Moduli of abelian varieties and p-divisible groups:
Density of Hecke orbits, and a conjecture by Grothendieck

Ching-Li Chai[1] & Frans Oort
VII-2006

Conference on Arithmetic Geometry,
Göttingen 17 July - 11 August 2006.
Informal notes, not for publication.

In the week 7 – 11 August 2006 we give a course, and here are notes for that course. Our main topic will be: *geometry and arithmetic of $\mathcal{A}_g \otimes \mathbb{F}_p$, the moduli space of polarized abelian varieties in positive characteristic.* We illustrate properties of these topics, and available techniques by treating two topics:

Density of ordinary Hecke orbits

and

A conjecture by Grothendieck on deformations of p-divisible groups.

Program:

Lecture 1. Frans Oort – *Introduction:* *Hecke orbits, and the Grothendieck conjecture.*	Monday.1
Lecture 2. Ching-Li Chai – – *Serre-Tate theory.*	Monday.2
Lecture 3. Frans Oort – – *The Tate-conjecture: ℓ-adic and p-adic.*	Tuesday.1
Lecture 4. Ching-Li Chai – – *Dieudonné modules and Cartier modules.*	Tuesday.2
Lecture 5. Frans Oort – *Cayley-Hamilton:* – *a conjecture by Manin and the weak Grothendieck conjecture.*	Wednesday.1
Lecture 6. Ching-Li Chai – – *Hilbert modular varieties.*	Wednesday.2
Lecture 7. Frans Oort – – *Deformations of p-divisible groups to $a \leq 1$.*	Thursday.1
Lecture 8. Frans Oort – – *Proof of the Grothendieck conjecture.*	Friday.1
Lecture 9. Ching-Li Chai – – *Proof of the density of ordinary Hecke orbits.*	Friday.2

[1]Partially supported by a grant DMS04-00482 from the National Science Foundation

We are going to present proofs of two recent results. The main point is that the *methods* used for these proofs are interesting. The main emphasis of our talks will be to present 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 seems that we are at a loss in positive characteristic. However the opposite is true. Phenomena, only occurring 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. It is about these tools in positive characteristic that will be the focus of our talks.

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 an 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 of our talks is that we have chosen certain central topics, and for those we will take 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 it concerns 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. Please notify us if something is not clear enough. We write:

$\boxed{\textbf{BB}}$ A Black Box, please accept that this result is true.

$\boxed{\textbf{Th}}$ This is one of the central results, and we will explain.

$\boxed{\textbf{Extra}}$ This is a result, which is interesting, but which will not be discussed in the course.

Notation to be used will be explained in Section 10; please consult that section every time before we start. In order to be somewhat complete we will gather related interesting other results and questions and conjectures in Section 11.

§1. Introduction: Hecke orbits, and the Grothendieck conjecture

In this section I will discuss the two theorems we are going to prove in this course. I will give the relevant definitions, and try to make the statements clear.

Hecke orbits.

(1.1) An abelian variety A of dimension g over a field K is called *ordinary* if

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

More generally,

$$\text{the number } f \text{ such that } \#\left(A[p](k)\right) = p^f \text{ is called the } p\text{-rank of } A,$$

and $f = g$ is the case of ordinary abelian varieties.

We say an elliptic curve E is *supersingular* if it is not ordinary. Equivalently: E is supersingular if $E[p](k) = 0$. This terminology stems from Deuring; explanation: an elliptic curve in characteristic zero is said to determine a *singular* j-value if the endomorphism ring over an algebraically closed field is larger than $\mathbb{Z}$, in fact of rank 2 over $\mathbb{Z}$; a *supersingular* elliptic curve E over k has $\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}(E)) = 4$.

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 condition will be given later, and more explanation will follow as soon as we have Dieudonné modules and the theory of Newton polygons at our disposal, see Section 4.

Note that $f(A) = 0$ does not imply the abelian variety is supersingular in case $\dim(A) \geq 3$.

