_p}$-linear p-divisible group is a pair $(X \to S, \iota)$, where $X \to S$ is a p-divisible group, and $\iota : \mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathrm{End}_S(X)$ is an injective ring homomorphism such that $\iota(1) = \mathrm{Id}_X$. Every $(\mathcal{O}_{E_p})$-linear p-divisible group $(X \to S, \iota)$ decomposes canonically into a product $(X \to S, \iota) = \prod_{j=1}^s (X_j, \iota_j)$, where (X_j, ι_j) is an $\mathcal{O}_{F_{v_j}}$-linear p-divisible group, defined to be the image of the idempotent in $\mathcal{O}_{E_p}$ corresponding to the factor $\mathcal{O}_{F_{v_j}}$ of $\mathcal{O}_{E_p}$.

    (ii) An $\mathcal{O}_{E_p}$-linear p-divisible group $(X \to S, \iota)$ is said to have rank two if in the decomposition $(X \to S, \iota) = \prod_{j=1}^s (X_j, \iota_j)$ in (i) above we have $\mathrm{ht}(X_j/S) = 2\,[F_{v_j} : \mathbb{Q}_p]$ for all $j = 1, \ldots, s$.

    (iii) An $\mathcal{O}_{E_p}$-linear polarization $(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_p)$-linear p-divisible group $(X \to S, \iota)$ is a symmetric isogeny $\lambda : X \to X^t$ such that $\lambda \circ \iota(u) = \iota(u)^t \circ \lambda$ for all $u \in \mathcal{O}_{E_p}$.

    (iv) A rank-two $\mathcal{O}_{E_p}$-linear p-divisible group $(X \to S, \iota)$ is of HB-type if it admits an $\mathcal{O}_{E_p}$-linear polarization.

Exercise 6.6. Show that for every $\mathcal{O}_E$-linear abelian scheme of HB-type $(A \to S, \iota)$, the associated $(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_p)$-linear p-divisible group $(A[p^\infty], \iota[p^\infty])$ is of HB-type.

Definition 6.7. Let $E = F_1 \times \cdots \times F_r$, where $F_1, \ldots, F_r$ are totally real number fields. Let $\mathcal{O}_E = \mathcal{O}_{F_1} \times \cdots \times \mathcal{O}_{F_r}$ be the product of the ring of integers of $F_1, \ldots, F_r$. Let $k \supset \mathbb{F}_p$ be an algebraically closed field as before. Let $n \geq 3$ be an integer such that $(n, p) = 1$. Let $(\mathcal{L}, \mathcal{L}^+)$ be an invertible $\mathcal{O}_E$-module with a notion of positivity. The Hilbert modular variety $\mathcal{M}_{E, \mathcal{L}, \mathcal{L}^+, n}$ over k is a smooth scheme over k of dimension $[E : \mathbb{Q}]$ such that for every k-scheme S the set of S-valued points of $\mathcal{M}_{E, \mathcal{L}, \mathcal{L}^+, n}$ is the set of isomorphism class of 6-tuples $(A \to S, \iota, \mathcal{L}, \mathcal{L}^+, \lambda, \eta)$, where

(i) $(A \to S, \iota)$ is an $\mathcal{O}_E$-linear abelian scheme of HB-type;

(ii) $\lambda : \mathcal{L} \to \operatorname{Hom}_{\mathcal{O}_E}^{\mathrm{sym}}(A, A^t)$ is an $\mathcal{O}_E$-linear homomorphism such that $\lambda(u)$ is an $\mathcal{O}_E$-linear polarization of A for every $u \in \mathcal{L} \cap \mathcal{L}^+$, and the homomorphism $A \otimes_{\mathcal{O}_E} \mathcal{L} \xrightarrow{\sim} A^t$ induced by λ is an isomorphism of abelian schemes.

(iii) η is an $\mathcal{O}_E$-linear level-n structure for $A \to S$, i.e., an $\mathcal{O}_E$-linear isomorphism from the constant group scheme $(\mathcal{O}_E/n\mathcal{O}_E)_S^2$ to $A[n]$.

Remark 6.8. Let $(A \to S, \iota, \lambda, \eta)$ be an $\mathcal{O}_E$-linear abelian scheme with polarization sheaf by $(\mathcal{L}, \mathcal{L}^+)$ and a level-n structure satisfying the condition in (ii) above. Then the $\mathcal{O}_E$-linear polarization λ induces an $\mathcal{O}_E/n\mathcal{O}_E$-linear isomorphism

$$(\mathcal{O}_E/n\mathcal{O}_E) = \bigwedge^2 (\mathcal{O}_E/n\mathcal{O}_E)^2 \xrightarrow{\sim} \mathcal{L}^{-1}\mathcal{D}_E^{-1} \otimes_{\mathbb{Z}} \mu_n$$

over S, where $\mathcal{D}_E$ denotes the invertible $\mathcal{O}_E$-module $\mathcal{D}_{F_1} \times \cdots \times \mathcal{D}_{F_r}$. This isomorphism is a discrete invariant of the quadruple $(A \to S, \iota, \lambda, \eta)$. The above invariant defines a morphism f_n from the Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ to the finite étale scheme $\Xi_{E,\mathcal{L},n}$ over k, where the finite étale k-scheme $\Xi_{E,\mathcal{L},n}$ is defined by $\Xi_{E,\mathcal{L},n} := \underline{\operatorname{Isom}}(\mathcal{O}_E/n\mathcal{O}_E, \mathcal{L}^{-1}\mathcal{D}_E^{-1} \otimes_{\mathbb{Z}} \mu_n)$. Notice that $\Xi_{E,\mathcal{L},n}$ is an $(\mathcal{O}_E/n\mathcal{O}_E)^{\times}$-torsor; it is constant over k because k is algebraically closed. The morphism f_n is faithfully flat.

Although we defined the Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ over an algebraically closed field $k \supset \mathbb{F}_p$, we could have defined it over $\mathbb{F}_p$. Then we should use the étale $(\mathcal{O}_E/n\mathcal{O}_E)^{\times}$-torsor $\Xi_{E,\mathcal{L},n} := \underline{\operatorname{Isom}}(\mathcal{O}_E/n\mathcal{O}_E, \mathcal{L}^{-1}\mathcal{D}_E^{-1} \otimes_{\mathbb{Z}} \mu_n)$ over $\mathbb{F}_p$, and we have a faithfully flat morphism $f_n : \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n} \to \Xi_{E,\mathcal{L},n}$ over $\mathbb{F}_p$.

Remark 6.9.

(i) We have followed [**22**] in the definition of Hilbert modular varieties, except that E is a product of totally real number fields, rather than a totally real number field as in [**22**].

(ii) The product decompositions

$$\mathcal{O}_E = \mathcal{O}_{F_1} \times \cdots \times \mathcal{O}_{F_r} \quad \text{and} \quad (\mathcal{L}, \mathcal{L}^+) = (\mathcal{L}_1, \mathcal{L}_1^+) \times \cdots \times (\mathcal{L}_r, \mathcal{L}_r^+)$$

induce a natural isomorphism

$$\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n} \xrightarrow{\sim} \mathcal{M}_{F_1,\mathcal{L}_1,\mathcal{L}_1^+,n} \times \cdots \times \mathcal{M}_{F_r,\mathcal{L}_r,\mathcal{L}_r^+n}.$$

Remark 6.10. The $\mathcal{O}_E$-linear homomorphism λ in Def. 6.7 should be thought of as specifying a family of $\mathcal{O}_E$-linear polarizations, instead of only one polarization: every element $u \in \mathcal{L} \cap \mathcal{L}^+$ gives a polarization $\lambda(u)$ on $A \to S$. Notice that given a point $x_0 = [(A, \iota, \lambda, \eta)]$ in $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(k)$, there may not exist an $\mathcal{O}_E$-linear principal polarization on A, because that means that the element of the strict ideal class group represented by $(\mathcal{L}, \mathcal{L}^+)$ is trivial. However, every point $[(A, \iota, \lambda, \eta)]$ of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ admits an $\mathcal{O}_E$-linear polarization of degree prime to p, because there exists an element $u \in \mathcal{L}^+$ such that $\operatorname{Card}(\mathcal{L}/\mathcal{O}_E \cdot u)$ is not divisible by p. In [**89**] and [**88**] a version of Hilbert modular varieties was defined by specifying a polarization degree d which is prime to p. The resulting Hilbert modular variety is not necessarily irreducible over $\mathbb{F}$; rather it is a disjoint union of modular varieties of the form $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$.

Theorem 6.11. $\boxed{\text{BB}}$ *Notation as above.*

(i) *The modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ over the algebraically closed field $k \supset \mathbb{F}_p$ is normal and is a local complete intersection. Its dimension is equal to $\dim_{\mathbb{Q}}(E)$.*

(ii) *Every fiber of $f_n : \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n} \to \Xi_{E,\mathcal{L},n}$ is irreducible.*

(iii) *The morphism f_n is smooth outside a closed subscheme of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ of codimension at least two.*

Remark.

(i) See [**22**] for a proof of Theorem 6.11 which uses the arithmetic toroidal compactification constructed in [**71**].

(ii) The modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ is not smooth over k if any one of the totally real fields F_i is ramified above p.

6.12. Hecke orbits on Hilbert modular varieties. Let E, $\mathcal{L}$ and $\mathcal{L}^+$ be as before. Denote by $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}{}^\sim$ the projective system $\left(\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}\right)_n$ of Hilbert modular varieties over $\mathbb{F}$, where n runs through all positive integers such that $n \geq 3$ and $\gcd(n,p) = 1$. It is clear that the profinite group $\mathrm{SL}_2(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}^{\wedge,(p)})$ operates on the tower $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^\sim$, by pre-composing with the $\mathcal{O}_E$-linear level structures. Here $\mathbb{Z}^{\wedge,(p)} = \prod_{\ell \neq p} \mathbb{Z}_\ell$. The transition maps in the projective system are

$$\pi_{mn,n} : \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,mn} \to \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n} \qquad (mn,p) = 1, n \geq 3, m \geq 1 \,.$$

The map $\pi_{mn,n}$ is defined by the following construction. Let

$$[m] : (\mathcal{O}_E/n\mathcal{O}_E)^2 \to (\mathcal{O}_E/mn\mathcal{O}_E)^2$$

be the injection induced by "multiplication by m". Given a point $(A, \iota, \lambda, \eta)$ of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,mn}$, the composition $\eta \circ [m]$ factors through the inclusion $i_{m,n} : A[m] \hookrightarrow A[mn]$ to give a level-n structure η' such that $\eta \circ [m] = i_{m,n} \circ \eta'$.

Let $\Xi_E^\sim$ be the projective system $(\Xi_{E,n})_n$, where n also runs through all positive integers such that $n \geq 3$ and $(n,p) = 1$. The transition maps are defined similarly. The maps $f_n : \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n} \to \Xi_{E,n}$ define a map $f^\sim : \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^\sim \to \Xi_E^\sim$ between projective systems.

It is clear that the profinite group $\mathrm{SL}_2(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}^{\wedge,(p)})$ operates on the right of the tower $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^\sim$, by pre-composing with the $\mathcal{O}_E$-linear level structures. Moreover this action is compatible with the map $f^\sim : \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^\sim \to \Xi_E^\sim$ between projective systems.

The above right action of the compact group $\mathrm{SL}_2(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}^{\wedge,(p)})$ on the projective system $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^\sim$ extends to a right action of $\mathrm{SL}_2(E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)})$ on $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^\sim$. Again this action is compatible with $f^\sim : \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^\sim \to \Xi_E^\sim$. This action can be described as follows. A geometric point of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^\sim$ is a quadruple $(A, \iota_A, \lambda_A, \widetilde{\eta_A})$, where the infinite prime-to-p level structure

$$\widetilde{\eta_A} : \coprod_{\ell \neq p} (\mathcal{O}_E[1/\ell]/\mathcal{O}_E) \xrightarrow{\sim} \coprod_{\ell \neq p} A[\ell^\infty]$$

is induced by a compatible system of level-n structures, n running through integers such that $(n,p) = 1$ and $n \geq 3$. Suppose that we have a $\gamma \in \mathrm{SL}_2(E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)})$, and $m\,\gamma$ belongs to $\mathrm{M}_2(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}^{\wedge,(p)})$, where m is a non-zero integer which is prime to p. Then the image of the point $(A, \iota_A, \lambda_A, \widetilde{\eta_A})$ under γ is a quadruple $(B, \iota_B, \lambda_B, \widetilde{\eta_B})$ such that there exists an $\mathcal{O}_E$-linear prime-to-p isogeny $m\beta : B \to A$ such that the

diagram

$$
\begin{array}{ccc}
\coprod_{\ell \neq p}(\mathcal{O}_E[1/\ell]/\mathcal{O}_E)^2 & \xrightarrow{\ \widetilde{\eta_A}\ } & \coprod_{\ell \neq p} A[\ell^\infty] \\
{\scriptstyle m\gamma}\big\uparrow & & \big\uparrow{\scriptstyle m\beta} \\
\coprod_{\ell \neq p}(\mathcal{O}_E[1/\ell]/\mathcal{O}_E)^2 & \xrightarrow[\ \widetilde{\eta_B}\ ]{} & \coprod_{\ell \neq p} B[\ell^\infty]
\end{array}
$$

commutes. Note that ι_B and λ_B are determined by the requirement that $m\beta$ is an $\mathcal{O}_E$-linear isogeny and $m^{-1} \cdot m\beta$ respects the polarizations λ_A and λ_B. In the above notation, as the point $(A, \iota_A, \lambda_A, \widetilde{\eta_A})$ varies, we get a prime-to-p quasi-isogeny $\beta = m^{-1} \cdot (m\beta)$ attached to γ, between the universal abelian schemes.

On a fixed level $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$, the action of $\mathrm{SL}_2(E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)})$ on the projective system $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^{\sim}$ induces a family of finite étale correspondences, which will be called $\mathrm{SL}_2(E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)})$-Hecke correspondences on $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$, or prime-to-$p$ SL_2-Hecke correspondences for short. Suppose x_0 is a geometric point of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$, and $x^{\sim}$ is point of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}^{\sim}$ lifting x_0. Then the prime-to-p SL_2-Hecke orbit of x_0, denoted $\mathcal{H}_{\mathrm{SL}_2}^{(p)}(x_0)$, is the image in $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ of the orbit $\mathrm{SL}_2(E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)}) \cdot \widetilde{x_0}$. The set $\mathcal{H}_{\mathrm{SL}_2}^{(p)}(x_0)$ is countable.

Theorem 6.13. *Let* $x_0 = [(A_0, \iota_0, \lambda_0, \eta_0)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(k)$ *be a closed point of* $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ *such that* A_0 *is an ordinary abelian scheme. Let* $\Sigma_{E,p} = \{\wp_1, \ldots, \wp_s\}$ *be the set of all prime ideals of* $\mathcal{O}_E$ *containing* p. *Then we have a natural isomorphism*

$$
\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0} \cong \prod_{j=1}^{s} \underline{\mathrm{Hom}}_{\mathbb{Z}_p} \left(\mathrm{T}_p(A_0[\wp_j^\infty]_{\text{ét}}) \otimes_{(\mathcal{O}_E \otimes \mathbb{Z}_p)} \mathrm{T}_p(A_0^t[\wp_j^\infty]_{\text{ét}}), \mathbb{G}_m^\wedge \right) .
$$

In particular, the formal completion of the Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ *at the ordinary point* x_0 *has a natural structure as a* $[E : \mathbb{Q}]$-*dimensional* $(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_p)$-*linear formal torus, non-canonically isomorphic to* $(\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{G}_m^\wedge$.

PROOF. By the Serre-Tate theorem, we have

$$
\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0} \cong \prod_{j=1}^{s} \underline{\mathrm{Hom}}_{\mathcal{O}_E \otimes \mathbb{Z}_p} \left(\mathrm{T}_p(A_0[\wp_j^\infty]_{\text{ét}}), A_0[\wp_j^\infty]_{\text{mult}}^\wedge \right) ,
$$

where $A_0[\wp_j^\infty]_{\text{mult}}^\wedge$ is the formal torus attached to $A_0[\wp_j^\infty]_{\text{mult}}$, or equivalently the formal completion of A_0. The character group of the last formal torus is naturally isomorphic to the p-adic Tate module $\mathrm{T}_p(A_0^t[\wp_j^\infty]_{\text{ét}})$ attached to the maximal étale quotient of $A_0^t[\wp_j^\infty]_{\text{ét}}$. $\qquad\square$

Proposition 6.14. *Notation as in 6.13. Assume that* $k = \mathbb{F}$, *so that*

$$
x_0 = [(A_0, \iota_0, \lambda_0, \eta_0)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(\mathbb{F})
$$

and A_0 *is an ordinary* $\mathcal{O}_E$-*linear abelian variety of HB-type over* $\mathbb{F}$.

(i) *There exist totally imaginary quadratic extensions* K_i *of* F_i, $i = 1, \ldots, r$ *such that*

$$
\mathrm{End}_{\mathcal{O}_E}^0(A_0) \cong K_1 \times \cdots \times K_r =: K .
$$

Moreover, for every prime ideal $\wp_j$ of $\mathcal{O}_E$ containing p, we have

$$\mathrm{End}_{\mathcal{O}_E}(A_0) \otimes_{\mathcal{O}_E} \mathcal{O}_{E_{\wp_j}} \xrightarrow{\sim} \mathrm{End}_{\mathcal{O}_{E_{\wp_j}}}(A_0[\wp_j^\infty]_\mathrm{mult}) \times \mathrm{End}_{\mathcal{O}_{E_{\wp_j}}}(A_0[\wp_j^\infty]_\mathrm{\acute{e}t})$$

$$\cong \mathcal{O}_{E_{\wp_j}} \times \mathcal{O}_{E_{\wp_j}} \xleftarrow{\sim} \mathcal{O}_K \otimes_{\mathcal{O}_E} \mathcal{O}_{E_{\wp_j}} .$$

In particular, the quadratic extension K_i/F_i is split above every place of F_i above p, for all $i = 1, \ldots, r$.

(ii) *Let $\mathrm{H}_{x_0} = \{u \in (\mathcal{O}_E \otimes \mathbb{Z}_p)^\times \mid u \cdot \bar{u} = 1\}$, where $u \mapsto \bar{u}$ denotes the product of the complex conjugations on $K_1, \ldots, K_r$. Then both projections*

$$\mathrm{pr}_1 : \mathrm{H}_{x_0} \to \prod_{\wp \in \Sigma_{E,p}} \left(\mathrm{End}_{\mathcal{O}_{E_\wp}}(A_0[\wp_j^\infty]_\mathrm{mult}) \right)^\times \cong \prod_{\wp \in \Sigma_{E,p}} \mathcal{O}_{E_\wp}^\times$$

and

$$\mathrm{pr}_2 : \mathrm{H}_{x_0} \to \prod_{\wp \in \Sigma_{E,p}} \left(\mathrm{End}_{\mathcal{O}_{E_\wp}}(A_0[\wp^\infty]_\mathrm{\acute{e}t}) \right)^\times \cong \prod_{\wp \in \Sigma_{E,p}} \mathcal{O}_{E_\wp}^\times$$

are isomorphisms. Here $\Sigma_{E,p}$ denotes the set consisting of all prime ideals of $\mathcal{O}_E$ which contain p.

(iii) *The group H_{x_0} operates on the $(\mathcal{O}_E \otimes_\mathbb{Z} \mathbb{Z}_p)$-linear formal torus $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0}$ through the character*

$$\mathrm{H}_{x_0} \ni t \longmapsto \mathrm{pr}_1(t)^2 \in (\mathcal{O}_E \otimes_\mathbb{Z} \mathbb{Z}_p)^\times .$$

(iv) *Notation as in (ii) above. Let Z be a reduced, irreducible closed formal subscheme of the formal scheme $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0}$ which is stable under the natural action of an open subgroup U_{x_0} of H_{x_0} on $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0}$. Then there exists a subset $S \subset \Sigma_{E,p}$ such that*

$$Z = \prod_{\wp \in S} \underline{\mathrm{Hom}}_{\mathbb{Z}_p} \left(\mathrm{T}_p(A_0[\wp^\infty]_\mathrm{\acute{e}t}) \otimes_{(\mathcal{O}_E \otimes \mathbb{Z}_p)} \mathrm{T}_p(A_0^t[\wp^\infty]_\mathrm{\acute{e}t}), \mathbb{G}_m^\wedge \right)$$

PROOF. The statement (i) is a consequence of Tate's theorem on endomorphisms of abelian varieties over a finite field, see [**79**]. The statement (ii) follows from (i). The statement (iii) is immediate from the displayed canonical isomorphism in Theorem 6.13. It remains to prove (iv).

By Theorem 2.26 and Theorem 6.13, we know that Z is a formal subtorus of the formal torus

$$\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0} = \prod_{\wp \in \Sigma_{E,p}} \underline{\mathrm{Hom}}_{\mathbb{Z}_p} \left(\mathrm{T}_p(A_0[\wp^\infty]_\mathrm{\acute{e}t}) \otimes_{(\mathcal{O}_E \otimes \mathbb{Z}_p)} \mathrm{T}_p(A_0^t[\wp^\infty]_\mathrm{\acute{e}t}), \mathbb{G}_m^\wedge \right) .$$

Let $X_*(Z)$ be the group of formal cocharacters of the formal torus Z. We know that $X_*(Z)$ is a $\mathbb{Z}_p$-submodule of the cocharacter group

$$\prod_{\wp \in \Sigma_{E,p}} (\mathrm{T}_p(A_0[\wp^\infty]_\mathrm{\acute{e}t}))^\vee \otimes_{(\mathcal{O}_E \otimes \mathbb{Z}_p)} (\mathrm{T}_p(A_0^t[\wp^\infty]_\mathrm{\acute{e}t}))^\vee$$

of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0}$, which is co-torsion free. Moreover $X_*(Z)$ is stable under the action of H_{x_0}. Denote by $\mathcal{O}$ the closed subring of $\prod_{\wp \in \Sigma_{E,p}} \mathcal{O}_\wp$ generated by the image of the projection pr_1 in (ii). Since the image of H_{x_0} under the projection pr_1 is an open subgroup of $\prod_{\wp \in \Sigma_{E,p}} \mathcal{O}_\wp^\times$, the subring $\mathcal{O}$ of $\prod_{\wp \in \Sigma_{E,p}} \mathcal{O}_\wp$ is an order of

$\prod_{\wp \in \Sigma_{E,p}} \mathcal{O}_\wp$. So $X_*(Z) \otimes \mathbb{Q}$ is stable under the action of $\prod_{\wp \in \Sigma_{E,p}} E_\wp$. It follows that there exists a subset $S \subset \Sigma_{E,p}$ such that $X_*(Z) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is equal to

$$\prod_{\wp \in S} \left(\mathrm{T}_p(A_0[\wp^\infty]_{\text{ét}}) \right)^\vee \otimes_{\mathcal{O}_E \otimes \mathbb{Z}_p} \left(\mathrm{T}_p(A_0^t[\wp^\infty]_{\text{ét}}) \right)^\vee .$$

Since $X_*(Z)$ is a co-torsion free $\mathbb{Z}_p$-submodule of

$$\prod_{\wp \in \Sigma_{E,p}} \left(\mathrm{T}_p(A_0[\wp^\infty]_{\text{ét}}) \right)^\vee \otimes_{(\mathcal{O}_E \otimes \mathbb{Z}_p)} \left(\mathrm{T}_p(A_0^t[\wp^\infty]_{\text{ét}}) \right)^\vee ,$$

we see that $X_*(Z) = \left(\prod_{\wp \in S} \left(\mathrm{T}_p(A_0[\wp^\infty]_{\text{ét}}) \right)^\vee \otimes_{\mathcal{O}_E \otimes \mathbb{Z}_p} \left(\mathrm{T}_p(A_0^t[\wp^\infty]_{\text{ét}}) \right)^\vee \right)$. □

Corollary 6.15. *Let* $x_0 = [(A_0, \iota_0, \lambda_0, \eta_0)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(\mathbb{F})$ *be an ordinary* $\mathbb{F}$-*point of the Hilbert modular variety* $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ *as in* 6.14. *Let* Z *be a reduced closed subscheme of* $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ *such that* $x_0 \in Z(\mathbb{F})$. *Assume that* Z *is stable under all* $\mathrm{SL}_2(\mathbb{A}_f^{(p)})$-*Hecke correspondences on* $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(\mathbb{F})$. *Then there exists a subset* S_{x_0} *of the set* $\Sigma_{E,p}$ *of prime ideals of* $\mathcal{O}_E$ *containing* p *such that*

$$Z^{/x_0} = \prod_{\wp \in S} \underline{\mathrm{Hom}}_{\mathbb{Z}_p} \left(\mathrm{T}_p(A_0[\wp^\infty]_{\text{ét}}) \otimes_{(\mathcal{O}_E \otimes \mathbb{Z}_p)} \mathrm{T}_p(A_0^t[\wp^\infty]_{\text{ét}}), \mathbb{G}_m^\wedge \right) .$$

Here $Z^{/x_0}$ *is the formal completion of* Z *at the closed point* x_0.

PROOF. Notation as in 6.14. Recall that $K = \mathrm{End}^0_{\mathcal{O}_E}(A_0)$. Denote by U_K the unitary group attached to K; U_K is a linear algebraic group over $\mathbb{Q}$ such that $\mathrm{U}_K(\mathbb{Q}) = \{u \in K^\times \mid u \cdot \bar{u} = 1\}$. By 6.14 (i), $\mathrm{U}_K(\mathbb{Q}_p)$ is isomorphic to $(E \otimes \mathbb{Q}_p)^\times$. Denote by $\mathrm{U}_K(\mathbb{Z}_p)$ the compact open subgroup of $\mathrm{U}_K(\mathbb{Q}_p)$ corresponding to the subgroup $(\mathcal{O}_E \otimes \mathbb{Z}_p)^\times \subset (\mathcal{O}_E \otimes \mathbb{Q}_p)^\times$. This group $\mathrm{U}_K(\mathbb{Z}_p)$ is isomorphic to the group H_{x_0} in 6.14 (ii), via the projection to the first factor in the displayed formula in 6.14 (i). We have a natural action of $\mathrm{U}_K(\mathbb{Z}_p)$ on

$$\mathrm{Def}((A_0, \iota_0, \lambda_0)[p^\infty])/\mathbb{F}) \cong \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0}$$

by the definition of the deformation functor $\mathrm{Def}((A_0, \iota_0, \lambda_0)[p^\infty])$.

Denote by $\mathrm{U}_K(\mathbb{Z}_{(p)})$ the subgroup $\mathrm{U}_K(\mathbb{Q}) \cap \mathrm{U}_K(\mathbb{Z}_p)$ of $\mathrm{U}_K(\mathbb{Q})$; in other words $\mathrm{U}_K(\mathbb{Z}_{(p)})$ consisting of all elements $u \in \mathrm{U}_K(\mathbb{Q})$ such that u induces an automorphism of $A_0[p^\infty]$. Since Z is stable under all $\mathrm{SL}_2(\mathbb{A}_f^{(p)})$-Hecke correspondences, the formal completion $Z^{/x_0}$ at x_0 of the subvariety $Z \subset \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0}$ is stable under the natural action of the subgroup $\mathrm{U}_K(\mathbb{Z}_{(p)})$ of $\mathrm{U}_K(\mathbb{Q})$. By the weak approximation theorem for linear algebraic groups (see [**70**], 7.3, Theorem 7.7 on page 415), $\mathrm{U}_K(\mathbb{Z}_{(p)})$ is p-adically dense in $\mathrm{U}_K(\mathbb{Z}_p)$. So $Z^{/x_0} \subset \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}^{/x_0}$ is stable under the action of $\mathrm{U}_K(\mathbb{Z}_p)$ by continuity. We conclude the proof by invoking 6.14 (iii) and (iv). □

Exercise 6.16. Let (A, ι) be an $\mathcal{O}_E$-linear abelian variety of HB-type over a perfect field $K \supset \mathbb{F}_p$. Show that $\mathrm{M}_p((A, \iota)[p^\infty])$ is a free $(\mathcal{O}_E \otimes_\mathbb{Z} \mathbb{Z}_p)$-module of rank two.

Exercise 6.17. Let $x = [(A, \iota, \lambda, \eta)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(k)$ be a geometric point of a Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$, where $k \supset \mathbb{F}_p$ is an algebraically closed field. Assume that $\mathrm{Lie}(A/k)$ is a free $(\mathcal{O}_E \otimes_\mathbb{Z} k)$-module of rank one. Show that $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ is smooth at x over k.

Exercise 6.18. Let $k \supset \mathbb{F}_p$ be an algebraically closed field. Assume that p is unramified in E, i.e., $E \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a product of unramified extension of $\mathbb{Q}_p$. Show that $\mathrm{Lie}(A/k)$ is a free $(\mathcal{O}_E \otimes_{\mathbb{Z}} k)$-module of rank one for every geometric point $[(A, \iota, \lambda, \eta)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(k)$.

Exercise 6.19. Give an example of a geometric point

$$x = [(A, \iota, \lambda, \eta)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(k)$$

such that $\mathrm{Lie}(A/k)$ is not a free $(\mathcal{O}_E \otimes_{\mathbb{Z}} k)$-module of rank one.

7. Deformations of p-divisible groups to $a \leq 1$

Main references: [**20**], [**66**].

In this section we will prove and use the following rather technical result.

Theorem 7.1. $\boxed{\text{Th}}$ (Deformation to $a \leq 1$) *Let X_0 be a p-divisible group over a field K. There exists an integral scheme S, a point $0 \in S(K)$ and a p-divisible group $\mathcal{X} \to S$ such that the fiber $\mathcal{X}_0$ is isomorphic to X_0, and for the generic point $\eta \in S$ we have*

$$\mathcal{N}(X_0) = \mathcal{N}(X_\eta) \quad and \quad a(X_\eta) \leq 1.$$

See [**20**], 5.12 and [**66**], 2.8.

Note that if X_0 is ordinary (i.e., every slope of $\mathcal{N}(X_0)$ is either 1 or 0), there is not much to prove: $a(X_0) = 0 = a(X_\eta)$; if however X_0 is not ordinary, the theorem says something non-trivial and in that case we end with $a(X_\eta) = 1$.

At the end of this section we discuss the quasi-polarized case.

7.2. *In this section we prove* Theorem 7.1 *in case X_0 is simple.* Surprisingly, this is the most difficult step. We will see, in Section 8, that once we have the theorem in this special case, 7.1 and 7.14 will follow without much trouble.

The proof (and the only one we know) of this special case given here is a combination of general theory, and a computation. We start with one of the tools.

Theorem 7.3. $\boxed{\text{BB}}$ (Purity of the Newton polygon stratification) *Let S be an integral scheme, and let $X \to S$ be a p-divisible group. Let $\gamma = \mathcal{N}(X_\eta)$ be the Newton polygon of the generic fiber. Let $S \supset D = S_{\neq \gamma} := \{s \mid \mathcal{N}(A_s) \not\succeq \gamma\}$ (Note that D is closed in S by Grothendieck-Katz.) Then either D is empty or $\mathrm{codim}(D \subset S) = 1$.*

We know two proofs of this theorem, and both proofs are non-trivial. See [**20**], Theorem 4.1. Also see [**82**], th. 6.1; this second proof of purity was analyzed and re-proved [**82**], [**59**], [**83**], [**92**].

When this result was first announced, it was met by disbelief. Why? If you follow the proof by Katz, see [**40**], 2.3.2, you see that $D = S_{\neq \gamma} \subset S$ is given by "many" defining equations. From that point of view "codimension one" seems unlikely. In fact it is not known (to our knowledge) whether there exists a scheme structure on $D = S_{\neq \gamma}$ such that $(D, \mathcal{O}_D) \subset S$ is a Cartier divisor (locally principal) (i.e., locally a complete intersection, or locally a set-theoretic complete intersection).

7.4. Minimal p-divisible groups. We define the p-divisible group $H_{m,n}$ as in [20], 5.3; also see [69]. See also Exercise 4.52 for another description of $H_{m,n}$ when $K \supset \mathbb{F}_{p^{m+n}}$. Let $K \supset \mathbb{F}_p$ be a perfect field. Let M be a free $W(K)$-module of rank $m + n$, with free generators $e_0, \ldots, e_{m+n-1}$. Extend $e_0, \ldots, e_{m+n-1}$ to a family $(e_i)_{i \in \mathbb{Z}}$ of elements of M indexed by $\mathbb{Z}$ by the requirement that $e_{i+m+n} = p \cdot e_i$ for all $i \in \mathbb{Z}$. Define a σ-linear operator $\mathcal{F} : M \to M$ and a σ^{-1}-linear operator $\mathcal{V} : M \to M$ by

$$\mathcal{F} \cdot e_i = e_{i+n}, \quad \mathcal{V} \cdot e_i = e_{i+m} \qquad \forall i \in \mathbb{Z}.$$

This is a Dieudonné module, and the p-divisible group, whose covariant Dieudonné module is M, is denoted $H_{m,n}$.

Remark. We see that $H_{m,n}$ is defined over $\mathbb{F}_p$; for any field L we will write $H_{m,n}$ instead of $H_{m,n} \otimes L$ if no confusion can occur.

Remark. The p-divisible group $H_{m,n}$ is the "minimal p-divisible group" with Newton polygon equal to δ, the isoclinic Newton polygon of height $m + n$ and slope $m/(m + n)$. For properties of minimal p-divisible groups see [69]. Such groups are of importance in understanding various stratifications of $\mathcal{A}_g$.

Remark. Suppose that the perfect field K contains $\mathbb{F}_{p^h}$, where $h := m + n$. Then the p-divisible group $H_{m,n}$ defined above coincides with the one defined in Exercise 4.52; this is clear from 4.52 (3). Moreover $\mathrm{End}^0(H_{m,n})$ is an h^2-dimensional central division algebra over $\mathbb{Q}_p$ with Brauer invariant $m/(m + n)$, and $\mathrm{End}(H_{m,n})$ is the maximal order of $\mathrm{End}^0(H_{m,n})$. See the paragraph after the statement of [20, 5.4], where the opposite sign convention for Brauer invariants is used.

With the sign convention used both here and also in 4.52, that $\mathrm{End}^0(H_{m,n})$ has Brauer invariant $m/(m + n)$ means that there exists an injective $\mathbb{Q}_p$-linear ring homomorphism

$$j \colon \mathrm{frac} W(\mathbb{F}_{p^h}) \longrightarrow \mathrm{End}^0(H_{m,n})$$

and an element $\Phi \in \mathrm{End}^0(H_{m,n})^{\times}$ such that

$$\Phi \cdot j(x) \cdot \Phi^{-1} = j(\sigma(x)) \qquad \forall x \in \mathrm{frac}(W(\mathbb{F}_{p^h}))$$

and

$$\frac{\mathrm{ord}(\Phi)}{\mathrm{ord}(p)} = \frac{m}{h} \pmod{\mathbb{Z}}.$$

Let's compute the Brauer invariant of $\mathrm{End}^0(H_{m,n})$. Let ϕ be the $W(K)$-linear endomorphism of M such that $\phi(e_i) = e_{i+m}$ for all $i = 0, 1, \ldots, h - 1$. Choose and fix an integer c such that $c \cdot n \equiv 1 \pmod{h}$. For every $x \in W(\mathbb{F}_h)$, let $\jmath(x)$ be the $W(K)$-linear endomorphism of M such that

$$\jmath(x) \colon e_i \mapsto \sigma^{ci}(x) \cdot e_i \qquad \forall i = 0, 1, \ldots, h - 1.$$

It is easy to see that ϕ (resp. $\jmath(x)$) commutes with $\mathcal{F}$ and $\mathcal{V}$, hence defines an element $\Phi \in \mathrm{End}(H_{m,n})$ (resp. $j(x) \in \mathrm{End}(H_{m,n})$), and the commutation relation

$$\Phi \circ j(x) = j(\sigma(x)) \circ \Phi \qquad \forall x \in W(\mathbb{F}_{p^h})$$

is satisfied. Because $\phi^h = p^m \cdot \mathrm{Id}_M$, we have $h \cdot \mathrm{ord}(\Phi) = m \cdot \mathrm{ord}(p)$. So the Brauer invariant of $\mathrm{End}^0(H_{m,n})$ is indeed $m/(m+n)$. See 4.52 (5) for an alternative proof, where $\mathrm{End}^0(H_{m,n})$ is identified with the opposite algebra D^{opp} of the central division algebra D over $\mathbb{Q}_p$ with Brauer invariant $n/(m + n)$.

7.5. The simple case, notation. We follow [20], §5, §6. In order to prove 7.1 in case X_0 is simple we fix notations, to be used for the rest of this section. Let $m \geq n > 0$ be relatively prime integers. We will write $r = (m-1)(n-1)/2$. We write δ for the isoclinic Newton polygon with slope $m/(m+n)$ with multiplicity $m+n$.

We want to understand all p-divisible groups isogenous to $H := H_{m,n}$ (m and n will remain fixed).

Lemma 7.6. $\boxed{\text{BB}}$ *Work over a perfect field K. For every $X \sim H$ there is an isogeny $\varphi : H \to X$ of degree p^r.*

A proof of this lemma is not difficult and is left as an Exercise.

7.7. Construction. Consider the functor

$$S \quad \mapsto \quad \{(\varphi, X) \mid \varphi : H \times S \to X, \ \deg(\varphi) = p^r\}.$$

from the category of schemes over $\mathbb{F}_p$ to the category of sets. This functor is representable; denote the representing object by $(T = T_{m,n}, H_T \to \mathcal{G}) \to \mathrm{Spec}(\mathbb{F}_p)$. Note, using the lemma, that for any $X \sim H$ over a perfect field K there exists a point $x \in T(K)$ such that $X \cong \mathcal{G}_x$.

Discussion. The scheme $T = T_{m,n}$ constructed above is closely related to the Rapoport-Zink spaces $\mathcal{M} = \mathcal{M}(H_{m,n})$ in [72], Theorem 2.16, as follows. The formal scheme $\mathcal{M}$ represents a functor on the category Nilp of all $W(\mathbb{F}_p)$-schemes S such that p is locally nilpotent on S; the value $\mathcal{M}(S)$ for an object S in Nilp is the set of isomorphism classes $(X \to S, \rho : H_{m,n} \times_{\mathrm{Spec}(\mathbb{F}_p)} \overline{S} \to X \times_S \overline{S})$, where $X \to S$ is a p-divisible group, $\overline{S} = S \times_{\mathrm{Spec}(W(\mathbb{F}_p))} \mathrm{Spec}(\mathbb{F}_p)$, and ρ is a quasi-isogeny over $\overline{S}$. From the definition of T we get a morphism $f : T \to \mathcal{M}_r \times_{\mathrm{Spec}(W(\mathbb{F}_p))} \mathrm{Spec}(\mathbb{F}_p)$, where $\mathcal{M}_r$ is the open-and-closed formal subscheme whose points (X, ρ) have the property that the degree of the quasi-isogeny ρ is equal to p^r. Let $\overline{\mathcal{M}}_r^{\mathrm{red}}$ be the scheme with the same topological space as $\mathcal{M}_r$ whose structure sheaf is the quotient of $\mathcal{O}_{\mathcal{M}}/(p, \mathcal{I})$ by the nilpotent radical of $\mathcal{O}_{\mathcal{M}}/(p, \mathcal{I})$, where I is a sheaf of definition of the formal scheme $\mathcal{M}$. Let T^{red} be the reduced subscheme underlying T, and let $f^{\mathrm{red}} : T^{\mathrm{red}} \to \overline{\mathcal{M}}_r^{\mathrm{red}}$ be the morphism induced by f. Then Lemma 7.6 and the fact that $\mathrm{End}(H)^0$ is a division algebra imply that $f : T(k) \to \mathcal{M}_r(k)$ is a bijection for any algebraically closed field $k \supset \mathbb{F}_p$, so $f^{\mathrm{red}} : T^{\mathrm{red}} \to \overline{\mathcal{M}}_r^{\mathrm{red}}$ is an isomorphism.

Theorem 7.8. $\boxed{\text{Th}}$ *The scheme T is geometrically irreducible of dimension r over $\mathbb{F}_p$. The set $T(a=1) \subset T$ is open and dense in T.*

See [20], Theorem 5.11. *Note that* 7.1 *follows from this theorem in case $X_0 \sim H_{m,n}$.* We focus on a proof of 7.8.

Remark. Suppose we have proved the case that $X_0 \sim H_{m,n}$. Then by duality we have $X_0^t \sim H_{m,n}^t = H_{n,m}$, and this case follows also. Hence it suffices to consider only the case $m \geq n > 0$.

Notational Remark. In this section we will not consider abelian varieties. The letters A, B, etc. in this section will not be used for abelian varieties. Semi-modules will only be considered in this section and in later sections these letters again will be used for abelian varieties.

Definition 7.9. We say that $A \subset \mathbb{Z}$ is a *semi-module* or more precisely, an (m,n)-semi-module, if

- A is bounded from below, and if
- for every $x \in A$ we have $a + m, a + n \in A$.

We write $A = \{a_1, a_2, \dots\}$ with $a_j < a_{j+1} \ \forall j$. We say that semi-modules A, B are *equivalent* if there exists $t \in \mathbb{Z}$ such that $B = A + t := \{x + t \mid x \in A\}$.

We say that A is *normalized* if:

(1) $A \subset \mathbb{Z}_{\geq 0}$,
(2) $a_1 < \cdots < a_r \leq 2r$,
(3) $A = \{a_1, \dots, a_r\} \cup [2r, \infty)$;
   notation: $[y, \infty) := \mathbb{Z}_{\geq y}$.

Write $A^t = \mathbb{Z}\backslash(2r - 1 - A) = \{y \in \mathbb{Z} \mid 2r - 1 - y \notin A\}$.

Explanation. For a semi-module A the set $\mathbb{Z}\backslash A$ of course is a "$(-m, -n)$-semi-module". Hence $\{y \mid y \notin A\}$ is a semi-module; then normalize.

Example. Write $\langle 0 \rangle$ for the semi-module generated by 0, i.e., consisting of all integers of the form $im + jn$ for $i, j \geq 0$.

Exercise.

(4) Note that $\langle 0 \rangle$ indeed is normalized. Show that $2r - 1 \notin \langle 0 \rangle$.
(5) Show: if A is normalized then A^t is normalized.
(6) $A^{tt} = A$.
(7) For every B there is a unique normalized A such that $A \sim B$.
(8) If A is normalized then: $A = \langle 0 \rangle \iff 0 \in A \iff 2r - 1 \notin A$.

7.10. Construction. *Work over a perfect field. For every $X \sim H_{m,n}$ there exists a semi-module.*

An isogeny $X \to H$ gives an inclusion

$$\mathbb{D}(X) \quad \hookrightarrow \quad \mathbb{D}(H) = M = \bigoplus_{0 \leq i < m+n} W{\cdot}e_i.$$

Write $M^{(i)} = \pi^i{\cdot}M$. Define

$$B \quad := \quad \{j \mid \mathbb{D}(X) \cap M^{(j)} \neq \mathbb{D}(X) \cap M^{(j+1)}\},$$

i.e., B is the set of values where the filtration induced on $\mathbb{D}(X)$ jumps. It is clear that B is a semi-module. Let A be the unique normalized semi-module equivalent to B.

Notation. The normalized semi-module constructed in this way will be called the *type* of X, denoted by $\mathrm{Type}(X)$.

Let A be a normalized semi-module. We denote by $U_A \subset T$ the set where the semi-module A is realized:

$$U_A \quad = \quad \{t \in T \mid \mathrm{Type}(\mathcal{G}_t) = A\}.$$

Proposition 7.11.

(1) $U_A \hookrightarrow T$ *is locally closed,* $T = \bigsqcup_A U_A$.
(2) $A = \langle 0 \rangle \iff a(X) = 1$.
(3) $U_{\langle 0 \rangle}$ *is geometrically irreducible and has dimension* r.
(4) *If* $A \neq \langle 0 \rangle$ *then every component of* U_A *has dimension strictly less than* r.

For a proof see [**20**], the proof on page 233, and 6.5 and 6.15. The argument is not very deep but somewhat involved (combinatorics and studying explicit equations).

7.12. $\boxed{\text{BB}}$ Let Y_0 be any p-divisible group over a field K, of dimension d and let c be the dimension of Y_0^t. The universal deformation space is isomorphic to $\mathrm{Spf}(K[[t_1, \cdots, t_{cd}]])$ and the generic fiber of that universal deformation is ordinary; in this case its Newton polygon ρ has c slopes equal to 1 and d slopes equal to 0. See 2.5. See [**38**], 4.8, [**20**], 5.15.
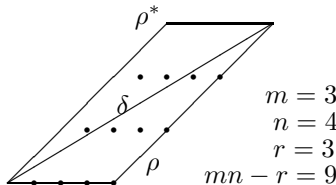
7.13. We prove 7.8, using 7.3 and 7.11. Note that the Zariski closure $(U_{\langle 0 \rangle})^{\mathrm{Zar}} \subset T$ is geometrically irreducible, and has dimension r; we want to show equality $(U_{\langle 0 \rangle})^{\mathrm{Zar}} = T$. Suppose there would be an irreducible component T' of T not contained in $(U_{\langle 0 \rangle})^{\mathrm{Zar}}$. By 7.11 (3) and (4) we see that $\dim(T') < r$. Let $y \in T'$, with corresponding p-divisible group Y_0.

Consider the formal completion $T^{/y}$ of T at y. Write $D = \mathrm{Def}(Y_0)$ for the universal deformation space of Y_0. The moduli map $T^{/y} \to D = \mathrm{Def}(Y_0)$ is an immersion, see [**20**], 5.19. Let $T'' \subset D$ be the image of $(T')^{/y}$ in D; we conclude that no irreducible component of T'' is contained in any irreducible component of the image of $T^{/y} \to D$ in D, i.e., every component of T'' is an component of $\mathcal{W}_\delta(D)$. Clearly $\dim(T') = \dim(T'') < r$.