Let A and B be abelian varieties over a field K. A $\mathbb{Q}$-isogeny, also called a *quasi-isogeny*, from A to B, is an element of $\mathrm{Hom}(A, B)\otimes_{\mathbb{Z}}\mathbb{Q}$; any element $\phi \in \mathrm{Hom}(A, B)\otimes_{\mathbb{Q}}$ can be realized by a diagram $A \stackrel{\alpha}{\leftarrow} C \stackrel{\beta}{\rightarrow} B$ where α, β are isogenies of abelian varieties. Let p, ℓ be prime numbers. We define a $\mathbb{Z}_{(p)}$-isogeny (resp. $\mathbb{Z}[1/\ell]$-isogeny) to be an element of $\mathrm{Hom}(A, B)\otimes_{\mathbb{Z}} Z_{(p)}$ (resp. an element of $\mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} Z[1/\ell]$); such an element can be realized by a diagram $A \stackrel{\alpha}{\leftarrow} C \stackrel{\beta}{\rightarrow} B$ where α and β are isogenies such that there exists an integer N which is relatively prime to p (resp. a power of ℓ) and $N \cdot \mathrm{Ker}(\alpha) = N \cdot \mathrm{Ker}(\beta) = 0$. In the above $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at the prime ideal $(p) = p\mathbb{Z}$; i.e. $\mathbb{Z}_{(p)}$ consists of rational numbers whose denominators are relatively prime to p.

(1.2) Definition. Let $\Gamma \subset \mathbb{Q}$ be a subring. We say that $\psi : A \to B$ is a Γ-isogeny between abelian varieties A and B if there exists an isogeny $\psi' : A \to B$ and an element γ *inGamma* such that $\psi' = \gamma{\cdot}\psi$.

A $\mathbb{Q}$-isogeny usually is called a quasi-isogeny. Note that $\gamma{\cdot}\psi = \psi{\cdot}\gamma$.

(1.3) Definition. Let $[(A, \lambda)] = x \in \mathcal{A}_g$ be the moduli point of a polarized abelian variety over a field K. We say $[(B, \mu)] = y$ is in the Hecke orbit of x if there exists a field Ω,

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

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

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: $y \in \mathcal{H}^{(p)}(x)$.

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

Remark. We have given the definition of the so-called Sp_{2g}-Hecke-orbit. On can also define the (slightly bigger) $\mathrm{CSp}_{2g}(\mathbb{Z})$-Hecke-orbits by the usual Hecke correspondences, see [27], VII.3, also see 1.6 below,

$$\mathcal{H}^{\mathrm{Sp}}(x) = \mathcal{H}(x) \subset \mathcal{H}^{\mathrm{CSp}}(x).$$

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

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

where $[(B,\mu)] = y$ and $[(A,\lambda)] = x$.

Remark. Suppose $y \in \mathcal{H}^{(p)}(x)$ and suppose $\deg(\lambda) = \deg(\mu)$; then $\deg(\varphi)$ and $\deg(\psi)$ are not divisible by p, which explains the terminology "prime-to-p".

Remark. The diagrams which define $\mathcal{H}(x)$ as above give representable correspondences between components of the moduli scheme; these correspondences could be denoted by Sp-Isog, whereas the correspondences considered in [27], VII.3 could be denoted by CSp-Isog.

(1.4) Remark/Exercise. (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 (dense in the classical topology, dense in the Zariski topology).

(1.5) 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. Note that every elliptic curve has a unique principal polarization.
(1) **Remark.** *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, 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 of proving 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; conclude $\mathcal{H}(x)$ is dense in $\mathcal{A}_1$.

Remark. More generally in fact, as we see in [8], Proposition 1 on page 448: $\mathcal{H}_\ell(x) \cap \mathcal{A}_{g,1}$ *is finite if and only if* $[(A,\lambda)] = x \in \mathcal{A}_g$ *where* A *is supersingular.*
Remark. For elliptic curves we have defined (supersingular)$\Leftrightarrow$ (non-ordinary). For $g = 2$ on can see that (supersingular) $\Leftrightarrow$ $(f = 0)$. However, see Section 4, we can define supersingular as those abelian varieties where the Newton polygon has all slopes equal to 1/2; for $g > 2$ there do exist abelian varieties of p-rank zero which are not supersingular.