Obvious, but crucial observation. *Consider the graph of all Newton polygons*

$$\zeta \quad \text{with} \quad \delta \prec \zeta \prec \rho.$$

The longest path in this graph has length $\leq mn - r$.

$$\rho^*$$
$$m = 3$$
$$n = 4$$
$$r = 3$$
$$mn - r = 9$$

PROOF. Consider the Newton polygon ρ, in this case given by n slopes equal to 0 and m slopes equal to 1. Note that $\gcd(m,n) = 1$, hence the Newton polygon δ does not contain integral points except its beginning and end points. Consider the interior of the parallelogram given by ρ and by ρ^*, the upper convex polygon given by: first m slopes equal to 1 and then n slopes equal to 0. The number of interior points of this parallelogram equals $(m-1)(n-1)$. Half of these are above δ, and half of these are below δ. Write $\delta \gneqq (i,j)$ for the property "(i,j) is strictly below δ", and $(i,j) \prec \rho$ for "(i,j) is upon or above ρ". We see:

$$\#\left(\{(i,j) \mid \delta \gneqq (i,j) \prec \rho\}\right) = (m-1)(n-1)/2 + (m+n-1) = mn - r.$$

We use the following fact: If $\zeta_1 \gneqq \zeta_2$, then there is an integral point on ζ_2 strictly below ζ_1. One can even show that all maximal chains of Newton polygons in the fact above have the same length, and in fact equal to

$$\#\left(\{(i,j) \mid \delta \gneqq (i,j) \prec \rho\}\right).$$

This finishes the proof of the claim. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

As $\dim(\mathrm{Def}(Y_0)) = mn$ this observation implies by purity, see 7.3, that every irreducible component of $\mathcal{W}_\delta(D)$ had dimension at least r. This is a contradiction to the assumption of the existence of T', i.e., $\dim(T') = \dim(T'') < r$. Hence $(U_{\langle 0 \rangle})^{\mathrm{Zar}} = T$. This proves Theorem 7.8. Hence we have proved Theorem 7.1 in the case when X_0 is isogenous to $H_{m,n}$. $\qquad\qquad\qquad\qquad\qquad\qquad \square$

Theorem 7.14. ⬚Th⬚ (Deformation to $a \leq 1$ in the principally quasi-polarized case) *Let X_0 be a p-divisible group over a field K with a principal quasi-polarization $\lambda_0 : X_0 \to X_0^t$. There exists an integral scheme S, a point $0 \in S(K)$ and a principally quasi-polarized p-divisible group $(\mathcal{X}, \lambda) \to S$ such that there is an isomorphism $(X_0, \lambda_0) \cong (\mathcal{X}, \lambda)_0$, and for the generic point $\eta \in S$ we have:*

$$\mathcal{N}(X_0) = \mathcal{N}(X_\eta) \quad and \quad a(X_\eta) \leq 1.$$

See [**20**], 5.12 and [**66**], 3.10.

Corollary 7.15. ⬚Th⬚ (Deformation to $a \leq 1$ in the case of principally polarized abelian varieties) *Let (A_0, λ_0) be a principally polarized abelian variety over K. There exists an integral scheme S, a point $0 \in S(K)$ and a principally polarized abelian scheme $(A, \lambda) \to S$ such that there is an isomorphism $(A_0, \lambda_0) \cong (A, \lambda)_0$, and for the generic point $\eta \in S$ we have*

$$\mathcal{N}(A_0) = \mathcal{N}(A_\eta) \quad and \quad a(X_\eta) \leq 1.$$

7.16. The non-principally polarized case. Note that the analog of the theorem and of the corollary is not correct in general in the *non-principally polarized case*. Here is an example, see [**39**], 6.10, and also see [**45**], 12.4 and 12.5 where more examples are given. *Consider $g = 3$, let σ be the supersingular Newton polygon; it can be proved that for any $x \in \mathcal{W}_\sigma(\mathcal{A}_{3,p})$ we have $a(A_x) \geq 2$.*

We will show that for $\xi_1 \prec \xi_2$ we have in the principally polarized case:

$$\mathcal{W}^0_{\xi_1}(\mathcal{A}_{g,1}) =: W^0_{\xi_1} \quad \subset \quad (W^0_{\xi_2})^{\mathrm{Zar}} = W_{\xi_2} := \mathcal{W}_{\xi_2}(\mathcal{A}_{g,1}).$$

In the non-principally polarized case this inclusion and the equality $(W^0_{\xi_2})^{\mathrm{Zar}} = W_{\xi_2}$ do not hold in general as is demonstrated by the following example. Let $g = 3$, and $\xi_1 = \sigma$ the supersingular Newton polygon, and $\xi_2 = (2, 1) + (1, 2)$. Clearly $\xi_1 \prec \xi_2$. By [**39**], 6.10, there is a component of $\mathcal{W}_\sigma(\mathcal{A}_{g,p^2})$ of dimension 3; more generally see [**45**], Theorem 10.5 (ii) for the case of $\mathcal{W}_\sigma(\mathcal{A}_{g,p^{[(g-1)^2/2]}})$ and components of dimension equal to $g(g-1)/2$. As the p-rank 0 locus in $\mathcal{A}_g$ has pure dimension equal to $g(g+1)/2 + (f - g) = g(g-1)/2$, see [**56**], Theorem 4.1, this shows the existence of a polarized supersingular abelian variety (of dimension 3, respectively of any dimension at least 3) which cannot be deformed to a non-supersingular abelian variety with p-rank equal to zero.

Many more examples where $(W^0_\xi)^{\mathrm{Zar}} \neq W_\xi$ follow from [**58**], Section 3.

8. Proof of the Grothendieck conjecture

Main reference: [**66**].

Definition 8.1. ⬚Extra⬚ Let X be a p-divisible group over a base S. A filtration

$$0 = X^{(0)} \subset X^{(1)} \subset \cdots \subset X^{(s)} = X$$

of X by p-divisible subgroups $X_i \to S$ is *the slope filtration* of X if there exists rational numbers $\tau_1, \tau_2, \ldots, \tau_s$ with $1 \geq \tau_1 > \tau_2 > \cdots > \tau_s \geq 0$ such that $Y_i := X^{(i)}/X^{(i-1)}$ is an isoclinic p-divisible group over S with slope τ_i for $i = 1, \ldots, s$.

Remark. Clearly, if a slope filtration exists, it is unique.

From the Dieudonné-Manin classification it follows that the slope filtration on X exists if K is perfect.

By Grothendieck and Zink we know that for every p-divisible group over any field K the slope filtration exists; see [**94**], Corollary 13.

In general for a p-divisible group $X \to S$ over a base a slope filtration on X/S does not exists. Even if the Newton polygon is constant in a family, in general the slope filtration does not exist.

Definition 8.2. We say that $0 = X^{(0)} \subset X^{(1)} \subset \cdots \subset X^{(s)} = X$ is a *maximal filtration* of $X \to S$ if every geometric fiber of $Y^{(i)} := X^{(i)}/X^{(i-1)}$ for $1 \le i \le s$ is *simple* and isoclinic of slope τ_i with $\tau_1 \ge \tau_2 \ge \cdots \ge \tau_s$.

Lemma. $\boxed{\text{BB}}$ *For every X over k a maximal filtration exists.*

See [**66**], 2.2.

Lemma 8.3. $\boxed{\text{BB}}$ *Let $\{X_0^{(i)}\}$ be a p-divisible group X_0 with maximal filtration over k. There exists an integral scheme S and a p-divisible group X/S with a maximal filtration $\{X^{(i)}\} \to S$ and a closed point $0 \in S(k)$ such that $\mathcal{N}(Y^{(i)})$ is constant for $1 \le i \le s$, such that $\{X^{(i)}\}_0 = \{X_0^{(i)}\}$ and such that for the generic point $\eta \in S$ we have $a(X_\eta) \le 1$.*

See [**66**], Section 2. A proof of this lemma uses Theorem 7.8.

In Section 7 we proved 7.8, and obtained as a corollary 7.1 in the case of a simple p-divisible group. From the previous lemma we derive a proof for Theorem 7.1.

Definition 8.4. We say that a p-divisible group X_0 over a field K is a *specialization* of a p-divisible group X_η over a field L if there exists an integral scheme $S \to \mathrm{Spec}(K)$, a k-rational point $0 \in S(K)$, and $\mathcal{X} \to S$ such that $X_0 = \mathcal{X}_0$, and for the generic point $\eta \in S$ we have $L = K(\eta)$ and $X_\eta = \mathcal{X}_\eta$.

This can be used for p-divisible groups, for abelian schemes, etc.

Proposition 8.5. *Let X_0 be a specialization of $X_\eta = Y_0$, and let Y_0 be a specialization of Y_ρ. Then X_0 is a specialization of Y_ρ.*

Using Theorem 5.10 and Theorem 7.1 along with the proposition above, we derive a proof of the Grothendieck Conjecture (Theorem 1.22). $\qquad\square$

Corollary 8.6. (of Theorem 1.22) *Let X_0 be a p-divisible group, $\beta = \mathcal{N}(X_0)$. Every component of the locus $\mathcal{W}_\beta(\mathrm{Def}(X_0))$ has dimension $\diamond(\beta)$.*

Definition 8.7. Let (X, λ) be a principally polarized p-divisible group over S. We say that a filtration

$$0 = X^{(0)} \subset X^{(1)} \subset \cdots \subset X^{(s)} = X$$

of X by p-divisible subgroups $X^{(0)}, \ldots, X^{(s)}$ over S is *a maximal symplectic filtration* of (X, λ) if:

- each quotient $Y^{(i)} := X^{(i)}/X^{(i-1)}$ for $i = 1, \ldots, s$ is a p-divisible group over S,
- every geometric fiber of $Y^{(i)}$ for $1 \le i \le s$ is simple of slope τ_i,
- $\tau_1 \ge \tau_2 \ge \cdots \ge \tau_s$, and
- $\lambda : X \to X^t$ induces an isomorphism

$$\lambda_i : Y^{(i)} \to (Y^{(s+1-i)})^t \quad \text{for} \quad 0 < i \le (s+1)/2.$$

Lemma 8.8. *For every principally polarized (X, λ) over k there exists a maximal symplectic filtration.*

See [**66**], 3.5.

8.9. Using this definition and this lemma, we show the principally polarized analog 7.15 of 7.14; see [**66**], Section 3. Hence Corollary 7.15 follows. Using 7.15 and Theorem 5.19 we derive a proof for:

Theorem 8.10. (An analog of the Grothendieck conjecture) *Let $K \supset \mathbb{F}_p$. Let (X_0, λ_0) be a principally quasi-polarized p-divisible group over K. Write $\mathcal{N}(X_0) = \xi$ for its Newton polygon. Given a Newton polygon ζ "below" ξ, i.e., $\xi \prec \zeta$, there exists a deformation (X_η, λ_η) of (X_0, λ_0) such that $\mathcal{N}(\mathcal{X}_\eta) = \zeta$.*

Corollary 8.11. *Let $K \supset \mathbb{F}_p$. Let (A_0, λ_0) be a principally polarized abelian variety over K. Write $\mathcal{N}(A_0) = \xi$ for its Newton polygon. Given a Newton polygon ζ "below" ξ, i.e., $\xi \prec \zeta$, there exists a deformation (A_η, λ_η) of (A_0, λ_0) such that $\mathcal{N}(\mathcal{X}_\eta) = \zeta$.*

Corollary 8.12. *Let ξ be a symmetric Newton polygon. Every component of the stratum $W_\xi = \mathcal{W}_\xi(\mathcal{A}_{g,1})$ has dimension equal to $\triangle(\xi)$.*

9. Proof of the density of ordinary Hecke orbits

In this section we give a proof of Theorem 1.8 on the density of ordinary Hecke orbits, restated as Theorem 9.1 below. To establish Theorem 1.8, we need the analogous statement for a Hilbert modular variety; see 9.2 for the precise statement.

Here is a list of tools we will use; many have been explained in previous sections.

- (i) Serre-Tate coordinates, see §2.
- (ii) Local stabilizer principle, see 9.5 and 9.6.
- (iii) Local rigidity for group actions on formal tori, see 2.26.
- (iv) Consequence of EO stratification, see 9.7.
- (iv) Hilbert trick, see 9.10.

The logical structure of the proof of Theorem 1.8 is as follows. We first prove the density of ordinary Hecke orbits on Hilbert modular varieties. Then we use the Hilbert trick to show that the Zariski closure of any prime-to-p Hecke orbit on $\mathcal{A}_{g,1,n}$ contains a *hypersymmetric ordinary point*. Finally we use the local stabilizer principle and the local rigidity to conclude the proof of 1.8. Here by a hypersymmetric ordinary point we just mean that the underlying abelian variety is isogenous to $E \times \cdots \times E$, where E is an ordinary elliptic curve over $\mathbb{F}$; see [**15**] for the general notion of hypersymmetric abelian varieties.

The Hilbert trick is based on the following observation. Given an ordinary point $x = [(A_x, \lambda_x, \eta_x)] \in \mathcal{A}_{g,1,n}(\mathbb{F})$, the prime-to-$p$ Hecke orbit of x contains, up to a possibly inseparable isogeny correspondence, the (image of) the prime-to-p Hecke orbit of a point $h = [(A_y, \iota_y, \lambda_y, \eta_y)]$ of a Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$ such that A_y is isogenous to A_x, because $\mathrm{End}^0(A_x)$ contains a product $E = F_1 \times \cdots \times F_r$ of totally real fields with $[E : \mathbb{Q}] = g$. So if we can establish the density of the prime-to-p Hecke orbit of y in $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$, then we know that the Zariski closure of the prime-to-p Hecke orbit of x contains the image of the Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$ in $\mathcal{A}_{g,1,n}$ under a finite isogeny correspondence, i.e., a scheme T over $\mathbb{F}$ and finite $\mathbb{F}$-morphisms $g : T \to \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$ and $f : T \to \mathcal{A}_{g,1,n}$ such that the pullback by g of the universal abelian scheme over $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$ is isogenous to the pullback by f of the universal abelian scheme over $\mathcal{A}_{g,1,n}$. Since $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$

contains ordinary hypersymmetric points, $\left(\mathcal{H}_{\mathrm{Sp}}^{(p)}(x)\right)^{\mathrm{Zar}}$ also contains an ordinary hypersymmetric point. Then the linearization method afforded by the combination of the *local stabilizer principle* and the *local rigidity* implies that the dimension of $\left(\mathcal{H}_{\mathrm{Sp}}^{(p)}(x)\right)^{\mathrm{Zar}}$ is equal to $g(g+1)/2$, hence $\left(\mathcal{H}_{\mathrm{Sp}}^{(p)}(x)\right)^{\mathrm{Zar}} = \mathcal{A}_{g,1,n}$ because $\mathcal{A}_{g,1,n}$ is geometrically irreducible, see 10.26.

To prove the density of ordinary Hecke orbits on a Hilbert modular variety, the linearization method is again crucial. Since a Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$ is "small", there are only a finite number of possibilities as to what (the formal completion of) the Zariski closure of an ordinary Hecke orbit can be; the possibilities are indexed by the set of all subsets of prime ideals of $\mathcal{O}_E$. To pin down the number of possibilities down to one, one can use either the consequence of EO-stratification that the Zariski closure of any Hecke-invariant subvariety of a Hilbert modular variety contains a supersingular point, or de Jong's theorem on extending homomorphisms between p-divisible groups. We follow the first approach here; see 9.11 and [**7**, §8] for the second approach.

Theorem 9.1. *Let $n \geq 3$ be an integer prime to p. Let $x = [(A_x, \lambda_x, \eta_x)] \in \mathcal{A}_{g,1,n}(\mathbb{F})$ such that A_x is ordinary.*

(i) *The prime-to-p $\mathrm{Sp}_{2g}(\mathbb{A}_f^{(p)})$-Hecke orbit of x is dense in the moduli space $\mathcal{A}_{g,1,n}$ over $\mathbb{F}$ for any prime number $\ell \neq p$, i.e.,*

$$\left(\mathcal{H}_{\mathrm{Sp}}^{(p)}(x)\right)^{\mathrm{Zar}} = \mathcal{A}_{g,1,n}.$$

(ii) *The $\mathrm{Sp}_{2g}(\mathbb{Q}_\ell)$-Hecke orbit of x dense in the moduli space $\mathcal{A}_{g,1,n}$ over $\mathbb{F}$, i.e.,*

$$\left(\mathcal{H}_{\ell}^{\mathrm{Sp}}(x)\right)^{\mathrm{Zar}} = \mathcal{A}_{g,1,n}.$$

Theorem 9.2. *Let $n \geq 3$ be an integer prime to p. Let $E = F_1 \times \cdots \times F_r$, where $F_1, \ldots, F_r$ are totally real number fields. Let $\mathcal{L}$ be an invertible $\mathcal{O}_E$-module, and let $\mathcal{L}^+$ be a notion of positivity for $\mathcal{L}$. Let $y = [(A_y, \iota_y, \lambda_y, \eta_y)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(\mathbb{F})$ be a point of the Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ such that A_y is ordinary. Then the $\mathrm{SL}_2(E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)})$-Hecke orbit of y on $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ is Zariski dense in $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ over $\mathbb{F}$.*

Proposition 9.3. *Let $n \geq 3$ be a integer prime to p.*

(i) *Let $x \in \mathcal{A}_{g,1,n}(\mathbb{F})$ be a closed point of $\mathcal{A}_{g,1,n}$. Let $Z(x)$ be the Zariski closure of the prime-to-p Hecke orbit $\mathcal{H}_{\mathrm{Sp}}^{(p)}(x)$ in $\mathcal{A}_{g,1,n}$ over $\mathbb{F}$. Then $Z(x)$ is smooth at x over $\mathbb{F}$.*

(ii) *Let $y \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(\mathbb{F})$ be a closed point of a Hilbert modular variety $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}$. Let $Z_F(y)$ be the Zariski closure of the prime-to-p Hecke orbit $\mathcal{H}_{\mathrm{SL}_2}^{(p)}(y)$ on $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}$ over $\mathbb{F}$. Then $Z_F(y)$ is smooth at y over $\mathbb{F}$.*

PROOF. We give the proof of (ii) here. The proof of (i) is similar and left to the reader.

Because Z_F is reduced, there exists a dense open subset $U \subset Z_F$ which is smooth over $\mathbb{F}$. This open subset U must contain an element y' of the dense subset $\mathcal{H}_{\mathrm{SL}_2}^{(p)}(y)$ of Z_F, so Z_F is smooth over $\mathbb{F}$ at y'. Since prime-to-p Hecke

correspondences are defined by schemes over $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n} \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}$ such that both projections to $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}$ are étale, Z_F is smooth at y as well. $\square$

Remark.

(i) Proposition 9.3 is an analog of the following well-known fact. Let X be a reduced scheme over an algebraically closed field k on which an algebraic group operates transitively. Then X is smooth over k.

(ii) The proof of Proposition 9.3 also shows that all irreducible components of $Z(x)$ (resp. $Z_F(y)$) have the same dimension: For any non-empty subset $U_1 \subset Z_F(y)$ and any open subset $W_1 \ni y$, there exist a non-empty subset $U_2 \subset U_1$, an open subset $W_2 \ni y$ and a non-empty étale correspondence between U_2 and W_2.

Theorem 9.4. $\boxed{\text{BB}}$ *Let Z be a reduced closed subscheme of $\mathcal{A}_{g,1,n}$ over $\mathbb{F}$ such that no maximal point of Z is contained in the supersingular locus of $\mathcal{A}_{g,1,n}$. If Z is stable under all $\mathrm{Sp}_{2g}(\mathbb{Q}_\ell)$-Hecke correspondences on $\mathcal{A}_{g,1,n}$, then Z is stable under all $\mathrm{Sp}_{2g}(\mathbb{A}_f^{(p)})$-Hecke correspondences.*

Remark. This is proved in [**11**, Proposition 4.6].

Local stabilizer principle

Let $k \supset \mathbb{F}_p$ be an algebraically closed field. Let Z be a reduced closed subscheme of $\mathcal{A}_{g,1,n}$ over k. Let $z = [(A_z, \lambda_z, \eta_z)] \in Z(k) \subset \mathcal{A}_{g,1,n}(k)$ be a closed point of Z. Let $*_z$ be the Rosati involution on $\mathrm{End}^0(A_z)$. Denote by H_z the unitary group attached to the semisimple algebra with involution $(\mathrm{End}^0(A_z), *_z)$, defined by

$$\mathrm{H}_z(R) = \left\{ x \in (\mathrm{End}^0(A_z) \otimes_{\mathbb{Q}} R)^\times \mid x \cdot *_0(x) = *_0(x) \cdot x = \mathrm{Id}_{A_z} \right\}$$

for any $\mathbb{Q}$-algebra R. Denote by $\mathrm{H}_z(\mathbb{Z}_p)$ the subgroup of $\mathrm{H}_z(\mathbb{Q}_p)$ consisting of all elements $x \in \mathrm{H}_z(\mathbb{Q}_p)$ such that x induces an automorphism of $(A_z, \lambda_z)[p^\infty]$. Denote by $\mathrm{H}_z(\mathbb{Z}_{(p)})$ the group $\mathrm{H}_z(\mathbb{Q}) \cap \mathrm{H}_z(\mathbb{Z}_p)$, i.e., its elements consist of all elements $x \in \mathrm{H}_z(\mathbb{Q})$ such that x induces an automorphism of $(A_z, \lambda_z)[p^\infty]$. Note that the action of $\mathrm{H}_z(\mathbb{Z}_p)$ on $A_z[p^\infty]$ makes $\mathrm{H}_z(\mathbb{Z}_p)$ a subgroup of $\mathrm{Aut}((A_z, \lambda_z)[p^\infty])$. Denote by $\mathcal{A}_{g,1,n}^{/z}$ (resp. $Z^{/z}$) the formal completion of $\mathcal{A}_{g,1,n}$ (resp. Z) at z. The compact p-adic group $\mathrm{Aut}((A_z, \lambda_z)[p^\infty])$ operates naturally on the deformation space $\mathrm{Def}((A_z, \lambda_z)[p^\infty]/k)$. So we have a natural action of $\mathrm{Aut}((A_z, \lambda_z)[p^\infty])$ on the formal scheme $\mathcal{A}_{g,1,n}^{/z}$ via the canonical isomorphism

$$\mathcal{A}_{g,1,n}^{/z} = \mathrm{Def}((A_z, \lambda_z)/k) \xrightarrow[\sim]{\text{Serre-Tate}} \mathrm{Def}((A_z, \lambda_z)[p^\infty]/k) .$$

Theorem 9.5. (local stabilizer principle) *Notation as above. Suppose that Z is stable under all $\mathrm{Sp}_{2g}(\mathbb{A}_f^{(p)})$-Hecke correspondences on $\mathcal{A}_{g,1,n}$. Then the closed formal subscheme $Z^{/z}$ in $\mathcal{A}_{g,1,n}^{/z}$ is stable under the action of the subgroup $\mathrm{H}_z(\mathbb{Z}_p)$ of $\mathrm{Aut}((A_z, \lambda_z)[p^\infty])$.*

PROOF. Consider the projective system $\mathcal{A}_{g,1}^{\sim} = \varprojlim_m \mathcal{A}_{g,1,m}$ over k, where m runs through all integers $m \geq 1$ which are prime to p. The pro-scheme $\mathcal{A}_{g,1}^{\sim}$ classifies triples $(A \to S, \lambda, \eta)$, where $A \to S$ is an abelian scheme up to prime-to-p isogenies, λ is a principal polarization of $A \to S$, and

$$\eta : \mathrm{H}_1(A_z, \mathbb{A}_f^{(p)}) \xrightarrow{\sim} \underline{\mathrm{H}}_1(A/S, \mathbb{A}_f^{(p)})$$

is a symplectic prime-to-p level structure. Here we have used the first homology groups of A_z attached to the base point z to produce the standard representation of the symplectic group Sp_{2g}. Take $S_z = \mathcal{A}_{g,1,n}^{/z}$, let $(A^{/z}, \lambda^{/z}) \to \mathcal{A}_{g,1,n}^{/z}$ be the restriction of the universal principally polarized abelian scheme to $\mathcal{A}_{g,1,n}^{/z}$, and let $\eta^{/z}$ be the tautological prime-to-p level structure, we get an S_z-point of the tower $\mathcal{A}_{g,1}^{\sim}$ that lifts $S_z \hookrightarrow \mathcal{A}_{g,1,n}$.

Let γ be an element of $\mathrm{H}_z(\mathbb{Z}_{(p)})$. Let γ_p (resp. $\gamma^{(p)}$) be the image of γ in the local stabilizer subgroup $\mathrm{H}_z(\mathbb{Z}_p) \subset \mathrm{Aut}((A_z, \lambda_z)[p^\infty])$ (resp. in $\mathrm{H}_z(\mathbb{A}_f^{(p)})$). From the definition of the action of $\mathrm{Aut}((A_z, \lambda_z)[p^\infty])$ on $\mathcal{A}_{g,1,n}^{/z}$ we have a commutative diagram

$$
\begin{array}{ccc}
(A^{/z}, \lambda^{/z})[p^\infty] & \xrightarrow{f_\gamma[p^\infty]} & (A^{/z}, \lambda^{/z})[p^\infty] \\
\downarrow & & \downarrow \\
\mathcal{A}_{g,1,n}^{/z} & \xrightarrow{u_\gamma} & \mathcal{A}_{g,1,n}^{/z}
\end{array}
$$

where u_γ is the action of γ_p on $\mathcal{A}_{g,1,n}^{/z}$ and $f_\gamma[p^\infty]$ is an isomorphism over u_γ whose fiber over z is equal to γ_p. Since γ_p comes from a prime-to-p quasi-isogeny, $f_\gamma[p^\infty]$ extends to a prime-to-p quasi-isogeny f_γ over u_γ, such that the diagram

$$
\begin{array}{ccc}
A^{/z} & \xrightarrow{f_\gamma} & A^{/z} \\
\downarrow & & \downarrow \\
\mathcal{A}_{g,1,n}^{/z} & \xrightarrow{u_\gamma} & \mathcal{A}_{g,1,n}^{/z}
\end{array}
$$

commutes and f_γ preserves the polarization $\lambda^{/z}$. Clearly the fiber of f_γ at z is equal to γ as a prime-to-p isogeny from A_z to itself. From the definition of the action of the symplectic group $\mathrm{Sp}(\mathrm{H}_1(A_z, \mathbb{A}_f^{(p)}), \langle \cdot, \cdot \rangle)$ one sees that u_γ coincides with the action of $(\gamma^{(p)})^{-1}$ on $\mathcal{A}_{g,1}^{\sim}$. Since Z is stable under all $\mathrm{Sp}_{2g}(\mathbb{A}_f^{(p)})$-Hecke correspondences, we conclude that $Z^{/z}$ is stable under the action of u_γ, for every $\gamma \in \mathrm{H}_z(\mathbb{Z}_{(p)})$.

By the weak approximation theorem for linear algebraic groups (see [**70**], 7.3, Theorem 7.7 on page 415), $\mathrm{H}_z(\mathbb{Z}_{(p)})$ is p-adically dense in $\mathrm{H}_z(\mathbb{Z}_p)$. So $Z^{/z}$ is stable under the action of $\mathrm{H}_z(\mathbb{Z}_p)$ by the continuity of the action of $\mathrm{Aut}((A_z, \lambda_z)[p^\infty])$. $\quad\square$

Remark. The group $\mathrm{H}_z(\mathbb{Z}_{(p)})$ can be thought of as the "stabilizer subgroup" at z inside the family of prime-to-p Hecke correspondences: Every element $\gamma \in \mathrm{H}_z(\mathbb{Z}_{(p)})$ gives rise to a prime-to-p Hecke correspondence with z as a fixed point.

We set up notation for the local stabilizer principle for Hilbert modular varieties. Let $E = F_1 \times \cdots \times F_r$, where $F_1, \ldots, F_r$ are totally real number fields. Let $\mathcal{L}$ be an invertible $\mathcal{O}_E$-module, and let $\mathcal{L}^+$ be a notion of positivity for $\mathcal{L}$. Let $m \geq 3$ be a positive integer which is prime to p. Let Y be a reduced closed subscheme of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$ over $\mathbb{F}$. Let $y = [(A_y, \iota_y, \lambda_y, \eta_y)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}(\mathbb{F})$ be a closed point in $Y \subset \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$. Let $*_y$ be the Rosati involution attached to λ on the semisimple algebra $\mathrm{End}_{\mathcal{O}_E}^0(A_y) = \mathrm{End}_{\mathcal{O}_E}(A_y) \otimes_{\mathcal{O}_E} E$. Denote by H_y the unitary group over $\mathbb{Q}$

attached to $(\mathrm{End}_{\mathcal{O}_E}^0(A_y), *_y)$, so

$$\mathrm{H}_y(R) = \left\{ u \in \left(\mathrm{End}_{\mathcal{O}_E}^0(A_y) \otimes_{\mathbb{Q}} R\right)^\times \mid u \cdot *_y(u) = *_y(u) \cdot u = \mathrm{Id}_{A_y} \right\}$$

for every $\mathbb{Q}$-algebra R. Let $\mathrm{H}_y(\mathbb{Z}_p)$ be the subgroup of $\mathrm{H}_y(\mathbb{Q}_p)$ consisting of all elements of $\mathrm{H}_y(\mathbb{Q}_p)$ which induce an automorphism of $(A_y[p^\infty], \iota_y[p^\infty], \lambda_y[p^\infty])$. Denote by $\mathrm{H}_y(\mathbb{Z}_{(p)})$ the intersection of $\mathrm{H}_y(\mathbb{Q})$ and $\mathrm{H}_y(\mathbb{Z}_p)$ inside $\mathrm{H}_y(\mathbb{Q}_p)$, i.e., it consists of all elements $u \in \mathrm{H}_y(\mathbb{Q})$ such that u induces an automorphism of $(A_y, \iota_y, \lambda_y)[p^\infty]$.

The compact p-adic group $\mathrm{Aut}((A_y, \iota_y, \lambda_y)[p^\infty])$ operates naturally on the local deformation space $\mathrm{Def}((A_y, \iota_y, \lambda_y)[p^\infty]/k)$. So we have a natural action of the compact p-adic group $\mathrm{Aut}((A_y, \iota_y, \lambda_y)[p^\infty])$ on the formal scheme $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}^{/y}$ via the canonical isomorphism

$$\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}^{/y} = \mathrm{Def}((A_y, \iota_y, \lambda_y)/k) \xrightarrow[\sim]{\text{Serre-Tate}} \mathrm{Def}((A_y, \iota_y, \lambda_y)[p^\infty]/k) .$$

Theorem 9.6. *Notation as above. Assume that the closed subscheme*

$$Y \subset \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$$

over $\mathbb{F}$ is stable under all $\mathrm{SL}_2(E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)})$-Hecke correspondences on the Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$. Then the closed formal subscheme $Y^{/y}$ of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}^{/y}$ is stable under the action by elements of the subgroup

$$\mathrm{H}_y(\mathbb{Z}_p) \subset \mathrm{Aut}(A_y[p^\infty], \iota_y[p^\infty], \lambda_y[p^\infty]).$$

PROOF. The proof of Theorem 9.6 is similar to that of Theorem 9.5, and is already contained in the proof of Corollary 6.15. □

Theorem 9.7. $\boxed{\text{BB}}$ *Let $n \geq 3$ be an integer relatively prime to p. Let ℓ be a prime number, $\ell \neq p$.*

    (i) *Every closed subset of $\mathcal{A}_{g,n}$ over $\mathbb{F}$ which is stable under all Hecke correspondences on $\mathcal{A}_{g,n}$ coming from $\mathrm{Sp}_{2g}(\mathbb{Q}_\ell)$ contains a supersingular point.*

    (ii) *Similarly, every closed subset in a Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ over $\mathbb{F}$ which is stable under all $\mathrm{SL}_2(E \otimes \mathbb{Q}_\ell)$-Hecke correspondences on $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ contains a supersingular point.*

Remark. Theorem 9.7 follows from the main theorem of [**67**] and Proposition 9.8 below. See also 3.22.

Proposition 9.8. $\boxed{\text{BB}}$ *Let $k \supset \mathbb{F}_p$ be an algebraically closed field. Let ℓ be a prime number, $\ell \neq p$. Let $n \geq 3$ be an integer prime to p.*

    (i) *Let $x = [(A_x, \lambda_x, \eta_x)] \in \mathcal{A}_{g,1,n}(k)$ be a closed point of $\mathcal{A}_{g,1,n}$. If A_x is supersingular, then the prime-to-p Hecke orbit $\mathcal{H}_{\mathrm{Sp}_{2g}}^{(p)}(x)$ is finite. Conversely, if A_x is not supersingular, then the ℓ-adic Hecke orbit $\mathcal{H}_\ell^{\mathrm{Sp}_{2g}}(x)$ is infinite for every prime number $\ell \neq p$.*

    (ii) *Let $y = [(A_y, \iota_y, \lambda_y, \eta_y)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(k)$ be a closed point of a Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$. If A_y is supersingular, then the prime-to-p Hecke orbit $\mathcal{H}_{\mathrm{SL}_{2,E}}^{(p)}(y)$ is finite. Conversely, if A_y is not supersingular, then the v-adic Hecke orbit $\mathcal{H}_v^{\mathrm{SL}_{2,E}}(y)$ is infinite for every prime ideal $\wp_v$ of $\mathcal{O}_E$ which does not contain p.*

Remark.

(1) The statement (i) is proved in Proposition 1, p. 448 of [**9**], see 1.14. The proof of (ii) is similar. The key to the proof of the second part of (i) is a bijection

$$\mathcal{H}_\ell^{\mathrm{Sp}_{2g}}(x) \xleftarrow{\sim} \left(\mathrm{H}_x(\mathbb{Q}) \cap \prod_{\ell' \neq \ell} K_\ell \right) \backslash \mathrm{Sp}_{2g}(\mathbb{Q}_\ell)/K_\ell$$

where ℓ' runs through all prime numbers not equal to ℓ or p, H_x is the unitary group attached to $(\mathrm{End}^0(A_x), *_x)$ as in Theorem 9.5. The compact groups $K_{\ell'}$ and K_ℓ are defined as follows: for every prime number $\ell' \neq p$, $K_{\ell'} = \mathrm{Sp}_{2g}(\mathbb{Z}_{\ell'})$ if $(\ell', n) = 1$, and $K_{\ell'}$ consists of all elements $u \in \mathrm{Sp}_{2g}(\mathbb{Z}_{\ell'})$ such that $u \equiv 1 \pmod{n}$ if $\ell'|n$. We have an injection $\mathrm{H}_x(\mathbb{A}_f^{(p)}) \to \mathrm{Sp}_{2g}(\mathbb{A}_f^{(p)})$ as in Theorem 9.5, so that the intersection $\mathrm{H}_x(\mathbb{Q}) \cap \prod_{\ell' \neq \ell} K_\ell$ makes sense. The second part of (i) follows from the group-theoretic fact that a double coset as above is finite if and only if H_x is a form of Sp_{2g}.

(2) When the abelian variety A_x in (i) (resp. A_y in (ii)) is ordinary, one can also use the canonical lifting to $W(k)$ to show that $\mathcal{H}_\ell^{\mathrm{Sp}_{2g}}(x)$ (resp. $\mathcal{H}_v^{\mathrm{SL}_2,E}(y)$) is infinite.

The following irreducibility statement is handy for the proof of Theorem 9.2, because it shortens the argument and simplifies the logical structure of the proof.

Theorem 9.9. $\boxed{\mathbf{BB}}$ *Let W be a locally closed subscheme of $\mathcal{M}_{F,n}$ over $\mathbb{F}$ which is smooth over $\mathbb{F}$ and stable under all $\mathrm{SL}_2(F \otimes \mathbb{A}_f^{(p)})$-Hecke correspondences. Assume that the $\mathrm{SL}_2(F \otimes \mathbb{A}_f^{(p)})$-Hecke correspondences operate transitively on the set $\Pi_0(W)$ of irreducible components of W, and some (hence all) maximal point of W corresponds to a non-supersingular abelian variety. Then W is irreducible.*

Remark. The argument in [**11**] works in the situation of 9.9. The following observations may be helpful.

(i) The group $\mathrm{SL}_2(F \otimes \mathbb{A}_f^{(p)})$ has no proper subgroup of finite index. This statement can be verified directly without difficulty. It can also be explained in a more general context: The linear algebraic group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{SL}_2)$ over $\mathbb{Q}$ is semisimple, connected and simply connected. Therefore every subgroup of finite index in $\mathrm{SL}_2(F \otimes \mathbb{Q}_\ell)$ is equal to $\mathrm{SL}_2(F \otimes \mathbb{Q}_\ell)$, for every prime number ℓ.

(ii) The only part of the argument in [**11**] that needs to be supplemented is the end of (4.1), where the fact that Sp_{2g} is simple over $\mathbb{Q}_\ell$ is used. Let G_ℓ be the image group of the ℓ-adic monodromy ρ_Z attached to Z. By definition, G_ℓ is a closed subgroup of $\mathrm{SL}_2(F \otimes \mathbb{Q}_\ell) = \prod_{v|\ell} \mathrm{SL}_2(F_v)$, where v runs through all places of F above ℓ. In the present situation of a Hilbert modular variety $\mathcal{M}_F$, we need to know the fact that the projection of G_ℓ to the factor $\mathrm{SL}_2(F_v)$ is non-trivial for every place v of F above ℓ and for every $\ell \neq p$.

Theorem 9.10. (Hilbert trick) *Given $x_0 \in \mathcal{A}_{g,1,n}(\mathbb{F})$, then there exist*

(a) *totally real number fields $F_1, \ldots, F_r$ such that $\sum_{i=1}^r [E_i : \mathbb{Q}] = g$,*

(b) *an invertible $\mathcal{O}_E$-module $\mathcal{L}$ with a notion of positivity $\mathcal{L}^+$, i.e., $\mathcal{L}^+$ is a union of connected components of $\mathcal{L} \otimes_{\mathbb{Q}} \mathbb{R}$ such that $\mathcal{L} \otimes \mathbb{R}$ is the disjoint union of $\mathcal{L}^+$ with $-\mathcal{L}^+$,*

(c) *a positive integer a and a positive integer m such that $(m, p) = 1$ and $m \equiv 0 \pmod{n}$,*

(d) *a finite flat morphism $g : \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$,*

(e) *a finite morphism $f : \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{A}^{\mathrm{ord}}_{g,n}$,*

(f) *a point $y_0 \in \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}(\mathbb{F})$*

such that the following properties are satisfied.

(i) *There exists a projective system $\mathcal{M}^{\mathrm{ord},\sim}_{E,\mathcal{L},\mathcal{L}^+;a}$ of finite étale coverings of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ on which the group $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$ operates. This action of $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$ induces Hecke correspondences on $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$*

(ii) *The morphism g is equivariant with respect to Hecke correspondences coming from $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$. In other words, there is an $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$-equivariant morphism $g^\sim$ from the projective system $\mathcal{M}^{\mathrm{ord},\sim}_{E,\mathcal{L},\mathcal{L}^+;a}$ to the projective system $\left(\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,md} \right)_{d \in \mathbb{N} - p\mathbb{N}}$ which lifts g.*

(iii) *There exists an injective homomorphism $j_E : \mathrm{SL}_2(E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)}) \to \mathrm{Sp}_{2g}(\mathbb{A}_f^{(p)})$ such that the finite morphism f is Hecke equivariant with respect to j_E.*

(iv) *We have $f(y_0) = x_0$.*

(v) *For every geometric point $z \in \mathcal{M}^{\mathrm{ord}}_{E,m;a}$, the abelian variety underlying the fiber over $g(z) \in \mathcal{M}^{\mathrm{ord}}_{E,m}$ of the universal abelian scheme over $\mathcal{M}^{\mathrm{ord}}_{E,m}$ is isogenous to the abelian variety underlying the fiber over $f(z) \in \mathcal{A}^{\mathrm{ord}}_{g,n}(\mathbb{F})$ of the universal abelian scheme over $\mathcal{A}^{\mathrm{ord}}_{g,n}(\mathbb{F})$.*

Remark. The scheme $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ is defined in Step 3 of the proof of Theorem 9.10.

Lemma. *Let A be an ordinary abelian variety over $\mathbb{F}$ which is simple. Then*

(i) *$K := \mathrm{End}^0(A)$ is a totally imaginary quadratic extension of a totally real number field F;*

(ii) *$[F : \mathbb{Q}] = \dim(A)$;*

(iii) *F is fixed by the Rosati involution attached to any polarization of A;*

(iii) *Every place $\wp$ of F above p splits in K.*

PROOF. The statements (i)–(iv) are immediate consequences of Tate's theorem for abelian varieties over finite fields; see [**79**]. □

Lemma. *Let K be a CM field, let $E := \mathrm{M}_d(K)$, and let $*$ be a positive involution on E which induces the complex conjugation on K. Then there exists a CM field L which contains K and a K-linear ring homomorphism $h : L \to E$ such that $[L : K] = d$ and $h(L)$ is stable under the involution $*$.*

PROOF. This is an exercise in algebra. A proof using Hilbert irreducibility can be found on p. 458 of [**9**]. □

PROOF OF THEOREM 9.10 (HILBERT TRICK).
Step 1. Consider the abelian variety A_0 attached to the given point

$$x_0 = [(A_0, \lambda_0, \eta_0)] \in \mathcal{A}^{\mathrm{ord}}_{g,1,n}(\mathbb{F}).$$

By the two lemmas above there exist totally real number fields $F_1, \ldots, F_r$ and an embedding $\iota_0 : E := F_1 \times \cdots \times F_r \hookrightarrow \mathrm{End}^0(A_0)$ such that E is fixed under the Rosati involution on $\mathrm{End}^0(A_0)$ attached to the principal polarization λ_0, and $[E : \mathbb{Q}] = g = \dim(A_0)$.

The intersection of E with $\mathrm{End}(A_0)$ is an order $\mathcal{O}_1$ of E, so we can regard A_0 as an abelian variety with action by $\mathcal{O}_1$. We claim that there exists an $\mathcal{O}_E$-linear abelian variety B and an $\mathcal{O}_1$-linear isogeny $\alpha : B \to A_0$. This claim follows from a standard "saturation construction" as follows. Let d be the order of the finite abelian group $\mathcal{O}_E / \mathcal{O}_1$. Since A_0 is ordinary, one sees by Tate's theorem (the case when K is a finite field in Theorem 3.16) that $(d, p) = 1$. For every prime divisor $\ell \neq p$ of d, consider the ℓ-adic Tate module $\mathrm{T}_\ell(A_0)$ as a lattice inside the free rank two E-module $\mathrm{V}_\ell(A_0)$. Then the lattice Λ_ℓ generated by $\mathcal{O}_E \cdot \mathrm{T}_\ell(A_0)$ is stable under the action of $\mathcal{O}_E$ by construction. The finite set of lattices $\{\Lambda_\ell : \ell | d\}$ defines an $\mathcal{O}_E$-linear abelian variety B and an $\mathcal{O}_1$-linear isogeny $\beta_0 : A_0 \to B$ which is killed by a power d^i of d. Let $\alpha : B \to A_0$ be the isogeny such that $\alpha \circ \beta_0 = [d^i]_{A_0}$. The claim is proved.

Step 2. The construction in Step 1 gives us a triple (B, α, ι_{x_0}), where B is an abelian variety B over $\mathbb{F}$, $\alpha : B \to A_x$ is an isogeny over $\mathbb{F}$, and $\iota_B : \mathcal{O}_E \to \mathrm{End}(B)$ is an injective ring homomorphism such that $\alpha^{-1} \circ \iota_x(u) \circ \alpha = \iota_B(u)$ for every $u \in \mathcal{O}_E$. Let $\mathcal{L}_B := \mathrm{Hom}^{\mathrm{sym}}_{\mathcal{O}_E}(B, B^t)$ be set of all $\mathcal{O}_E$-linear symmetric homomorphisms from B to the dual B^t of B. The set $\mathcal{L}_B$ has a natural structure as an $\mathcal{O}_E$-module. By Tate's theorem (the case when K is a finite field in Theorem 3.16, see 10.17) one sees that $\mathcal{L}_B$ is an invertible $\mathcal{O}_E$-module, and the natural map

$$\lambda_B : B \otimes_{\mathcal{O}_E} \mathcal{L}_B \to B^t$$

is an $\mathcal{O}_E$-linear isomorphism. The subset of elements in $\mathcal{L}$ which are polarizations defines a notion of positivity $\mathcal{L}^+$ on $\mathcal{L}$ such that $\mathcal{L}_B \cap \mathcal{L}_B^+$ is the subset of $\mathcal{O}_E$-linear polarizations on (B, ι_B).

Step 3. Recall that the Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}_+,n}$ classifies (the isomorphism class of) all quadruples $(A \to S, \iota_A, \lambda_A, \eta_A)$, where $(A \to S, \iota_A)$ is an $\mathcal{O}_E$-linear abelian schemes, $\lambda_A : \mathcal{L} \to \mathrm{Hom}^{\mathrm{sym}}_{\mathcal{O}_E}(A, A^t)$ is an injective $\mathcal{O}_E$-linear map such that the resulting morphism $\mathcal{L} \otimes A \xrightarrow{\sim} A^t$ is an isomorphism of abelian schemes and every element of $\mathcal{L} \cap \mathcal{L}^+$ gives rise to an $\mathcal{O}_E$-linear polarization, and η_A is an $\mathcal{O}_E$-linear level structure on (A, ι_A). In the preceding paragraph, if we choose an $\mathcal{O}_E$-linear level-n structure η_B on (B, ι_B), then $y_1 := [(B, \iota_B, \lambda_B, \eta_B)]$ is an $\mathbb{F}$-point of the Hilbert modular variety $\mathcal{M}_{E,\mathcal{L}_B,\mathcal{L}_B^+,n}$. The element $\alpha^*(\lambda_0)$ is an $\mathcal{O}_E$-linear polarization on B, hence it is equal to $\lambda_B(\mu_0)$ for a unique element $\mu_0 \in \mathcal{L} \cap \mathcal{L}^+$.