(1.6) A bigger Hecke orbit. We define the notion of CSp-Hecke orbits. 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 $\varphi : A \to B$ 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 morphisms $\mathrm{Isog}_g \subset \mathcal{A}_g \times \mathcal{A}_g$ on $\mathcal{A}_g$, also see [27], 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; notation $\mathcal{H}^{\mathrm{Sp}}(x)$ (resp. $\mathcal{H}^{(p)}_{\mathrm{Sp}}(x)$, resp. $cH_\ell^{\mathrm{CSp}}(x)$.) Note that $\mathcal{H}^{\mathrm{CSp}}(x) \supset \mathcal{H}(x)$. This slightly bigger Hecke orbit will play no role in this course. However it is nice to see the relation between the Hecke orbit 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.

(1.7) Theorem $\boxed{\textbf{Th}}$ **(Density of ordinary Hecke orbits.)** *Let* $[(A,\lambda)] = x$ *be the moduli point of a polarized* ordinary *abelian variety. Let* ℓ *be a prime number different from* p*. The Hecke-*ℓ*-orbit* $\mathcal{H}_\ell(x)$ *is dense in* $\mathcal{A}_{g,1}$*:*

$$(\mathcal{H}_\ell(x) \cap \mathcal{A}_{g,1})^{\mathrm{Zar}} = \mathcal{A}_{g,1}.$$

From this we conclude: $\mathcal{H}(x)$ *is dense in* $\mathcal{A}_g$*.*

See Theorem 9.1. This theorem was proved by Ching-Li Chai in 1995, see [8], Theorem 2 on page 477. Although CSp-Hecke orbits was used in [8], the same argument works for Sp-Hecke orbits as well. In our course we will present a proof of this theorem; we will follow [8] partly, but also present 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 [9] as long as [15] is not yet available.

(1.8) Exercise. (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 pull back of λ to E', hence μ has degree ℓ^2, and let $\mu' = \mu/\ell^2$, hence μ' is a principal polarization on E'. *Remark that* $[(E',\mu')] \in \mathcal{H}(x)$*. Show that* $[(E',\mu')] \notin \mathcal{H}^{\mathrm{Sp}}(x)$*.*

(1.9) Exercise. 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

$\mathcal{A}_1$.

(1.10) Theorem (Duality theorem for abelian schemes, see [67], Theorem 19.1) *Let* $\varphi : B \to A$ *be an isogeny of abelian schemes. Then we obtain an exact sequence*

$$0 \quad \to \quad \mathrm{Ker}(\varphi)^D \quad \longrightarrow \quad A^t \quad \xrightarrow{\varphi^t} \quad B^t \quad \to \quad 0.$$

(1.11) An example. Write $\mu_s = \mathrm{Ker}(\times s : \mathbb{G}_m \to \mathbb{G}_m)$ for every $s \in \mathbb{Z}_{>0}$. It is not difficult to see that $(\mu_p)^D = \underline{\mathbb{Z}/p}$, and in fact, $(\mu_{p^b})^D = \underline{\mathbb{Z}/p^b}$.
Conclusion. *For an ordinary abelian variety A over k, we have*

$$A[p] \quad \cong \quad ((\mu_p)^g) \times \left((\underline{\mathbb{Z}/p})^g\right).$$

In fact, by definition we have that $A[p](k) \cong (\mathbb{Z}/p)^g$. This implies that $(\underline{\mathbb{Z}/p^b})^g \subset A$. By the duality theorem we have $A[p]^D \subset A^t$. Hence $(\mu_{p^b})^g \subset A^t$. As A admits a polarization we have an isogeny $A \sim A^t$. We conclude that $(\mu_p)^g \subset A$. Hence the result. $\square$

Note that for an ordinary abelian variety A over an arbitrary field K the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ acts on $A[p]^{\mathrm{loc}}$ and on $A[p]^{\mathrm{et}} = A[p]/A[p]^{\mathrm{loc}}$, and these actions need not be trivial. Moreover if K is not perfect, the extension $0 \to A[p]^{\mathrm{loc}} \to A[p] \to A[p]^{\mathrm{et}} \to 0$ need not be split; this will be studied extensively in Section 2.

(1.12) Reminder. Let N be a finite group scheme over a field K suppose that the rank of N is is prime to the characteristic of k. Then N is etale over K; e.g. see [65].