Choose a positive integer m_1 with $\gcd(m_1, p) = 1$ and $a \in \mathbb{N}$ such that $\mathrm{Ker}(\alpha)$ is killed by $m_1 p^a$. Let $m = m_1 n$. Let $(A, \iota_A, \lambda_A, \eta_A) \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ be the universal polarized $\mathcal{O}_E$-linear abelian scheme over the ordinary locus $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$. Define a scheme $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ over $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ by

$$\underline{\mathrm{Isom}}^{\mathcal{O}_E}_{\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}} \left((B, \iota_B, \lambda_B)[p^a] \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}, (A, \iota_A, \lambda_A)[p^a] \right).$$

In other words $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ is the moduli space of $\mathcal{O}_E$-linear ordinary abelian varieties with level-mp^a structure, where we have used the $\mathcal{O}_E$-linear polarized truncated p-divisible group $(B, \iota_B, \lambda_B)[p^m]$ as the "model" for the mp^a-torsion subgroup

scheme of the universal abelian scheme over $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$. Let

$$g : \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$$

be the structural morphism of $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$, the source of g being an fppf sheaf of sets on the target of g. Notice that the structural morphism $g : \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ has a natural structure as a torsor over the constant finite flat group scheme

$$\underline{\mathrm{Aut}}\,((B,\iota_B,\lambda_B)[p^a]) \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}\,.$$

We have constructed the finite flat morphism g as promised in Theorem 9.10 (d). We record some properties of this morphism.

The group $\underline{\mathrm{Aut}}\,(B,\iota_B,\lambda_B)[p^a])$ sits in the middle of a short exact sequence

$$0 \to \underline{\mathrm{Hom}}_{\mathcal{O}_E}\,(B[p^a]_{\mathrm{\acute{e}t}}, B[p^a]_{\mathrm{mult}}) \to \underline{\mathrm{Aut}}\,((B,\iota_B,\lambda_B)[p^a]) \to \underline{\mathrm{Aut}}_{\mathcal{O}_E}\,(B[p^a]_{\mathrm{\acute{e}t}}) \to 0\,.$$

The morphism $g : \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ factors as

$$\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \xrightarrow{g_1} \mathcal{M}^{\mathrm{ord,\acute{e}t}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \xrightarrow{g_2} \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}\,,$$

where g_1 is defined as the push-forward by the surjection

$$\underline{\mathrm{Aut}}\,((B,\iota_B,\lambda_B)[p^a]) \twoheadrightarrow \underline{\mathrm{Aut}}_{\mathcal{O}_E}\,(B[p^a]_{\mathrm{\acute{e}t}})$$

of the $\underline{\mathrm{Aut}}\,((B,\iota_B,\lambda_B)[p^a])$-torsor $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$. Note that the morphism g_1 is finite flat and purely inseparable, and $\mathcal{M}^{\mathrm{ord,\acute{e}t}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ is integral. Moreover $\mathcal{M}^{\mathrm{ord,\acute{e}t}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ and $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ are irreducible by [74], [23], [71] and [22].

Step 4. Let $\pi_{n,m} : \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m} \to \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ be the natural projection. Denote by

$$A[mp^a] \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$$

the kernel of $[mp^a]$ on $A \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$, and let $g^*A[mp^a] \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ be the pullback of $A[mp^a] \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ by g. By construction the $\mathcal{O}_E$-linear finite flat group scheme $g^*A[mp^a] \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ is constant via a tautological trivialization

$$\psi : \underline{\mathrm{Aut}}\,(B,\iota_B,\lambda_B)[p^a]) \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m} \xrightarrow{\sim} \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$$

Choose a point $y_0 \in \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}(\mathbb{F})$ such that $(\pi_{n,m} \circ g)(y_0) = y_1$. The fiber over y_0 of $g^*A[mp^a] \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ is naturally identified with $B[mp^a]$. Let $K_0 :=$ $\mathrm{Ker}(\alpha : B \to A_0)$, and let

$$K := \psi\left(K_0 \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}\right)\,,$$

the subgroup scheme of $g^*A[mp^a]$ which corresponds to the constant group K_0 under the trivialization ψ. The element $\mu_0 \in \mathcal{L} \cap \mathcal{L}^+$ defines a polarization on the abelian scheme $g^*A \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$, the pullback by g of the universal polarized $\mathcal{O}_E$-linear abelian scheme over $A \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$. The group K is a maximal totally isotropic subgroup scheme of $g^*\mathrm{Ker}(\lambda_A(\mu_0)) \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$, because $g^*\mathrm{Ker}(\lambda_A(\mu_0))$ is constant and K_0 is a maximal totally isotropic subgroup scheme of $\mathrm{Ker}(\lambda_B(\mu_0))$.

Consider the quotient abelian scheme

$$(A' \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}) := (g^*A \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a})/K.$$

Recall that we have defined an element $\mu_0 \in \mathcal{L} \cap \mathcal{L}^+$ in Step 3. The polarization $g^*(\lambda_A(\mu_0))$ on the abelian scheme $g^*A \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ descends to the quotient abelian scheme $A' \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$, giving it a principal polarization $\lambda_{A'}$. Moreover the n-torsion subgroup scheme $A'[n] \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ is constant, as can be checked easily. Choose a level-n structure $\eta_{A'}$ for A'. The triple $(A', \lambda_{A'}, \eta_{A'})$ over $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ defines a morphism $f : \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{A}^{\mathrm{ord}}_{g,1,n}$ by the modular definition of $\mathcal{A}^{\mathrm{ord}}_{g,1,n}$, since every fiber of $A' \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ is ordinary by construction. We have constructed the morphism f as required in 9.10 (e), and also the point y_0 as required in 9.10 (f).

Step 5. So far we have constructed the morphisms g and f as required in Theorem 9.10. To construct the homomorphism j_E as required in (iii), one uses the first homology group $V := \mathrm{H}_1(B, \mathbb{A}_f^{(p)})$, and the symplectic pairing $\langle \cdot, \cdot \rangle$ induced by the polarization $\alpha^*(\lambda_0) = \lambda_B(\mu_0)$ constructed in Step 3. Notice that V has a natural structure as a free $E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)}$-module of rank two. Also, V is a free $\mathbb{A}_f^{(p)}$-module of rank $2g$. So we get an embedding $j_E : \mathrm{SL}_{E \otimes \mathbb{A}_f^{(p)}}(V) \hookrightarrow \mathrm{Sp}_{\mathbb{A}_f^{(p)}}(V, \langle \cdot, \cdot \rangle)$. We have finished the construction of j_E.

We define $\mathcal{M}^{\mathrm{ord},\sim}_{E,\mathcal{L},\mathcal{L}^+,a}$ to be the projective system $\varprojlim_{md} \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,md;a}$, where d runs through all positive integers which are prime to p. This finishes the last construction needed for Theorem 9.10.

By construction we have $f(y_0) = x_0$, which is statement (iv). The statement (v) is clear by construction. The statements (i)–(iii) can be verified without difficulty from the construction. $\square$

PROOF OF THEOREM 9.2. (Density of ordinary Hecke orbits in $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$)
Reduction step.

From the product decomposition

$$\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n} = \mathcal{M}_{F_1,\mathcal{L}_1,\mathcal{L}_1^+,n} \times_{\mathrm{Spec}(\mathbb{F})} \cdots \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}_{F_r,\mathcal{L}_r,\mathcal{L}_r^+,n}$$

of the Hilbert modular variety $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$, we see that it suffices to prove Theorem 9.2 when $r = 1$, i.e., $E = F_1 =: F$ is a totally real number field. Assume this is the case from now on.

The rest of the proof is divided into four steps.

Step 1. (Serre-Tate coordinates for Hilbert modular varieties)
CLAIM. The Serre-Tate local coordinates at a closed ordinary point $z \in \mathcal{M}^{\mathrm{ord}}_{F,\mathcal{L},\mathcal{L}^+,n}$ of a Hilbert modular variety $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}$ admits a canonical decomposition

$$\mathcal{M}^{/z}_{F,\mathcal{L},\mathcal{L}^+,n} \cong \prod_{\wp \in \Sigma_{F,p}} \mathcal{M}^z_\wp, \qquad \mathcal{M}^z_\wp = \underline{\mathrm{Hom}}_{\mathcal{O}_{F,\wp}} \left(\mathrm{T}_p(A_z[\wp^\infty]_{\mathrm{\acute{e}t}}), \ e_\wp \cdot A_z^{/0} \right),$$

where

- the indexing set $\Sigma_{F,p}$ is the finite set consisting of all prime ideals of $\mathcal{O}_F$ above p,
- the $(\mathcal{O}_F \otimes \mathbb{Z}_p)$-linear formal torus $A_z^{/0}$ is the formal completion of the ordinary abelian variety A_z,
- $e_\wp$ is the irreducible idempotent in $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ so that $e_\wp \cdot (\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ is equal to the factor $\mathcal{O}_{F_\wp}$ of $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Notice that $e_\wp A_z^{/0}$ is the formal torus attached to the multiplicative p-divisible group $A_z[\wp^\infty]_{\text{mult}}$ over $\mathbb{F}$.

PROOF OF CLAIM. The decomposition $\mathcal{O}_F \otimes_\mathbb{Z} \mathbb{Z}_p = \prod_{\wp \in \Sigma_{F,p}} \mathcal{O}_{F_\wp}$ induces a decomposition of the formal scheme $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}^{/z}$ into a product

$$\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}^{/z} = \prod_{\wp \in \Sigma_{F,p}} \mathcal{M}_\wp^z$$

for every closed point z of $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}$: Let $(A/R, \iota)$ be an $\mathcal{O}_F$-linear abelian scheme over an Artinian local ring R. Then we have a decomposition

$$A[p^\infty] = \prod_{\wp \in \Sigma_{F,p}} A[\wp^\infty]$$

of the p-divisible group attached to A, where each $A[\wp^\infty]$ is a deformation of $A \times_{\text{Spec}(R)} \text{Spec}(R/\mathfrak{m})$ over $\text{Spec}(R)$.

If z corresponds to an ordinary abelian variety A_z, then $\mathcal{M}_\wp^z$ is canonically isomorphic to the $\mathcal{O}_{F,\wp}$-linear formal torus $\underline{\text{Hom}}_{\mathcal{O}_{F,\wp}}(A_z[\wp^\infty]_{\text{ét}}, e_\wp \cdot A_z^{/0})$, which is the factor "cut out" in the $(\mathcal{O}_F \otimes_\mathbb{Z} \mathbb{Z}_p)$-linear formal torus

$$\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}^{/z} = \underline{\text{Hom}}_{\mathcal{O}_F \otimes \mathbb{Z}_p}\left(\mathrm{T}_p(A_z[p^\infty]),\ A_z^{/0}\right)$$

by the idempotent $e_\wp$ in $\mathcal{O}_F \otimes \mathbb{Z}_p$. Each factor $\mathcal{M}_\wp^z$ in the above decomposition is a formal torus of dimension $[F_\wp : \mathbb{Q}_p]$, with a natural action by $\mathcal{O}_{F,\wp}^\times$; it is non-canonically isomorphic to the $\mathcal{O}_\wp$-linear formal torus $A_z^{/0}$. □

Step 2. (Linearization)

CLAIM. For every closed point $z \in Z_F^{\text{ord}}(\mathbb{F})$ in the ordinary locus of Z_F, there exists a non-empty subset $S_z \subset \Sigma_{F,p}$ such that $Z_F^{/z} = \prod_{\wp \in S_z} \mathcal{M}_\wp^z$, where $\mathcal{M}_\wp^z$ is the factor of the Serre-Tate formal torus $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}^{/z}$ corresponding to $\wp$.

PROOF OF CLAIM. The $\mathcal{O}_F$-linear abelian variety A_z is an ordinary abelian variety defined over $\mathbb{F}$. Therefore $\text{End}_{\mathcal{O}_F}^0(A_z)$ is a totally imaginary quadratic extension field K of F which is split over every prime ideal $\wp$ of $\mathcal{O}_F$ above p, by Tate's theorem (the case when K is a finite field in Theorem 3.16). By the local stabilizer principle, $Z_F^{/z}$ is stable under the norm-one subgroup U of $(\mathcal{O}_K \otimes_\mathbb{Z} \mathbb{Z}_p)^\times$. Since every prime $\wp$ of $\mathcal{O}_F$ above p splits in $\mathcal{O}_K$, U is isomorphic to $\prod_{\wp \in \Sigma_{F,p}} \mathcal{O}_{F,\wp}^\times$ through its action on the $(\mathcal{O}_F \otimes \mathbb{Z}_p)$-linear formal torus $A_z^{/0}$. The factor $\mathcal{O}_{F,\wp}^\times$ of U operates on the $\mathcal{O}_{F,\wp}$-linear formal torus $\mathcal{M}_\wp^z$ through the character $t \mapsto t^2$, i.e., a typical element $t \in U = \prod_{\wp \in \Sigma_{F,p}} \mathcal{O}_{F,\wp}^\times$ operates on the $(\mathcal{O}_F \otimes \mathbb{Z}_p)$-linear formal torus $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}^{/z}$ through the element $t^2 \in U = (\mathcal{O}_F \otimes \mathbb{Z}_p)^\times$. The last assertion can be seen through the formula

$$\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}^{/z} = \underline{\text{Hom}}_{\mathcal{O}_F \otimes \mathbb{Z}_p}\left(\mathrm{T}_p(A_z[p^\infty]_{\text{ét}}),\ A_z^{/0}\right),$$

because any element t of $U \xrightarrow{\sim} \mathcal{O}_F \otimes_\mathbb{Z} \mathbb{Z}_p$ operates via t (resp. t^{-1}) on the $(\mathcal{O}_F \otimes \mathbb{Z}_p)$-linear formal torus $e_\wp A_z^{/0}$ (resp. the $(\mathcal{O}_F \otimes \mathbb{Z}_p)$-linear p-divisible group $A_z[p^\infty]_{\text{ét}}$).

The local rigidity theorem 2.26 implies that $Z_F^{/z}$ is a formal subtorus of the Serre-Tate formal torus $\mathcal{M}_F^{/z}$. For every $\wp \in \Sigma_{F,p}$, let $X_{\wp,*}$ be the cocharacter group of the $\mathcal{O}_{F_\wp}$-linear formal torus $\mathcal{M}_\wp^z$, so that $\prod_{\wp \in \Sigma_{F,p}} X_{\wp,*}$ is the cocharacter group of the Serre-Tate formal torus $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}^{/z}$. Let Y_* be the cocharacter group

of the formal torus $Z_F^{/z}$. We know that Y_* is a co-torsion free $\mathbb{Z}_p$-submodule of the rank-one free $\left(\prod_{\wp \in \Sigma_{F,p}} \mathcal{O}_{F,\wp}\right)$-module $\prod_{\wp \in \Sigma_{F,p}} X_{\wp,*}$, and Y_* is stable under multiplication by elements of the subgroup $\prod_{\wp \in \Sigma_{F,p}} (\mathcal{O}_{F,\wp}^\times)^2$ of $\prod_{\wp \in \Sigma_{F,p}} \mathcal{O}_{F,\wp}^\times$. It is easy to see that the additive subgroup generated by $\prod_{\wp \Sigma_{F,p}} (\mathcal{O}_{F,\wp}^\times)^2$ is equal to $\prod_{\wp \in \Sigma_{F,p}} \mathcal{O}_{F,\wp}$, i.e., Y_* is a $\left(\prod_{\wp \in \Sigma_{F,p}} \mathcal{O}_{F,\wp}\right)$-submodule of $\prod_\wp X_{\wp,*}$. Hence there exists a subset $S_z \subseteq \Sigma_{F,p}$ such that $Y_* = \prod_{\wp \in S_z} X_{\wp,*}$. Since the prime-to-$p$ Hecke orbit $\mathcal{H}_{\mathrm{SL}_{2,F}}^{(p)}(x)$ is infinite by 9.8, we have $0 < \dim(Z_F) = \sum_{\wp \in S_z} [F_\wp : \mathbb{Q}_p]$, hence $S_z \neq \emptyset$ for every ordinary point $z \in Z_F(x)(\mathbb{F})$. We have proved the Claim in Step 2. □

Step 3. (Globalization)

CLAIM. The finite set S_z is independent of the point z, i.e., there exists a subset $S \subset \Sigma_{F,p}$ such that $S_z = \Sigma_{F,p}$ for all $z \in Z_F^{\mathrm{ord}}(\mathbb{F})$.

PROOF OF CLAIM. Consider the diagonal embedding $\Delta_Z : Z_F \to Z_F \times_{\mathrm{Spec}(\mathbb{F})} Z_F$, the diagonal embedding $\Delta_{\mathcal{M}} : \mathcal{M}_{F,n} \to \mathcal{M}_{F,n} \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}_{F,n}$, and the map $\Delta_{Z,\mathcal{M}}$ from Δ_Z to $\Delta_{\mathcal{M}}$ induced by the inclusion $Z_F \hookrightarrow \Delta_{\mathcal{M}}$. Let $\mathcal{P}_Z$ be the formal completion of $Z_F \times_{\mathrm{Spec}(\mathbb{F})} Z_F$ along $\Delta_Z(Z_F)$, and let $\mathcal{P}_{\mathcal{M}}$ be the formal completion of $\mathcal{M}_{F,n} \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}_{F,n}$ along $\Delta_{\mathcal{M}}(\mathcal{M}_{F,n})$. The map $\Delta_{Z,\mathcal{M}}$ induces a closed embedding $i_{Z,\mathcal{M}} : \mathcal{P}_Z \hookrightarrow \mathcal{P}_{\mathcal{M}}$. We regard $\mathcal{P}_Z$ (resp. $\mathcal{P}_{\mathcal{M}}$) as a formal scheme over Z_F (resp. $\mathcal{M}_{F,n}$) via the first projection.

The decomposition $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p = \prod_{\wp \in \Sigma_{F,p}} \mathcal{O}_{F,\wp}$ induces a fiber product decomposition

$$\mathcal{P}_{\mathcal{M}} = \prod_{\wp \in \Sigma_{F,p}} (\mathcal{P}_\wp \to \mathcal{M}_{F,n})$$

over the base scheme $\mathcal{M}_{F,n}$, where $\mathcal{P}_\wp \to \mathcal{M}_{F,n}$ is a smooth formal scheme of relative dimension $[F_\wp : \mathbb{Q}_p]$ with a natural section $\delta_\wp$, for every $\wp \in \Sigma_{F,p}$, and the formal completion of the fiber of $(\mathcal{M}_\wp, \delta_\wp)$ over any closed point z of the base scheme $\mathcal{M}_{F,n}$ is canonically isomorphic to the formal torus $\mathcal{M}_\wp^z$. In fact one can show that $\mathcal{M}_\wp \to \mathcal{M}_{F,n}$ has a natural structure as a formal torus of relative dimension $[F_\wp : \mathbb{Q}_p]$, with $\delta_\wp$ as the zero section; we will not need this fact here. Notice that $\mathcal{P}_Z \to Z_F$ is a closed formal subscheme of $\mathcal{P}_{\mathcal{M}} \times_{\mathcal{M}_{F,n}} Z_F \to Z_F$. The above consideration globalizes the "pointwise" construction of formal completions at closed points.

By Proposition 9.9, Z_F is irreducible. We conclude from the irreducibility of Z_F that there is a non-empty subset $S \subset \Sigma_{F,p}$ such that the restriction of $\mathcal{P}_Z \to Z_F$ to the ordinary locus Z_F^{ord} is equal to the fiber product over Z_F^{ord} of formal schemes $\mathcal{P}_\wp \times_{\mathcal{M}_{F,n}} Z_F^{\mathrm{ord}} \to Z_F^{\mathrm{ord}}$ over Z_F^{ord}, where $\wp$ runs through the subset $S \subseteq \Sigma_{F,p}$. We have proved the Claim in Step 3. □

Remark.

(i) Without using Proposition 9.9, the above argument shows that for each irreducible component Z_1 of Z_F^{ord}, there exists a subset $S \subset \Sigma_{F,p}$ such that $S_z = S$ for every closed point $z \in Z_1(\mathbb{F})$.

(ii) There is an alternative proof of the claim that S_z is independent of z: By Step 2, Z_F^{ord} is smooth over $\mathbb{F}$. Consider the relative cotangent sheaf $\Omega^1_{Z_F^{\mathrm{ord}}/\mathbb{F}}$, which is a locally free $\mathcal{O}_{Z_F^{\mathrm{ord}}}$-module. We recall that $\Omega^1_{\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}^{\mathrm{ord}}/\mathbb{F}}$

has a natural structure as a $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{F}_p$-module, from the Serre-Tate coordinates explained in Step 1. By Step 2, we have

$$\Omega^1_{Z_F^{\mathrm{ord}}/\mathbb{F}} \otimes_{\mathcal{O}_{Z_F,z}} \mathcal{O}^{\wedge}_{Z_F,z} = \sum_{\wp \in S_z} e_\wp \cdot \Omega^1_{\mathcal{M}^{\mathrm{ord}}_{F,\mathcal{L},\mathcal{L}^+,n}/\mathbb{F}} \otimes_{\mathcal{O}_{\mathcal{M}^{\mathrm{ord}}_{F,\mathcal{L},\mathcal{L}^+,n}}} \mathcal{O}^{\wedge}_{Z_F,z}$$

for every $z \in Z_F^{\mathrm{ord}}(\mathbb{F})$, where $\mathcal{O}^{\wedge}_{Z_F,z}$ is the formal completion of the local ring of Z_F at z. Therefore for each irreducible component Z_1 of Z_F^{ord} there exists a subset $S \subset \Sigma_{F,p}$ such that

$$\Omega^1_{Z_1/\mathbb{F}} = \sum_{\wp \in S} e_\wp \cdot \Omega^1_{\mathcal{M}^{\mathrm{ord}}_{F,\mathcal{L},\mathcal{L}^+,n}/\mathbb{F}} \otimes_{\mathcal{O}_{\mathcal{M}^{\mathrm{ord}}_{F,\mathcal{L},\mathcal{L}^+,n}}} \mathcal{O}_{Z_1/\mathbb{F}}\,.$$

Hence $S_z = S$ for every $z \in Z_1(\mathbb{F})$. This argument was used in [**9**]; see Proposition 5 on p. 473 in *loc. cit.*

(iii) One advantage of the globalization argument in Step 3 is that it makes the final Step 4 of the proof of Theorem 9.2 easier, as compared with the two-page proof of Proposition 7 on p. 474 of [**9**].

Step 4. We have $S = \Sigma_{F,p}$. Therefore $Z_F = \mathcal{M}_{F,n}$.

PROOF OF STEP 4.

Notation as in Step 3 above. For every closed point s of Z_F, the formal completion $Z_F^{/s}$ contains the product $\prod_{\wp \in S} \mathcal{M}^s_\wp$. By Theorem 9.7, Z_F contains a supersingular point s_0. Consider the formal completion $Z^{\wedge} := Z_F^{/s_0}$, which contains $W^{\wedge} := \prod_{\wp \in S} \mathcal{M}^{s_0}_\wp$, and the generic point $\eta_{W^{\wedge}}$ of $\mathrm{Spec}\left(\mathrm{H}^0(W^{\wedge}, \mathcal{O}_{W^{\wedge}})\right)$ is a maximal point of $\mathrm{Spec}\left(\mathrm{H}^0(Z^{\wedge}, \mathcal{O}_{Z^{\wedge}})\right)$. The restriction of the universal abelian scheme to $\eta_{W^{\wedge}}$ is an ordinary abelian variety. Hence $S = \Sigma_{F,p}$, otherwise $A_{\eta_{W^{\wedge}}}$ has slope $1/2$ with multiplicity at least $2 \sum_{\wp \notin S}[F_\wp : \mathbb{Q}_p]$. Theorem 9.2 is proved. $\square$

Remark. The proof of Theorem 9.2 can be finished without using Proposition 9.9 as follows. We saw in the Remark after Step 3 that S_z depends only on the irreducible component of Z_F^{ord} which contains z. The argument in Step 4 shows that at least the subset $S \subset \Sigma_{F,p}$ attached to one irreducible component Z_1 of Z_F^{ord} is equal to $\Sigma_{F,p}$. So $\dim(Z_1) = \dim(\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}) = [F : \mathbb{Q}]$. Since $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}$ is irreducible, we conclude that $Z_F = \mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}$.

PROOF OF THEOREM 9.1. (Density of ordinary Hecke orbits in $\mathcal{A}_{g,1,n}$.)

REDUCTION STEP. By Theorem 9.4, the weaker statement 9.1 (i) implies 9.1 (ii). So it suffices to prove 9.1 (i).

Remark. Our argument can be used to prove (ii) directly without appealing to Theorem 9.4. But some statements, including the local stabilizer principal for Hilbert modular varieties, need to be modified.

Step 1. (Hilbert trick)

Given $x \in \mathcal{A}_{g,n}(\mathbb{F})$, Apply Theorem 9.10 to produce a finite flat morphism

$$g : \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}\,,$$

where E is a product of totally real number fields, a finite morphism

$$f : \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{A}_{g,n}\,,$$

and a point $y_0 \in \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}(\mathbb{F})$ such that the following properties are satisfied.

(i) There exists a projective system $\mathcal{M}^{\mathrm{ord},\sim}_{E,\mathcal{L},\mathcal{L}^+;a}$ of finite étale coverings of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ on which the group $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$ operates. This action of $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$ induces Hecke correspondences on $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$

(ii) The morphism g is equivariant with respect to Hecke correspondences coming from $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$. In other words, there is a $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$-equivariant morphism $g^\sim$ from the projective system $\mathcal{M}^{\mathrm{ord},\sim}_{E,\mathcal{L},\mathcal{L}^+,a}$ to the projective system $\left(\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,mn}\right)_{n \in \mathbb{N}-p\mathbb{N}}$ which lifts g.

(iii) The finite morphism f is Hecke equivariant with respect to an injective homomorphism
$$j_E : \mathrm{SL}_2(E \otimes_\mathbb{Q} \mathbb{A}_f^{(p)}) \to \mathrm{Sp}_{2g}(\mathbb{A}_f^{(p)}) \,.$$

(iv) For every geometric point $z \in \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$, the abelian variety underlying the fiber over $g(z) \in \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ of the universal abelian scheme over $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ is isogenous to the abelian variety underlying the fiber over $f(z) \in \mathcal{A}^{\mathrm{ord}}_{g,n}(\mathbb{F})$ of the universal abelian scheme over $\mathcal{A}^{\mathrm{ord}}_{g,n}(\mathbb{F})$.

(v) We have $f(y_0) = x_0$.

Let $y := g(y_0) \in \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$.

Step 2. Let Z_{y_0} be the Zariski closure of the $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$-Hecke orbit of y_0 on $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$, and let Z_y be the Zariski closure of the $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$-Hecke orbit on $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$. By Theorem 9.2 we know that $Z_y = \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$. Since g is finite flat, we conclude that $g(Z_{y_0}) = Z_y \cap \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m} = \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$. We know that $f(Z_{y_0}) \subset Z_x$ because f is Hecke-equivariant.

Step 3. Let E_1 be an ordinary elliptic curve over $\mathbb{F}$. Let y_1 be an $\mathbb{F}$-point of $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$ such that A_{y_1} is isogenous to $E_1 \otimes_\mathbb{Z} \mathcal{O}_E$ and $\mathcal{L}_{y_1}$ contains an $\mathcal{O}_E$-submodule of finite index in $\lambda_{E_1} \otimes \mathcal{O}_E$, where λ_{E_1} denotes the canonical principal polarization on E_1. In the above the tensor product $E_1 \otimes_\mathbb{Z} \mathcal{O}_E$ is taken in the category of fppf sheaves over $\mathbb{F}$; the tensor product is represented by an abelian variety isomorphic to the product of g copies of E_1, with an action by $\mathcal{O}_E$. It is not difficult to check that such a point y_1 exists.

Let z_1 be a point of Z_{y_0} such that $g(z_1) = y_1$. Such a point y_1 exists because $g(Z_{y_0}) = \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}$ The point $x_1 = f(z_1)$ is contained in the Zariski closure $Z(x)$ of the prime-to-p Hecke orbit of x on $\mathcal{A}_{g,n}$. Moreover A_{x_1} is isogenous to the product of g copies of E_1 by property (iv) in Step 1. So $\mathrm{End}^0(A_{x_1}) \cong \mathrm{M}_g(K)$, where $K = \mathrm{End}^0(E)$ is an imaginary quadratic extension field of $\mathbb{Q}$ which is split above p. The local stabilizer principle says that $Z(x)^{/x_1}$ is stable under the natural action of an open subgroup of $\mathrm{SU}(\mathrm{End}^0(A_{x_1}), \lambda_{x_1})(\mathbb{Q}_p) \cong \mathrm{GL}_g(\mathbb{Q}_p)$.

Step 4. We know that $Z(x)$ is smooth at the ordinary point x over k, so $Z(x)^{/x}$ is reduced and irreducible. By the local stabilizer principle 9.5, $Z(x)^{/x}$ is stable under the natural action of the open subgroup H_x of $\mathrm{SU}(\mathrm{End}^0(A_{x_1}), *_{x_1})$ consisting of all elements $\gamma \in \mathrm{SU}(\mathrm{End}^0(A_{x_1}), *_{x_1})(\mathbb{Q}_p)$ such that $\gamma(A_{x_1}[p^\infty]) = A_{x_1}[p^\infty]$. By Theorem 2.26, $Z(x)^{/x_1}$ is a formal subtorus of the formal torus $\mathcal{A}^{/x_1}_{g,n}$, which is stable under the action of an open subgroup of $\mathrm{SU}(\mathrm{End}^0(A_{x_1}, \lambda_{x_1}))(\mathbb{Q}_p) \cong \mathrm{GL}_g(\mathbb{Q}_p)$.

Let X_* be the cocharacter group of the Serre-Tate formal torus $\mathcal{A}_{g,n}^{/x_1}$, and let Y_* be the cocharacter group of the formal subtorus $Z(x)^{/x_1}$. Both X_* and X_*/Y_* are free $\mathbb{Z}_p$-modules. It is easy to see that the restriction to $\mathrm{SL}_g(\mathbb{Q}_p)$ of the linear action of $\mathrm{SU}(\mathrm{End}^0(A_{x_1}), *_{x_1})(\mathbb{Q}_p) \cong \mathrm{GL}_g(\mathbb{Q}_p)$ on $X_* \otimes_{\mathbb{Z}} \mathbb{Q}_p$ is isomorphic to the second symmetric product of the standard representation of $\mathrm{SL}_g(\mathbb{Q}_p)$. It is well-known that the latter is an absolutely irreducible representation of $\mathrm{SL}_g(\mathbb{Q}_p)$. Since the prime-to-$p$ Hecke orbit of x is infinite, $Y_* \neq (0)$, hence $Y_* = X_*$. In other words $Z(x)^{/x_1} = \mathcal{A}_{g,n}^{/x_1}$. Hence $Z(x) = \mathcal{A}_{g,n}$ because $\mathcal{A}_{g,n}$ is irreducible. $\square$

Remark 9.11. We mentioned at the beginning of this section that there is an alternative argument for Step 4 of the proof of Theorem 9.2, which uses [**19**] instead of Theorem 9.7, and therefore is independent of [**67**]. We sketch the idea here; see §8 of [**7**] for more details.

We keep the notation in Step 3 of the proof of 9.2. Assume that $S \neq \Sigma_{F,p}$. Consider the universal $\mathcal{O}_F$-linear abelian scheme $(A \to Z_F^{\mathrm{ord}}, \iota)$ and the $(\mathcal{O}_F \otimes \mathbb{Z}_p)$-linear p-divisible group $(A \to Z_F^{\mathrm{ord}}, \iota)[p^\infty]$ over the base scheme Z_F^{ord}, which is smooth over $\mathbb{F}$. We have a canonical decomposition of $X_\wp := A[p^\infty] \to Z_F^{\mathrm{ord}}$ as the fiber product over Z_F^{ord} of $\mathcal{O}_\wp$-linear p-divisible groups $A[\wp^\infty] \to Z_F^{\mathrm{ord}}$, where $\wp$ runs through the finite set $\Sigma_{F,p}$ of all places of F above p. Let $X_1 \to Z_F^{\mathrm{ord}}$ (resp. $X_2 \to Z_F^{\mathrm{ord}}$) be the fiber product over Z_F^{ord} of those $X_\wp$'s with $\wp \in S$ (resp. with $\wp \notin S$), so that we have $A[p^\infty] = X_1 \times_{Z_F^{\mathrm{ord}}} X_2$.

We know that for every closed point s of Z_F^{ord}, the restriction to the formal completion $Z_F^{/s}$ of the $\left(\prod_{\wp \notin S} \mathcal{O}_\wp\right)$-linear p-divisible group $X_2 \to Z_F^{\mathrm{ord}}$ is constant. This means that $X_2 \to Z_F^{\mathrm{ord}}$ is the twist of a constant $\left(\prod_{\wp \notin S} \mathcal{O}_\wp\right)$-linear p-divisible group by a character

$$\chi : \pi_1^{\text{ét}}(Z_F^{\mathrm{ord}}) \to \prod_{\wp \notin S} \mathcal{O}_\wp^\times.$$

More precisely, one twists the étale part and toric part of the constant p-divisible group by χ and χ^{-1} respectively. Consequently $\mathrm{End}_{\prod_{\wp \notin S} \mathcal{O}_\wp}(X_2) \supseteq \prod_{\wp \notin S}(\mathcal{O}_\wp \times \mathcal{O}_\wp)$.

By the main results in [**19**], we have an isomorphism

$$\mathrm{End}_{\mathcal{O}_F}(A/Z_F^{\mathrm{ord}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \xrightarrow{\sim} \quad \mathrm{End}_{\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p}(A[p^\infty]/Z_F^{\mathrm{ord}})$$
$$\|$$
$$\mathrm{End}_{\prod_{\wp \in S} \mathcal{O}_\wp}(X_1) \times \mathrm{End}_{\prod_{\wp \notin S} \mathcal{O}_\wp}(X_2).$$

Since $\mathrm{End}_{\prod_{\wp \notin S} \mathcal{O}_\wp}(X_2) \supseteq \prod_{\wp \notin S}(\mathcal{O}_\wp \times \mathcal{O}_\wp)$, we conclude that $\mathrm{End}_{\mathcal{O}_F}(A/Z_F^{\mathrm{ord}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is either a totally imaginary quadratic extension field of F or a central quaternion algebra over F. This implies that the abelian scheme $A \to Z_F^{\mathrm{ord}}$ admits smCM (see §10.15), therefore it is isotrivial. We have arrived at a contradiction because $\dim(Z_F^{\mathrm{ord}}) > 0$ by 9.8. Therefore $S = \Sigma_{F,p}$.

10. Notations and some results used

10.1. Abelian varieties. For the definition of an abelian variety and an abelian scheme, see [**54**], II.4, [**55**], 6.1. The dual of an abelian scheme $A \to S$ will be denoted by $A^t \to S$. We avoid the notation $\hat{A}$ as in [**55**], 6.8 for the dual abelian scheme, because of possible confusion with the formal completion (of a ring, of a scheme at a subscheme).

An isogeny $\varphi : A \to B$ of abelian schemes is a finite, surjective homomorphism. It follows that $\mathrm{Ker}(\varphi)$ is finite and flat over the base, [**55**], Lemma 6.12. This defines a dual isogeny $\varphi^t : B^t \to A^t$. And see 10.11.

The dimension of an abelian variety we will usually denote by g. If $m \in \mathbb{Z}_{>1}$ and A is an abelian variety we write $A[m]$ for the group scheme of m-torsion points. Note that if $m \in \mathbb{Z}_{>0}$ is invertible on the base scheme S, then $A[m]$ is a group scheme finite étale over S; if moreover $S = \mathrm{Spec}(K)$, in this case it is uniquely determined by the Galois module $A[m](k)$. See 10.5 for details. If the characteristic p of the base field divides m, then $A[m]$ is a group scheme which is not reduced.

A divisor D on an abelian scheme A/S defines a morphism $\varphi_D : A \to A^t$, see [**54**], theorem on page 125, see [**55**], 6.2. A *polarization* on an abelian scheme $\mu : A \to A^t$ is an isogeny such that for every geometric point $s \in S(\Omega)$ there exists an ample divisor D on A_s such that $\lambda_s = \varphi_D$, see [**54**], Application 1 on page 60, and [**55**], Definition 6.3. Note that a polarization is *symmetric* in the sense that

$$\left(\lambda : A \to A^t \right) \quad = \quad \left(A \xrightarrow{\ \kappa\ } A^{tt} \xrightarrow{\ \lambda^t\ } A^t \right),$$

where $\kappa : A \to A^{tt}$ is the canonical isomorphism.

Writing $\varphi : (B, \mu) \to (A, \lambda)$ we mean that $\varphi : A \to A$ and $\varphi^*(\lambda) = \mu$, i.e.,

$$\mu = \left(B \xrightarrow{\ \varphi\ } A \xrightarrow{\ \lambda\ } A^t \xrightarrow{\ \varphi^t\ } B^t \right).$$

10.2. Warning. Most recent papers distinguish between an abelian variety defined over a field K on the one hand, and $A \otimes_K K'$ over $K' \supsetneqq K$ on the other hand. The notation $\mathrm{End}(A)$ stands for the ring of endomorphisms of A over K. This is the way Grothendieck taught us to choose our notation.

In pre-Grothendieck literature and in some modern papers there is confusion between on the one hand A/K and "the same" abelian variety over any extension field. Often it is not clear what is meant by "a point on A"; the notation $\mathrm{End}_K(A)$ can stand for the "endomorphisms defined over K", but then sometimes $\mathrm{End}(A)$ can stand for the "endomorphisms defined over $\overline{K}$".

Please adopt the Grothendieck convention that a scheme $T \to S$ is what it is, and any scheme obtained by base extension $S' \to S$ is denoted by $T \times_S S' = T_{S'}$, etc. For an abelian scheme $X \to S$ write $\mathrm{End}(X)$ for the endomorphism ring of $X \to S$ (old terminology "endomorphisms defined over S"). Do not write $\mathrm{End}_T(X)$ but $\mathrm{End}(X \times_S T)$.

10.3. Moduli spaces. We try to classify isomorphism classes of polarized abelian varieties (A, μ). This is described by the theory of moduli spaces; see [**55**]. In particular see Chapter 5 of this book, where the notions of coarse and fine moduli scheme are described. We adopt the notation of [**55**]. By $\mathcal{A}_g \to \mathrm{Spec}(\mathbb{Z})$ we denote the coarse moduli scheme of polarized abelian varieties of dimension g. Note that for an algebraically closed field k there is a natural identification of $\mathcal{A}_g(k)$ with the set of isomorphism classes of (A, μ) defined over k, with $\dim(A) = g$. We write $\mathcal{A}_{g,d}$ for the moduli space of polarized abelian varieties (A, μ) with $\deg(\mu) = d^2$. Note that $\mathcal{A}_g = \bigsqcup_d \mathcal{A}_{g,d}$. Given positive integers g, d, n, denote by $\mathcal{A}_{g,d,n} \to \mathrm{Spec}(\mathbb{Z}[1/dn])$ the moduli space considering polarized abelian varieties with a symplectic level-n structure; in this case it is assumed that we have chosen and fixed an isomorphism from the constant group scheme $\mathbb{Z}/n\mathbb{Z}$ to μ_n over k, so

that symplectic level-n structure makes sense. According to these definitions we have $\mathcal{A}_{g,d,1} = \mathcal{A}_{g,d} \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(\mathbb{Z}[1/d])$.

Most of the considerations in this course are over fields of characteristic p. Working over a field of characteristic p we should write $\mathcal{A}_g \otimes \mathbb{F}_p$ for the moduli space under consideration; however, in case it is clear what the base field K or the base scheme is, instead we will $\mathcal{A}_g$ instead of the notation $\mathcal{A}_g \otimes K$; we hope this will not cause confusion.

10.4. The Cartier dual. The group schemes considered will be assumed to be *commutative.* If G is a finite abelian group, and S is a scheme, we write $\underline{G}_S$ for the constant group scheme over S with fiber equal to G.

Let $N \to S$ be a finite locally free commutative group scheme. Let $\underline{\mathrm{Hom}}(N, \mathbb{G}_m)$ be the functor on the category of all S-schemes, whose value at any S-scheme T is $\mathrm{Hom}_T(N \times_S T, \mathbb{G}_m \times_{\mathrm{Spec}(\mathbb{Z})} T)$. This functor is a sheaf for the fpqc topology, and is representable by a flat locally free scheme N^D over S, see [**61**], I.2. This group scheme $N^D \to S$ is called the *Cartier dual* of $N \to S$, and it can be described explicitly as follows. If $N = \mathrm{Spec}(E) \to S = \mathrm{Spec}(R)$ we write $E^D := \mathrm{Hom}_R(E, R)$. The multiplication map on E gives a comultiplication on E^D, and the commutative comultiplication on E provides E^D with the structure of a commutative ring. With the inverse map they give E^D a structure of a commutative and cocommutative bialgebra over R, and make $\mathrm{Spec}(E^D)$ into a commutative group scheme. This commutative group scheme $\mathrm{Spec}(E^D)$ is naturally isomorphic to the Cartier dual N^D of N. It is a basic fact, easy to prove, that the natural homomorphism $N \to (N^D)^D$ is an isomorphism for every finite locally free group scheme $N \to S$.

Examples. The constant group schemes $\underline{\mathbb{Z}/n\mathbb{Z}}$ and $\mu_n := \mathrm{Ker}\,([n]_{\mathbb{G}_m})$ are Cartier dual to each other, over any base scheme. More generally, a finite commutative group scheme $N \to S$ is étale if and only if its Cartier dual $N^D \to S$ is *of multiplicative type*, i.e., there exists an étale surjective morphism $g : T \to S$, such that $N^D \times_S T$ is isomorphic to a direct sum of group schemes μ_{n_i} for suitable positive integers n_i. The above morphism $g : T \to S$ can be chosen to be finite étale surjective.

For every field $K \supset \mathbb{F}_p$, the group scheme α_p is self-dual. Recall that α_p is the kernel of the Frobenius endomorphism Fr_p on $\mathbb{G}_a$.

10.5. Étale finite group schemes as Galois modules. (Any characteristic.) Let K be a field, and let $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. The main theorem of Galois theory says that there is an equivalence between the category of finite étale K-algebras and the category of finite sets with a continuous G-action. Taking group objects on both sides we arrive at:

Theorem. *There is an equivalence between the category of commutative finite étale group schemes over K and the category of finite continuous G-modules.*

See [**84**], 6.4. Note that an analogous equivalence holds in the case of not necessarily commutative group schemes.

This is a special case of the following. Let S be a connected scheme, and let $s \in S$ be a geometric base point; let $\pi = \pi_1(S, s)$. *There is an equivalence between the category of étale finite schemes over S and the category of finite continuous π-sets.* Here $\pi_1(S, s)$ is the algebraic fundamental group defined by Grothendieck in SGA 1; see [**33**].

Hence the definition of $T_\ell(A)$ for an abelian variety over a field K with $\ell \neq \mathrm{char}(K)$ can be given as:

$$T_\ell(A) = \varprojlim_i \ A[\ell^i](K^{\mathrm{sep}}),$$

considered as a continuous $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module.

Definition 10.6. Let S be a scheme. A *p-divisible group* over S is an inductive system $X = (X_n, \iota_n)_{n \in \mathbb{N}_{>0}}$ of finite locally free commutative group schemes over S satisfying the following conditions.

(i) X_n is killed by p^n for every $n \geq 1$.

(ii) Each homomorphism $\iota_n : X_n \to X_{n+1}$ is a closed embedding.

(iii) For each $n \geq 1$ the homomorphism $[p]_{X_{n+1}} : X_{n+1} \to X_{n+1}$ factors through $\iota_n : X_n \to X_{n+1}$, such that the resulting homomorphism $X_{n+1} \to X_n$ is faithfully flat. In other words there is a faithfully flat homomorphism $\pi_n : X_{n+1} \to X_n$ such that such that $\iota_n \circ \pi_n = [p]_{X_{n+1}}$. Here $[p]_{X_{n+1}}$ is the endomorphism "multiplication by p" on the commutative group scheme X_{n+1}.

Sometimes one writes $X[p^n]$ for the finite group scheme X_n. Equivalent definitions can be found in [**34**, Chapter III] and [**49**, Chapter I] and [**38**]; these are basic references to p-divisible groups.

Some authors use the terminology "Barsotti-Tate group", a synonym for "p-divisible group".

A p-divisible group $X = (X_n)$ over S is said to be *étale* (resp. *toric*) if every X_n is finite étale over S (resp. of multiplicative type over S).

For any p-divisible group $X \to S$, there is a locally constant function $h : S \to \mathbb{N}$, called the *height* of X, such that $\mathcal{O}_{X_n}$ is a locally free $\mathcal{O}_S$-algebra of rank p^h for every $n \geq 1$.

Example.

(1) Over any base scheme S we have the constant p-divisible group $\underline{\mathbb{Q}_p/\mathbb{Z}_p}$ of height 1, defined as the inductive limit of the constant groups $\underline{p^{-n}\mathbb{Z}/\mathbb{Z}}$ over S.

(2) Over any base scheme S, the p-divisible group $\mu_{p^\infty} = \mathbb{G}_m[p^\infty]$ is the inductive system $(\mu_{p^n})_{n \geq 1}$, where $\mu_{p^n} := \mathrm{Ker}\,([p^n]_{\mathbb{G}_m})$.