(1.13) (1) Write Isog = Sp-Isog. Consider a component I of Isog_g defined by diagrams as in 1.6 with $\deg(\psi) = b$ and $\deg(\varphi) = c$. If b is not divisible by p, the first projection $\mathcal{A}_g \leftarrow I$ is etale; if c is not divisible by p, then the second projection $I \to \mathcal{A}_g$ is etale.
(2) Consider $\mathrm{Isog}_g^{\mathrm{ord}} \subset \mathrm{Isog}_g$, the largest subscheme (it is locally closed) lying over the ordinary locus (either in the first projection, or in the second projection, that is the same).
Exercise. *The two projections* $(\mathcal{A}_g)^{\mathrm{ord}} \leftarrow \mathrm{Isog}_g^{\mathrm{ord}} \to (\mathcal{A}_g)^{\mathrm{ord}}$ *are both surjective, etale, finite and flat.*
(3) $\boxed{\textbf{Extra}}$ *The projections* $(\mathcal{A}_g) \leftarrow \mathrm{Isog}_g \to (\mathcal{A}_g)$ *are both surjective and proper on every irreducible component of* Isog_g; this follows from [27], VII.4. The previous exercise (2) is not difficult; fact (3) is difficult; it uses the computation in [63].

(1.14) $\boxed{\textbf{BB}}$ In [63] it has been proved: $(\mathcal{A}_g)^{\mathrm{ord}}$ *is dense in* $\mathcal{A}_g$.

(1.15) *We see that for an* ordinary $[(A, \lambda)] = x$ *we have:*

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

Work over k. In fact, consider an irreducible component T of $\mathcal{A}_g$. As proven in [63] there is an ordinary point $y = [(B, \mu)] \in T$. By [59], Corollary 1 on page 2234, we see that there is an isogeny $(B, \mu) \to (A, \lambda)$, where λ is a principal polarization. By (2) in the previous section 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. $\square$

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

(1.16) Theorem $\boxed{\textbf{Extra}}$ (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 locus* $\mathcal{W}_\xi(\mathcal{A}_g \otimes \mathbb{F}_p)$*.*
A proof will be presented in [15].
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 [74] we find a precise conjectural description of the Zariski closure of $\mathcal{H}_\ell(x)$; that conjecture has been proved now, and it implies 1.16.

(1.17) Lemma $\boxed{\textbf{BB}}$ (Chai). *Let* $[(A,\lambda)] = x \in \mathcal{A}_{g,1}$*. Suppose that* A *is supersingular* (i.e. over an algebraically closed field A is isogenous with a product of supersingular elliptic curves, equivalently: all slopes in the Newton polygon $\mathcal{N}(A)$ are equal to $1/2$). *Then*

$$\mathcal{H}^{(p)}(x) \cap \mathcal{A}_{g,1} \quad \textit{is finite.}$$

See [8], Proposition 1 on page 448.
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.

A conjecture by Grothendieck.

(1.18) Definition, p-divisible groups. Suppose given $h \in \mathbb{Z}_{>0}$. Suppose given a base scheme S. Suppose given for every $i \in \mathbb{Z}_{>0}$ a finite, flat group scheme $G_i \to S$ of rank p^{ih}, and inclusions $G_i \subset G_{i+1}$ for every i such that $G_{i+1}[p^i] = G_i$. The inductive system $X = \{G_i \mid i\} \to S$ is called a p-divisible group of height h over S.
The notion of a Barsotti-Tate group, or BT-group, is the same as that of a p-divisible group. For more information see [39], Section 1.

Remark. Note that for every j and every $s \geq 0$ the map $\times p^s$ induces a surjection:

$$G_{j+s} \twoheadrightarrow G_j = G_{j+s}[p^j] \subset G_{j+s};$$

for every i and $s \geq 0$ we have an exact sequence of finite flat group schemes

$$0 \to G_i \longrightarrow G_{i+s} \longrightarrow G_s \to 0.$$

Example. 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).