(3) Let $A \to S$ be an abelian scheme. For every i we write $G_i = A[p^i]$. The inductive system $G_i \subset G_{i+s} \subset A$ defines a p-divisible group of height $2g$. We shall denote this by $X = A[p^\infty]$ (although of course "p^∞" strictly speaking is not defined). A homomorphism $A \to B$ of abelian schemes defines a morphism $A[p^\infty] \to B[p^\infty]$ of p-divisible groups.

10.7. The Serre dual of a p-divisible group. Let $X = (X_n)_{n \in \mathbb{Z}_{>0}}$ be a p-divisible group over a scheme S. The *Serre dual* of X is the p-divisible group $X^t = \left(X_n^{\mathrm{D}}\right)_{n \geq 1}$ over S, where $X_n^{\mathrm{D}} := \underline{\mathrm{Hom}}_S(X_n, \mathbb{G}_m)$ is the Cartier dual of X_n, the embedding $X_n^{\mathrm{D}} \to X_{n+1}^{\mathrm{D}}$ is the Cartier dual of the faithfully flat homomorphism $\pi_n : X_{n+1} \to X_n$, and the faithfully flat homomorphism $X_{n+1}^{\mathrm{D}} \to X_n^{\mathrm{D}}$ is the Cartier dual of the embedding $\iota_n : X_n \to X_{n+1}$.

As an example, over any base scheme S the p-divisible group μ_{p^∞} is the Serre dual of the constant p-divisible group $\underline{\mathbb{Q}_p/\mathbb{Z}_p}$, because μ_{p^n} is the Cartier dual of $\underline{p^{-n}\mathbb{Z}/\mathbb{Z}}$. Below are some basic properties of Serre duals.

(1) The height of X^t is equal to the height of X.

(2) The Serre dual of a short exact sequence of p-divisible groups is exact.

(3) The Serre dual of X^t is naturally isomorphic to X.

(4) A p-divisible group $X = (X_n)$ is *toric* if and only if its Serre dual $X^t = (X_n^{\mathrm{D}})$ is étale. If this is the case, then the sheaf $\underline{\mathrm{Hom}}(X, \mu_{p^\infty})$ of *characters* of X is the projective limit of the étale sheaves X_n^{D}, where the transition map $X_{n+1}^{\mathrm{D}} \to X_n^{\mathrm{D}}$ is the Cartier dual of the embedding $\iota_n : X_n \to X_{n+1}$.

(5) Let $A \to S$ be an abelian scheme, and let $A^t \to S$ be the dual abelian scheme. Then the Serre dual of the p-divisible group $A[p^\infty]$ attached to the abelian scheme $A \to S$ is the p-divisible group $A^t[p^\infty]$ attached to the dual abelian scheme $A^t \to S$; see 10.11.

10.8. Discussion. Over any base scheme S (in any characteristic) for an abelian scheme $A \to S$ and for a prime number ℓ invertible in $\mathcal{O}_S$ one can define $T_\ell(A/S)$ as follows. For $i \in \mathbb{Z}_{>0}$ one chooses $N_i := A[\ell^i]$, regarded as a smooth étale sheaf of free $\mathbb{Z}/\ell^i\mathbb{Z}$-modules of rank $2\dim(A)$, and we have surjective maps $[\ell] : N_{i+1} \to N_i$ induced by multiplication by ℓ. The projective system of the N_i's "is" a smooth étale sheaf of $\mathbb{Z}_\ell$-modules of rank $2\dim(A)$, called the ℓ-*adic Tate module* of A/S, denoted by $T_\ell(A/S)$. Alternatively, we can consider $T_\ell(A/S)$ as a projective system

$$T_\ell(A/S) \quad = \quad \varprojlim_{i \in \mathbb{N}} A[\ell^i]$$

of the finite étale group schemes $A[\ell^i]$ over S. This projective system we call the *Tate ℓ-group* of A/S. Any geometric fiber of $T_\ell(A/S)_{\bar{s}}$ is constant, hence the projective limit of $T_\ell(A/S)_{\bar{s}}$ is isomorphic to $(\underline{\mathbb{Z}_{\ell_s}})^{2g}$. If S is the spectrum of a field K, the Tate ℓ-group can be considered as a $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module on the group $\mathbb{Z}_\ell^{2g}$, see 10.5. *One should like to have an analogous concept for this notion in case p is not invertible on S.* This is precisely the role of $A[p^\infty]$ defined above. Historically a Tate ℓ-group is defined as a projective system, and the p-divisible group as an inductive system; it turns out that these are the best ways of handling these concepts (but the way in which direction to choose the limit is not very important). We see that the p-divisible group of an abelian variety should be considered as the natural substitute for the Tate ℓ-group.

In order to carry this analogy further we investigate aspects of $T_\ell(A)$ and wonder whether these can be carried over to $A[p^\infty]$ in case of an abelian variety A in characteristic p. The Tate ℓ-group is a twist of a pro-group scheme defined over $\mathrm{Spec}(\mathbb{Z}[1/\ell])$. What can be said in analogy about $A[p^\infty]$ in the case of an abelian variety A in characteristic p? We will see that *up to isogeny $A[p^\infty]$ is a twist of an ind-group scheme over $\mathbb{F}_p$*; however, "twist" here should be understood not only in the sense of separable Galois theory, but also using inseparable aspects: the main idea of Serre-Tate parameters, to be discussed in Section 2.

10.9. Let X be a p-divisible group over an Artinian local ring R whose residue field is of characteristic p.

(1) There exists a largest étale quotient p-divisible group $X_{\text{ét}}$ of X over R, such that every homomorphism from X to an étale p-divisible group factors uniquely through $X_{\text{ét}}$. The kernel of $X \to X_{\text{ét}}$ is called the *neutral component* of X, or the maximal connected p-divisible subgroup of X, denoted by X_{conn}.

(2) The Serre dual of the maximal étale quotient $X_{\text{ét}}^t$ of X^t is called the *toric part* of X, denoted X_{tor}. Alternatively, $X_{\text{tor}}[p^n]$ is the maximal subgroup scheme in $X[p^n]$ of multiplicative type, for each $n \geq 1$.

(3) We have two short exact sequences of p-divisible groups

$$0 \to X_{\text{tor}} \to X_{\text{conn}} \to X_{\ell\ell} \to 0$$

and

$$0 \to X_{\text{conn}} \to X \to X_{\text{ét}} \to 0$$

over R, where $X_{\ell\ell}$ is a p-divisible group over $R\dim(A)$ with trivial étale quotient and trivial toric part. The closed fiber of the p^n-torsion subgroup $X_{\ell\ell}[p^n]$ of $X_{\ell\ell}$ is unipotent for every $n \geq 1$.

(4) The scheme-theoretic inductive limit of X_{conn} (resp. X_{tor}) is a finite dimensional commutative formal group scheme $X_{\text{conn}}^{\wedge}$ over R (resp. a finite dimensional formal torus $X_{\text{tor}}^{\wedge}$ over R), called the *formal completion* of X_{conn} (resp. X_{tor}). The endomorphism $[p^n]$ on $X_{\text{conn}}^{\wedge}$ (resp. $X_{\text{tor}}^{\wedge}$) is faithfully flat; its kernel is canonically isomorphic to $X_{\text{conn}}[p^n]$ (resp. $X_{\text{tor}}[p^n]$). In particular one can recover the p-divisible groups X_{conn} (resp. X_{tor}) from the smooth formal group $X_{\text{conn}}^{\wedge}$ (resp. $X_{\text{tor}}^{\wedge}$).

(5) If $X = A[p^{\infty}]$ is the p-divisible group attached to an abelian scheme A over R, then $X_{\text{conn}}^{\wedge}$ is canonically isomorphic to the formal completion of A along its zero section.

A p-divisible group X over an Artinian local ring R whose maximal étale quotient is trivial is often said to be *connected*. Note that $X[p^n]$ is connected, or equivalently, geometrically connected, for every $n \geq 1$. The formal completion of a connected p-divisible group over R is usually called a *p-divisible formal group*. It is not difficult to see that a smooth formal group over an Artinian local ring R is a p-divisible formal group if and only its closed fiber is.

More information about the infinitesimal properties of p-divisible groups can be found in [**49**] and [**38**]. Among other things one can define the Lie algebra of a p-divisible group $X \to S$ when p is locally nilpotent in $\mathcal{O}_S$; it coincides with the Lie algebra of the formal completion of X_{conn} when S is the spectrum of an Artinian local ring.

10.10. The following are equivalent conditions for a g-dimensional abelian variety A over an algebraically closed field $k \supset \mathbb{F}_p$; A is said to be *ordinary* if these conditions are satisfied.

(1) $\text{Card}(A[p](k)) = p^g$, i.e., the p-rank of A is equal to g.

(2) $A[p^n](k) \cong \mathbb{Z}/p^n\mathbb{Z}$ for some positive integer n.

(3) $A[p^n](k) \cong \mathbb{Z}/p^n\mathbb{Z}$ for every positive integer n.

(4) The formal completion $A^{/0}$ of A along the zero point is a formal torus.

(5) The p-divisible group $A[p^{\infty}]$ attached to A is an extension of an étale p-divisible group of height g by a toric p-divisible group of height g.

(6) The σ-linear endomorphism on $\text{H}^1(A, \mathcal{O}_A)$ induced by the absolute Frobenius of A is bijective, where σ is the Frobenius automorphism on k.

Note that for an ordinary abelian variety A over a field $K \supset \mathbb{F}_p$ the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ acts on $A[p]_{\mathrm{loc}}$ and on $A[p]_{\text{ét}} = A[p]/A[p]_{\mathrm{loc}}$, and these actions need not be trivial. Moreover if K is not perfect, the extension

$$0 \to A[p]_{\mathrm{loc}} \to A[p] \to A[p]_{\text{ét}} \to 0$$

need not be split; this is studied extensively in Section 2.

Reminder. It is a general fact that every finite group scheme G over a field K sits naturally in the middle of a short exact sequence $0 \to G_{\mathrm{loc}} \to G \to G_{\text{ét}} \to 0$ of finite group schemes over K, where $G_{\text{ét}}$ is étale and G_{loc} is connected. If the rank of G is prime to the characteristic of K, then G is étale over K, i.e., G_{loc} is trivial; e.g. see [**60**].

10.11. We recall the statement of a basic duality result for abelian schemes over an arbitrary base scheme.

Theorem. (Duality theorem for abelian schemes, see [**61**], Theorem 19.1) *Let $\varphi : B \to A$ be an isogeny of abelian schemes. We obtain an exact sequence*

$$0 \quad \to \quad \mathrm{Ker}(\varphi)^D \quad \longrightarrow \quad A^t \quad \overset{\varphi^t}{\longrightarrow} \quad B^t \quad \to \quad 0.$$

An application. Let A be a g-dimensional abelian variety over a field $K \supset \mathbb{F}_p$, and let A^t be the dual abelian variety of A. Then $A[n]$ and $A^t[n]$ are dual to each other for every non-zero integer n. This natural duality pairing identifies the maximal étale quotient of $A[n]$ (resp. $A^t[n]$ with the Cartier dual of the maximal subgroup of $A^t[n]$ (resp. $A[n]$ of multiplicative type. This implies that the Serre dual of the p-divisible group $A[p^\infty]$ is isomorphic to $A^t[p^\infty]$. Since A and A^t are isogenous, we deduce that the maximal étale quotient of the p-divisible group $A[p^\infty]$ and the maximal toric p-divisible subgroup of $A[p^\infty]$ have the same height.

10.12. Endomorphism rings. Let A be an abelian variety over a field K, or more generally, an abelian scheme over a base scheme S. We write $\mathrm{End}(A)$ for the *endomorphism ring* of A. For every $n \in \mathbb{Z}_{>0}$, multiplication by n on A is an epimorphic morphism of schemes because it is faithfully flat, hence $\mathrm{End}(A)$ is torsion-free. In the case S is connected, $\mathrm{End}(A)$ is a free $\mathbb{Z}$-module of finite rank. We write $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ for the *endomorphism algebra* of A. By Wedderburn's theorem every central simple algebra is a matrix algebra over a division algebra. If A is K-simple the algebra $\mathrm{End}^0(A)$ is a division algebra; in that case we write:

$$\mathbb{Q} \quad \subset \quad L_0 \quad \subset \quad L := \mathrm{Centre}(D) \quad \subset \quad D = \mathrm{End}^0(A);$$

here L_0 is a totally real field, and either $L = L_0$ or $[L : L_0] = 2$ and in that case L is a CM-field. In case A is simple $\mathrm{End}^0(A)$ is one of the four types in the Albert classification (see below). We write:

$$[L_0 : \mathbb{Q}] = e_0, \quad [L : \mathbb{Q}] = e, \quad [D : L] = d^2.$$

10.13. Let $(A, \mu) \to S$ be a polarized abelian scheme. As μ is an isogeny, there exist μ' and $n \in \mathbb{Z}_{>0}$ such that $\mu' \cdot \mu = n$; think of μ'/n as the inverse of μ. We define the *Rosati involution* $\varphi \mapsto \varphi^\dagger$ by

$$\varphi \mapsto \varphi^\dagger := \frac{1}{n} \mu' \cdot \varphi^t \cdot \mu, \qquad \varphi \in D = \mathrm{End}^0(A).$$

The definition does not depend on the choice of μ' and n; it can be characterized by $\varphi^t \cdot \mu = \mu \cdot \varphi^\dagger$. This map $^\dagger : D \to D$ is an anti-involution on D.

The Rosati involution $^\dagger : D \to D$ is positive definite; for references see Proposition II in 3.10.

Definition. A *simple division algebra of finite degree over* $\mathbb{Q}$ *with a positive definite involution*, i.e., an anti-isomorphism of order two which is positive definite, is called an *Albert algebra*.

Applications to abelian varieties and the classification have been described by Albert, [**1**], [**4**] [**2**], [**3**].

10.14. Albert's classification. Any Albert algebra belongs to one of the following types.

Type I(e_0)   Here $L_0 = L = D$ is a totally real field.

Type II(e_0)   Here $d = 2$, $e = e_0$, $\mathrm{inv}_v(D) = 0$ for all infinite v, and D is an indefinite quaternion algebra over the totally real field $L_0 = L$.

Type III(e_0)   Here $d = 2$, $e = e_0$, $\mathrm{inv}_v(D) \neq 0$ for all infinite v, and D is a definite quaternion algebra over the totally real field $L_0 = L$.

Type IV(e_0, d)   Here L is a CM-field, $[F : \mathbb{Q}] = e = 2e_0$, and $[D : L] = d^2$.

10.15. smCM. We say that an abelian variety X over a field K *admits sufficiently many complex multiplications over* K, abbreviated by "smCM over K", if $\mathrm{End}^0(X)$ contains a commutative semi-simple subalgebra of rank $2 \cdot \dim(X)$ over $\mathbb{Q}$. Equivalently: for every simple abelian variety Y over K which admits a non-zero homomorphism to X the algebra $\mathrm{End}^0(Y)$ contains a field of degree $2 \cdot \dim(Y)$ over $\mathbb{Q}$. For other characterizations see [**21**], page 63, see [**53**], page 347.

Note that if a simple abelian variety X of dimension g over a field *of characteristic zero* admits smCM then its endomorphism algebra $L = \mathrm{End}^0(X)$ is a CM-field of degree $2g$ over $\mathbb{Q}$. We will use the terminology "CM-type" in the case of an abelian variety X over $\mathbb{C}$ which admits smCM, and where the type is given, i.e., the action of the endomorphism algebra on the tangent space $T_{X,0} \cong \mathbb{C}^g$ is part of the data.

Note however that there exist (many) abelian varieties A admitting smCM (defined over a field of positive characteristic), such that $\mathrm{End}^0(A)$ is not a field.

By Tate we know that an abelian variety over a finite field admits smCM, see 10.17. By Grothendieck we know that an abelian variety over an algebraically closed field $k \supset \mathbb{F}_p$ which admits smCM is isogenous to an abelian variety defined over a finite field, see 10.19.

Terminology. Let $\varphi \in \mathrm{End}^0(A)$. Then $d\varphi$ is a K-linear endomorphism of the tangent space. If the base field is $K = \mathbb{C}$, this is just multiplication by a complex matrix x, and every multiplication by a complex matrix x leaving invariant the lattice Λ, where $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$, gives rise to an endomorphism of A. If $g = 1$, i.e., A is an elliptic curve, and $\varphi \notin \mathbb{Z}$ then $x \in \mathbb{C}$ and $x \notin \mathbb{R}$. Therefore an endomorphism of an elliptic curve over $\mathbb{C}$ which is not in $\mathbb{Z}$ is sometimes called "a complex multiplication". Later this terminology was extended to all abelian varieties.

Warning. Sometimes the terminology "an abelian variety with CM" is used, when one wants to say "admitting smCM". An elliptic curve E has $\mathrm{End}(E) \supsetneqq \mathbb{Z}$ if and only if it admits smCM. Note that it is easy to give an abelian variety A which "admits CM", meaning that $\mathrm{End}(A) \supsetneqq \mathbb{Z}$, such that A does not admit smCM. However we will use the terminology "a CM-abelian variety" for an abelian variety which admits smCM.

Exercise 10.16. Show there exists an abelian variety A over a field k such that $\mathbb{Z} \subsetneqq \mathrm{End}(A)$ and such that A does not admit smCM.

Theorem 10.17. (Tate) *Let A be an abelian variety over a finite field.*
(1) *The algebra $\mathrm{End}^0(A)$ is semi-simple. Suppose A is simple; the center of $\mathrm{End}^0(A)$ equals $L := \mathbb{Q}(\pi_A)$.*
(2) *Suppose A is simple; then*

$$2g \quad = \quad [L : \mathbb{Q}] \cdot \sqrt{[D : L]}\,,$$

where g is the dimension of A. Hence: every abelian variety over a finite field admits smCM. See 10.15. Moreover we have

$$f_A \quad = \quad (\mathrm{Irr}_{\pi_A})^{\sqrt{[D:L]}}.$$

Here f_Z is the characteristic polynomial of the Frobenius morphism $\mathrm{Fr}_{A,\mathbb{F}_q} : A \to A$, and Irr_{π_A} is the irreducible polynomial over $\mathbb{Q}$ of the element π_A in the finite extension $L/\mathbb{Q}$.
(3) *Suppose A is simple,*

$$\mathbb{Q} \quad \subset \quad L := \mathbb{Q}(\pi_A) \quad \subset \quad D = \mathrm{End}^0(A).$$

The central simple algebra D/L

- *does not split at every real place of L,*
- *does split at every finite place not above p,*
- *and for $v \mid p$ the invariant of D/L is given by*

$$\mathrm{inv}_v(D/L) = \frac{v(\pi_A)}{v(q)} \cdot [L_v : \mathbb{Q}_p] \quad \mathrm{mod} \quad \mathbb{Z},$$

where L_v is the local field obtained from L by completing at v.

See [**78**], [**79**].

Remark 10.18. An abelian variety over a field of characteristic zero which admits smCM is defined over a number field; e.g. see [**77**], Proposition 26 on page 109.

Remark 10.19. The converse of Tate's result 10.17 (2) is almost true. We have the following theorem of Grothendieck: *Let A be an abelian variety over a field K which admits smCM; then A_k is isogenous to an abelian variety defined over a finite extension of the prime field, where $k = \overline{K}$; see [**62**].*

It is easy to give an example of an abelian variety (over a field of characteristic p), with smCM which is not defined over a finite field.

Exercise 10.20. Give an example of a simple abelian variety A over a field K such that $A \otimes \overline{K}$ is not simple.

10.21. Algebraization.

(1) Suppose we are given a formal p-divisible group X_0 over k with $\mathcal{N}(X_0) = \gamma$ ending at (h, c). We write $\mathcal{D}^\wedge = \mathrm{Def}(X_0)$ for the universal deformation space in equal characteristic p. By this we mean the following. Formal deformation theory of X_0 is prorepresentable; we obtain a formal scheme $\mathrm{Spf}(R)$ and a prorepresenting family $\mathcal{X}' \to \mathrm{Spf}(R)$. However, "a finite group scheme over a formal scheme actually is already defined over an actual scheme". Indeed, by [**17**], Lemma 2.4.4 on page 23, we know that there is an equivalence of categories of p-divisible groups over $\mathrm{Spf}(R)$, respectively over $\mathrm{Spec}(R)$. We write $\mathcal{D}(X_0) = \mathrm{Spec}(R)$, and corresponding to the pro-universal family $\mathcal{X}' \to \mathrm{Spf}(R)$ we have a family $\mathcal{X} \to \mathcal{D}(X_0)$. We will say that $\mathcal{X} \to \mathrm{Spec}(R) = \mathcal{D}(X_0)$ is the universal deformation of X_0 if the corresponding $\mathcal{X}' \to \mathrm{Spf}(R) = \mathcal{D}^\wedge = \mathrm{Def}(X_0)$ prorepresents the deformation functor.

  Note that for a formal p-divisible group $\mathcal{X}' \to \mathrm{Spf}(R)$, where R is moreover an integral domain, it makes sense to consider "the generic fiber" of $\mathcal{X}/\mathrm{Spec}(R)$.

(2) Let A_0 be an abelian variety. The deformation functor $\mathrm{Def}(A_0)$ is prorepresentable. We obtain the prorepresenting family $A \to \mathrm{Spf}(R)$, which is a formal abelian scheme. If $\dim(A_0) > 1$ this family is *not algebraizable*, i.e., it does not come from an actual scheme over $\mathrm{Spec}(R)$.

(3) Let (A_0, μ_0) be a polarized abelian variety. The deformation functor $\mathrm{Def}(A_0, \mu_0)$ is prorepresentable. We can use the Chow-Grothendieck theorem, see [**32**], III^1.5.4 (this is also called a theorem of "GAGA-type"): the formal polarized abelian scheme obtained is algebraizable, and we obtain the universal deformation as a polarized abelian scheme over $\mathcal{D}(A_0, \mu_0) = \mathrm{Spec}(R)$.

The notions mentioned in (1), (2) and (3) will be used without further mention, assuming the reader to be familiar with the subtle differences between $\mathcal{D}(-)$ and $\mathrm{Def}(-)$.

10.22. Fix a prime number p. Base schemes and base fields will be of characteristic p, unless otherwise stated. We write k or Ω for an algebraically closed field. For the rest of this section we are working in characteristic p.

10.23. The Frobenius morphism. For a scheme S over $\mathbb{F}_p$ (i.e., $p \cdot 1 = 0$ in all fibers of $\mathcal{O}_S$), we define the absolute Frobenius morphism $\mathrm{fr} : S \to S$; if $S = \mathrm{Spec}(R)$ this is given by $x \mapsto x^p$ in R.

For a scheme $A \to S$ we define $A^{(p)}$ as the fiber product of $A \to S \xleftarrow{\mathrm{fr}} S$. The morphism $\mathrm{fr} : A \to A$ factors through $A^{(p)}$. This defines $F_A : A \to A^{(p)}$, a morphism over S; this is called *the relative Frobenius morphism*. If A is a group scheme over S, the morphism $F_A : A \to A^{(p)}$ is a homomorphism of group schemes. For more details see [**35**], Exp. VII$_A$.4. The notation $A^{(p/S)}$ is (maybe) more correct.

Examples. Suppose $A \subset \mathbb{A}^n_R$ is given as the zero set of a polynomial $\sum_I a_I X^I$ (multi-index notation). Then $A^{(p)}$ is the zero set of $\sum_I a_I^p X^I$, and $A \to A^{(p)}$ is given, on coordinates, by raising these to the power p. Note that if a point

$(x_1, \cdots, x_n) \in A$ then indeed $(x_1^p, \ldots, x_n^p) \in A^{(p)}$, and $x_i \mapsto x_i^p$ describes $F_A : A \to A^{(p)}$ on points.

Let $S = \mathrm{Spec}(\mathbb{F}_p)$; for any $T \to S$ we have a canonical isomorphism $T \cong T^{(p)}$. In this case $F_T = \mathrm{fr} : T \to T$.

10.24. Verschiebung. Let A be a *commutative* group scheme flat over a characteristic p base scheme. In [**35**], Exp. VII$_A$.4 we find the definition of the "relative Verschiebung"

$$V_A : A^{(p)} \to A; \quad \text{we have:} \quad F_A \cdot V_A = [p]_{A^{(p)}}, \quad V_A \cdot F_A = [p]_A.$$

In case A is an abelian variety we see that F_A is a faithfully flat homomorphism, and $\mathrm{Ker}(F_A) \subset A[p]$. In this case we do not need the somewhat tricky construction of [**35**], Exp. VII$_A$.4: since the kernel of the isogeny $F_A : A \to A^{(p)}$ is killed by p, we can define V_A as the isogeny from $A^{(p)}$ to A such that $V_A \cdot F_A = [p]_A$, and the equality $F_A \cdot V_A = [p]_{A^{(p)}}$ follows from $F_A \cdot V_A \cdot F_A = [p]_{A^{(p)}} \cdot F_A$ because F_A is faithfully flat.

Remark 10.25. We use covariant Dieudonné module theory. The Frobenius on a group scheme G defines the Verschiebung on $\mathbb{D}(G)$; this we denote by $\mathcal{V}$, in order to avoid possible confusion. In the same way as "$\mathbb{D}(F) = \mathcal{V}$" we have "$\mathbb{D}(V) = \mathcal{F}$". See [**67**], 15.3.

Theorem 10.26. $\boxed{\text{BB}}$ (Irreducibility of moduli spaces) *Let K be a field, and consider $\mathcal{A}_{g,1,n} \otimes K$ the moduli space of principally polarized abelian varieties over K-schemes, where $n \in \mathbb{Z}_{>0}$ is prime to the characteristic of K. This moduli scheme is geometrically irreducible.*

For fields of characteristic zero this follows by complex uniformization. For fields of positive characteristic this was proved by Faltings in 1984, see [**27**], at the same time for $p > 2$ by Chai in his Harvard PhD thesis, see [**8**]; also see [**28**], IV.5.10. For a pure characteristic-p-proof see [**67**], 1.4.

11. A remark and some questions

11.1. In 1.13 we have seen that the closure of the *full* Hecke orbit equals the related Newton polygon stratum. That result finds its origin in the construction of two *foliations*, as in [**68**]: Hecke-prime-to-p actions "move" a point in a central leaf, and Hecke actions only involving compositions of isogenies with kernel isomorphic to α_p "move" a point in an isogeny leaf, called $\mathcal{H}_\alpha$-actions; as an open Newton polygon stratum, up to a finite map, is equal to the product of a central leaf and an isogeny leaf, the result 1.13 for an irreducible component of a Newton polygon stratum follows if we show that $\mathcal{H}_\ell(x)$ is dense in the central leaf passing through x.

In the case of ordinary abelian varieties the central leaf is the whole open Newton polygon stratum. As the Newton polygon goes up central leaves get smaller. Finally, for supersingular points a central leaf is finite (see Lemma 1.14) and an isogeny leaf of a supersingular point is the whole supersingular locus.

In order to finish a proof of 1.13 one shows that Hecke-α actions act transitively on the set of geometric components of the supersingular locus, and that any Newton polygon stratum in $\mathcal{A}_{g,1}$ which is not supersingular is geometrically irreducible, see [**14**].

11.2. Let D be an Albert algebra; i.e., D is a division algebra, it is of finite rank over $\mathbb{Q}$, and it has a positive definite anti-involution $\dagger : D \to D$. Suppose a characteristic is given. There exists a field k of that characteristic, and an abelian variety A over k such that $\operatorname{End}^0(A) \cong D$, and such that $\dagger$ is the Rosati involution given by a polarization on A. This was proved by Albert, and by Shimura over $\mathbb{C}$ (see [**76**], Theorem 5). In general this was proved by Gerritzen [**30**]; for more references see [**64**].

One can ask which possibilities we have for $\dim(A)$, once D is given. This question is completely settled in characteristic zero. From properties of D one can derive some restrictions on $\dim(A)$. However the question which dimensions $\dim(A)$ can appear for a given D in positive characteristic is not yet completely settled.

Also, there is not yet a complete criterion for which endomorphism algebras can appear in positive characteristic.

11.3. In Section 5, in particular see the proofs of 5.10 and 5.16, we have seen a natural way of introducing coordinates in the formal completion at a point x where $a \le 1$ on an (open) Newton polygon stratum:

$$(\mathcal{W}_\xi(\mathcal{A}_{g,1,n}))^{/x} = \operatorname{Spf}(B_\xi),$$

see the proof of 5.19. It would be nice to have a better understanding and interpretation of these "coordinates".

As in [**58**] we write

$$\triangle(\xi; \xi^*) := \{(x,y) \in \mathbb{Z} \mid (x,y) \prec \xi, \quad (x,y) \gneqq \xi^*, \quad x \le g\}.$$

We write

$$B_{(\xi;\xi^*)} = k[[Z_{x,y} \mid (x,y) \in \triangle(\xi;\xi^*)]].$$

The inclusion $\triangle(\xi; \xi^*) \subset \triangle(\xi)$ defines $B_\xi \twoheadrightarrow B_{(\xi;\xi^*)}$ by equating to zero those elements $Z_{x,y}$ with $(x,y) \notin \Delta(\xi;\xi^*)$. Hence $\operatorname{Spf}(B_{(\xi;\xi^*)}) \subset \operatorname{Spf}(B_\xi)$. We also have the inclusion $\mathcal{C}(x) \subset \mathcal{W}_\xi(\mathcal{A}_{g,1,n})$.

Question. Does the inclusion $\triangle(\xi, \xi^*) \subset \triangle(\xi)$ define the inclusion $(\mathcal{C}(x))^{/x} \subset (\mathcal{W}_\xi(\mathcal{A}_{g,1,n}))^{/x}$?

A positive answer would give more insight in these coordinates, also along a central leaf, and perhaps a new proof of results in [**58**].

References

1. A. A. Albert, *On the construction of Riemann matrices. I*, Ann. of Math. (2) **35** (1934), no. 1, 1–28. MR 1503140

2. ———, *A solution of the principal problem in the theory of Riemann matrices*, Ann. of Math. (2) **35** (1934), no. 3, 500–515. MR 1503176

3. ———, *Involutorial simple algebras and real Riemann matrices*, Ann. of Math. (2) **36** (1935), no. 4, 886–964. MR 1503260

4. ———, *On the construction of Riemann matrices. II*, Ann. of Math. (2) **36** (1935), no. 2, 376–394. MR 1503230

5. P. Berthelot, L. Breen, and W. Messing, *Théorie de Dieudonné cristalline. II*, Lecture Notes in Mathematics, vol. 930, Springer-Verlag, Berlin, 1982. MR 667344 (85k:14023)

6. L. Breen, *Rapport sur la théorie de Dieudonné*, Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. I, Astérisque, vol. 63, Soc. Math. France, Paris, 1979, pp. 39–66. MR 563459 (81j:14025)

7. C.-L. Chai, *Families of ordinary abelian varieties: canonical coordinates, p-adic monodromy, Tate-linear subvarieties and Hecke orbits*, http://www.math.upenn.edu/~chai/.

8. _____, *Compactification of Siegel moduli schemes*, London Mathematical Society Lecture Note Series, vol. 107, Cambridge University Press, Cambridge, 1985. MR 853543 (88b:32074)

9. _____, *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli*, Invent. Math. **121** (1995), no. 3, 439–479. MR 1353306 (96f:11082)

10. _____, *Hecke orbits on Siegel modular varieties*, Geometric methods in algebra and number theory, Progr. Math., vol. 235, Birkhäuser Boston, Boston, MA, 2005, pp. 71–107. MR 2159378 (2006f:11050)

11. _____, *Monodromy of Hecke-invariant subvarieties*, Pure Appl. Math. Q. **1** (2005), no. 2, 291–303, Special issue: in memory of Armand Borel. MR 2194726 (2006m:11084)

12. _____, *A rigidity result for p-divisible formal groups*, Asian J. Math. **12** (2008), no. 2, 193–202.

13. C.-L. Chai and F. Oort, *Hecke orbits*, In preparation.

14. _____, *Monodromy and irreducibility of leaves*, Conference on abelian varieties, Amsterdam May 2006, http://www.math.upenn.edu/~chai/, http://www.math.uu.nl/people/oort/.

15. _____, *Hypersymmetric abelian varieties*, Pure Appl. Math. Q. **2** (2006), no. 1, 1–27. MR 2217565 (2007a:14052)

16. G. Cornell and J. H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986, Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984. MR 861969 (89b:14029)

17. A. J. de Jong, *Crystalline Dieudonné module theory via formal and rigid geometry*, Inst. Hautes Études Sci. Publ. Math. (1995), no. 82, 5–96 (1996). MR 1383213 (97f:14047)

18. _____, *Barsotti-Tate groups and crystals*, Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998), no. Extra Vol. II, 1998, pp. 259–265. MR 1648076 (99i:14051)

19. _____, *Homomorphisms of Barsotti-Tate groups and crystals in positive characteristic*, Invent. Math. **134** (1998), no. 2, 301–333, Erratum **138** (1999), 225. MR 1650324 (2000f:14070a)

20. A. J. de Jong and F. Oort, *Purity of the stratification by Newton polygons*, J. Amer. Math. Soc. **13** (2000), no. 1, 209–241. MR 1703336 (2000m:14050)

21. P. Deligne, *Hodge cycles on abelian varieties*, Hodge cycles, motives, and Shimura varieties, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin, 1982, Notes by J.S. Milne, pp. 9–100. MR 654325 (84m:14046)

22. P. Deligne and G. Pappas, *Singularités des espaces de modules de Hilbert, en les caractéristiques divisant le discriminant*, Compositio Math. **90** (1994), no. 1, 59–79. MR 1266495 (95a:11041)

23. P. Deligne and K. A. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. **59** (1980), no. 3, 227–286. MR 579702 (81m:12019)

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

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

26. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR 718935 (85g:11026a)

27. _____, *Arithmetische Kompaktifizierung des Modulraums der abelschen Varietäten*, Workshop Bonn 1984 (Bonn, 1984), Lecture Notes in Mathematics, vol. 1111, Springer, Berlin, 1985, pp. 321–383. MR 797429 (87c:14050)

28. G. Faltings and C.-L. Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 22, Springer-Verlag, Berlin, 1990, With an appendix by David Mumford. MR 1083353 (92d:14036)

29. G. Faltings and G. Wüstholz (eds.), *Rational points*, Aspects of Mathematics, E6, Friedr. Vieweg & Sohn, Braunschweig, 1984, Papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn, 1983/1984. MR 766568 (87h:14016)

30. L. Gerritzen, *On multiplication algebras of Riemann matrices*, Math Ann **194** (1971), 109–122. MR 0288141 (44 #5339)

31. E. Z. Goren and F. Oort, *Stratifications of Hilbert modular varieties*, J. Algebraic Geom. **9** (2000), no. 1, 111–154. MR 1713522 (2000g:14034)

32. A. Grothendieck, *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I*, Inst. Hautes Études Sci. Publ. Math. (1961), no. 11, 167. MR 0163910 (29 #1209)

33. ———, *Revêtements étales et groupe fondamental*, Lecture Notes in Mathematics, vol. 224, Springer-Verlag, Berlin, 1971, Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par A. Grothendieck. Augmenté de deux exposés de M. Raynaud. MR 0354651 (50 #7129)

34. ———, *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Les Presses de l'Université de Montréal, Montreal, Que., 1974, Séminaire de Mathématiques Supérieures, No. 45 (Été, 1970). MR 0417192 (54 #5250)

35. A. Grothendieck and M. Demazure, *Schémas en groupes. I: Propriétés générales des schémas en groupes*, Lecture Notes in Mathematics, vol. 151, Springer-Verlag, Berlin, 1970, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. MR 0274458 (43 #223a)

36. M. Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics, vol. 78, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978. MR 506881 (82a:14020)

37. T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95. MR 0229642 (37 #5216)

38. L. Illusie, *Déformations de groupes de Barsotti-Tate (d'après A. Grothendieck)*, Astérisque (1985), no. 127, 151–198, Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell (L. Szpiro), Paris, 1983/84. MR 801922

39. T. Katsura and F. Oort, *Supersingular abelian varieties of dimension two or three and class numbers*, Algebraic geometry, Sendai, 1985, Adv. Stud. Pure Math., vol. 10, North-Holland, Amsterdam, 1987, pp. 253–281. MR 946242 (90c:14027)

40. N. M. Katz, *Slope filtration of F-crystals*, Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. I, Astérisque, vol. 63, Soc. Math. France, Paris, 1979, pp. 113–163. MR 563463 (81i:14014)

41. ———, *Appendix to Exposé V: Cristaux ordinaires et coordonnées canoniques*, Algebraic surfaces (Orsay, 1976–78), Lecture Notes in Mathematics, vol. 868, Springer, Berlin, 1981, Appendix to an article of P. Deligne, pp. 127–137. MR 638599 (83k:14039a)

42. ———, *Serre-Tate local moduli*, Algebraic surfaces (Orsay, 1976–78), Lecture Notes in Mathematics, vol. 868, Springer, Berlin, 1981, pp. 138–202. MR 638600 (83k:14039b)

43. H. Kraft, *Kommutative algebraische p-Gruppen (mit Anwendungen auf p-divisible Gruppen und abelsche Varietäten)*, Sonderforsch. Bereich Bonn, September 1975, 86 pp. manuscript.

44. M. Lazard, *Commutative formal groups*, Lecture Notes in Mathematics, vol. 443, Springer-Verlag, Berlin, 1975. MR 0393050 (52 #13861)

45. K.-Z. Li and F. Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Mathematics, vol. 1680, Springer-Verlag, Berlin, 1998. MR 1611305 (99e:14052)

46. J. Lubin, J-P. Serre, and J. Tate, *Elliptic curves and formal groups*, Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-July 31, 1964, http://www.ma.utexas.edu/users/voloch/lst.html.

47. J. Lubin and J. Tate, *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–59. MR 0238854 (39 #214)

48. Yu. I. Manin, *Theory of commutative formal groups over fields of finite characteristic*, Uspehi Mat. Nauk **18** (1963), no. 6 (114), 3–90, Translated in Russ. Math. Surveys **18** (1963), 1–80. MR 0157972 (28 #1200)

49. W. Messing, *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, vol. 264, Springer-Verlag, Berlin, 1972. MR 0347836 (50 #337)

50. S. Mochizuki, *The local pro-p anabelian geometry of curves*, Invent. Math. **138** (1999), no. 2, 319–423. MR 1720187 (2000j:14037)

51. L. Moret-Bailly, *Pinceaux de variétés abéliennes*, Astérisque (1985), no. 129, 266. MR 797982 (87j:14069)

52. S. Mori, *On Tate conjecture concerning endomorphisms of abelian varieties*, Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977) (Tokyo), Kinokuniya Book Store, 1978, pp. 219–230. MR 578861 (82d:14026)

53. D. Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varieties"*, Math. Ann. **181** (1969), 345–351. MR 0248146 (40 #1400)

54. ———, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970. MR 0282985 (44 #219)

55. D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2), vol. 34, Springer-Verlag, Berlin, 1994. MR 1304906 (95m:14012)

56. P. Norman and F. Oort, *Moduli of abelian varieties*, Ann. of Math. (2) **112** (1980), no. 3, 413–439. MR 595202 (82h:14026)

57. T. Oda and F. Oort, *Supersingular abelian varieties*, Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977) (Tokyo), Kinokuniya Book Store, 1978, pp. 595–621. MR 578876 (81f:14023)

58. F. Oort, *Foliations in moduli spaces of abelian varieties and dimension of leaves*, to appear.

59. ———, *Purity reconsidered*, Talk, Amsterdam XII-2002, ms 9 pp., http://www.math.uu.nl/people/oort/.

60. ———, *Algebraic group schemes in characteristic zero are reduced*, Invent. Math. **2** (1966), 79–80. MR 0206005 (34 #5830)

61. ———, *Commutative group schemes*, Lecture Notes in Mathematics, vol. 15, Springer-Verlag, Berlin, 1966. MR 0213365 (35 #4229)

62. ———, *The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field*, J. Pure Appl. Algebra **3** (1973), 399–408. MR 0330175 (48 #8513)

63. ———, *Lifting algebraic curves, abelian varieties, and their endomorphisms to characteristic zero*, Algebraic geometry, Bowdoin, 1985, Part 2 (S. J. Bloch, ed.), Proc. Sympos. Pure Math., vol. 46, Amer. Math. Soc., Providence, RI, 1987, pp. 165–195. MR 927980 (89c:14069)

64. ———, *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, Kinokuniya, Tokyo, 1988, pp. 469–502. MR 977774 (90j:11049)

65. ———, *Newton polygons and formal groups: conjectures by Manin and Grothendieck*, Ann. of Math. (2) **152** (2000), no. 1, 183–206. MR 1792294 (2002e:14075)

66. ———, *Newton polygon strata in the moduli space of abelian varieties*, Moduli of abelian varieties (Texel Island, 1999) (F. Oort C. Faber, G. van der Geer, ed.), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 417–440. MR 1827028 (2002c:14069)

67. ———, *A stratification of a moduli space of abelian varieties*, Moduli of abelian varieties (Texel Island, 1999) (F. Oort C. Faber, G. van der Geer, ed.), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 345–416. MR 1827027 (2002b:14055)

68. ———, *Foliations in moduli spaces of abelian varieties*, J. Amer. Math. Soc. **17** (2004), no. 2, 267–296 (electronic). MR 2051612 (2005c:14051)

69. ———, *Minimal p-divisible groups*, Ann. of Math. (2) **161** (2005), no. 2, 1021–1036. MR 2153405 (2006i:14042)

70. V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen. MR 1278263 (95b:11039)

71. M. Rapoport, *Compactifications de l'espace de modules de Hilbert-Blumenthal*, Compositio Math. **36** (1978), no. 3, 255–335. MR 515050 (80j:14009)

72. M. Rapoport and Th. Zink, *Period spaces for p-divisible groups*, Annals of Mathematics Studies, vol. 141, Princeton University Press, Princeton, NJ, 1996. MR 1393439 (97f:14023)

73. M. Raynaud, *"p-torsion" du schéma de Picard*, Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II, Astérisque, vol. 64, Soc. Math. France, Paris, 1979, pp. 87–148. MR 563468 (81f:14026)

74. K. A. Ribet, *p-adic interpolation via Hilbert modular forms*, Algebraic geometry (Humboldt State Univ., Arcata, Calif., 1974), Proc. Sympos. Pure Math., vol. 29, Amer. Math. Soc., Providence, R. I., 1975, pp. 581–592. MR 0419414 (54 #7435)

75. L. Schneps and P. Lochak (eds.), *Geometric Galois actions. 1*, London Mathematical Society Lecture Note Series, vol. 242, Cambridge University Press, Cambridge, 1997, Around Grothendieck's "Esquisse d'un programme". MR 1483106 (98e:14003)

76. G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. (2) **78** (1963), 149–192. MR 0156001 (27 #5934)

77. G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961. MR 0125113 (23 #A2419)

78. J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR 0206004 (34 #5829)

79. ———, *Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Mathematics, vol. 179, Springer-Verlag, Berlin, 1971, Exp. 352, pp. 95–110. MR 0272579 (42 #7460)

80. G. van der Geer, *Hilbert modular surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 16, Springer-Verlag, Berlin, 1988. MR 930101 (89c:11073)

81. G. van der Geer and B. Moonen, *Abelian varieties*, In preparation, http://staff.science.uva.nl/~bmoonen/boek/BookAV.html.

82. A. Vasiu, *Crystalline boundedness principle*, Ann. Sci. École Norm. Sup. (4) **39** (2006), no. 2, 245–300. MR 2245533 (2007d:14081)

83. ———, *Reconstructing p-divisible groups from their truncation of smaller level*, 2006, arXiv:math/0607268.

84. W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer-Verlag, New York, 1979. MR 547117 (82e:14003)

85. W. C. Waterhouse and J. S. Milne, *Abelian varieties over finite fields*, 1969 Number Theory Institute, State Univ. New York, Stony Brook, N.Y., 1969), Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R.I., 1971, pp. 53–64. MR 0314847 (47 #3397)

86. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948. MR 0027151 (10,262c)

87. ———, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946), Hermann & Cie., Paris, 1948. MR 0029522 (10,621d)

88. C.-F. Yu, *On reduction of Hilbert-Blumenthal varieties*, Ann. Inst. Fourier (Grenoble) **53** (2003), no. 7, 2105–2154. MR 2044169 (2005h:14062)

89. ———, *On the supersingular locus in Hilbert-Blumenthal 4-folds*, J. Algebraic Geom. **12** (2003), no. 4, 653–698. MR 1993760 (2004g:14044)

90. Ju. G. Zarhin, *Isogenies of abelian varieties over fields of finite characteristic*, Mat. Sb. (N.S.) **95(137)** (1974), 461–470, 472, English translation: *Math. USSR Sbornik* **24** (1974), 451–461. MR 0354685 (50 #7162b)

91. ———, *A remark on endomorphisms of abelian varieties over function fields of finite characteristic*, Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), 471–474, English translation: *Math. USSR-Izv.* **8** (1974), 477–480.

92. T. Zink, *de Jong-Oort purity for p-divisible groups*, preprint, http://www.mathematik.uni-bielefeld.de/~zink/z_publ.html.

93. ———, *Cartiertheorie kommutativer formaler Gruppen*, Teubner-Texte zur Mathematik [Teubner Texts in Mathematics], vol. 68, BSB B. G. Teubner Verlagsgesellschaft, Leipzig, 1984, With English, French and Russian summaries. MR 767090 (86j:14046)

94. ———, *On the slope filtration*, Duke Math. J. **109** (2001), no. 1, 79–95. MR 1844205 (2003d:14055)

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, U.S.A.

E-mail address: chai@math.upenn.edu

URL: http://www.math.upenn.edu/~chai/

Mathematisch Instituut, Budapestlaan 6, NL - 3584 CD TA Utrecht, The Netherlands

Current address: Postbus 80010,NL - 3508 TA Utrecht

E-mail address: F.Oort@uu.nl

URL: http://www.math.uu.nl/people/oort/