For p-divisible groups, inductive systems, we define homomorphisms by

$$\mathrm{Hom}(\{G_i\},\{H_j\}) \quad = \quad \lim_{\leftarrow i}\ \lim_{j \rightarrow}\ \mathrm{Hom}(G_i, H_j).$$

Note that a homomorphism $A \to B$ of abelian schemes defines a morphism $A[p^\infty] \to B[p^\infty]$ of p-divisible groups.

(1.19) Discussion. Over any base scheme S (in any characteristic) for an abelian scheme $A \to S$ and for a prime number ℓ invertible on S one can define $T_\ell(A/S)$ as follows. For $i \in \mathbb{Z}_{>0}$ one chooses $N_i := A[\ell^i]$, and we then define $\times\ell : N_{i+1} \to N_i$. This gives a *projective system*, and write

$$T_\ell(A/S) \quad = \quad \{A[\ell^i] \mid i \in \mathbb{Z}_{>0}\} \quad = \quad \lim_{\leftarrow i} A[\ell^i].$$

This is called the ℓ-Tate group of A/S. Any geometric fiber is $T_\ell(A/S)_s \cong (\underline{\mathbb{Z}_\ell}_s)^{2g}$. If S is the spectrum of a field, the Tate-ℓ can be considered as a Galois module of the group $\mathbb{Z}_\ell^{2g}$, see 10.17. *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). Hence 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 $A[p^\infty]$. The first is a twist of a pro-group scheme defined over $\mathbb{Z}$. What can be said in analogy about $A[p^\infty]$? 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.

(1.20) The Serre dual of a p-divisible group. Consider a p-divisible group $X = \{G_i\}$. The exact sequence $G_{j+s}/G_j = G_s$ by Cartier duality, see [67], I.2, defines an exact sequence

$$0 \to G_s^D \longrightarrow G_{j+s}^D \longrightarrow G_j^D \to 0.$$

These are used, in particular the inclusions

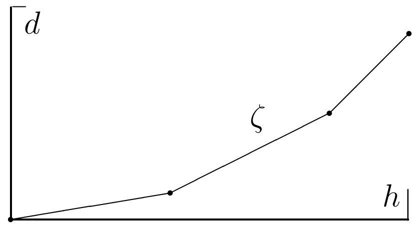
$$G_s^D \hookrightarrow G_{s+1}^D \quad = \quad (G_{s+1} \twoheadrightarrow G_s)^D\,,$$

to define the p-divisible group $X^t = \{G_s^D\}$, called *the Serre dual* of X. Using 1.10 we conclude: $(A[p^\infty])^t = A^t[p^\infty]$ (which is less trivial than notation suggests...).

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

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

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



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

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

Sometimes we will give a Newton polygon by data $\sum_i\ (m_i, n_i)$; here $m_i, n_i \in \mathbb{Z}_{\geq 0}$, with $\gcd(m_i, n_i) = 1$, and $m_i/(m_i + n_i) \leq m_j/(m_j + n_j)$ for $i \leq j$, and $h = \sum_i\ (m_i + n + i)$, $d = \sum_i m_i$. From these data we construct the related Newton polygon by choosing the slopes $m_i/(m_i + n_i)$ with multiplicities $h_i = m_i + n_i$. Conversely clearly any 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 $0 \leq j \leq h$. 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.)

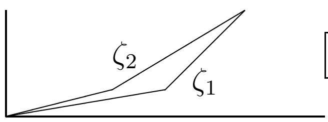
Later we will see: *a p-divisible group X over a field of characteristic p determines uniquely a Newton polygon.* In Section 4 a correct and precise definition will be given; moreover we will see (Dieudonné-Manin) that the isogeny class of a p-divisible group over k uniquely determines (and is uniquely determined by) its Newton polygon.

(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 3.9. 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.

(1.22) Newton polygons go up under specialization. In 1970 Grothendieck observed that " Newton polygons go up" under specialization. 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.



$\boxed{\zeta_1 \succ \zeta_2}$

Note that we use this notation only if Newton polygons with the same endpoints are considered.

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.

(1.23) Later we will show that isogenous p-divisible groups have the same Newton polygon. Using the construction defining a Newton polygon, see Section 4, and using 1.10, we will see that if $\mathcal{N}(X)$ is given by $\{\beta_i \mid 1 \leq i \leq h\}$ then $\mathcal{N}(X^t)$ is given by $\{1-\beta_h, \cdots, 1-\beta_1\}$.

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 [51], page 70; for any base field we can use the duality theorem over any base, see [67] Th. 19.1, also see 1.10.

(1.24) If S is a base scheme, $\mathcal{X} \to S$ 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

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

(1.25) Theorem $\boxed{\textbf{BB}}$ (Grothendieck and Katz; see [48], 2.3.2).

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

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

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

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

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

(1.27) We have seen that "Newton polygons go up under specialization". Does a kind of converse hold? In 1970 Grothendieck conjectured the converse. In [34], the appendix, we find a letter of Grothendieck to Barsotti, and on page 150 we read: "$\cdots$ *The wishful conjecture I have in mind now is the following: the necessary conditions $\cdots$ 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 $\cdots$ we want to know if every sequence of rational numbers satisfying $\cdots$ these numbers occur as the sequence of slopes of a fiber of G as some point of S.*"

(1.28) Theorem $\boxed{\textbf{Th}}$ (**The Grothendieck Conjecture**) (conjectured by Grothendieck, Montreal 1970). *Let K be a field of characteristic p, and let X_0 be a p-divisible group over K. We write $\mathcal{N}(X_0) =: \beta$ for its Newton Polygon. Suppose given a Newton Polygon γ "below" β, i.e. $\beta \prec \gamma$. Then there exists a deformation X_η of X_0 such that $\mathcal{N}(\mathcal{X}_\eta) = \gamma$.*
See §9. This was proved by Frans Oort in 2001. For a proof see [43], [70], [72].

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 series of lectures we will give a proof of this theorem, and we will see that this is an important tool in understanding Newton polygon strata in $\mathcal{A}_g$.

Why is the proof of this theorem difficult? A direct approach seems obvious: write down deformations of X_0, compute Newton polygons of generic 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 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 9.

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 [63].

§2. Serre-Tate theory

In this section we explain the deformation theory of abelian varieties and Barsotti-Tate 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 Barsotti-Tate groups.

(2) In contrast to the deformation theory for general algebraic varieties, the deformation theory for abelian varieties and Barsotti-Tate 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 Barsotti-Tate groups is the same as lifting the Hodge filtration. See Thm. 2.4 for the precise statement, and Thm.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 Barsotti-Tate group. See Thm. 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, 2.15. 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 Thm. 2.20 for the statement. In this case the action on the local moduli space mentioned in (3) above preserve 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 Thm. 2.27 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 Exer. 2.26 as an example of the last sentence.
Barsotti-Tate groups: [52], [39].
Crystalline deformation theory: [52], [4].
Serre-Tate Theorem: [52], [46].
Serre-Tate coordinates: [47].

(2.1) Deformation of abelian varieties and BT-groups: definitions

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 objects of $\mathrm{Art}_{W(K)}$ is a pair (R, j), where R is an Artinian local algebra and $\epsilon : W(K) \to R$ is an 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 $\epsilon : k \to R$ 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

$$\mathrm{SETS}$$

the category whose objects are sets and whose morphisms are isomorphisms of 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, ϵ) of $\mathrm{Art}_{W(K)}$, $\mathrm{Def}(A_0/W(K))(R, \epsilon)$ 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 $\mathrm{Def}(A_0/W(K))$ 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 $R/\mathfrak{m}_R$. Denote by $\mathfrak{Def}((A_0,\lambda_0)/K)$ the restriction of $\mathfrak{Def}(A_0/W(K))$ to the faithful subcategory $\mathfrak{Art}_K$ of $\mathfrak{Art}_{W(K)}$.

Definition. Let X_0 be a Barsotti-Tate group over a perfect field $K \supset \mathbb{F}_p$. Let

$$\mathrm{Def}(X_0/W(K)) : \mathrm{Art}_{W(k)} \to \mathrm{SETS}$$

be the deformation functor of X_0, 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 $(X \to \mathrm{Spec}(R),\epsilon)$, where $X \to \mathrm{Spec}(R)$ is a BT-group over $\mathrm{Spec}(R)$, and

$$\epsilon : X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R/\mathfrak{m}_R) \xrightarrow{\sim} X_0 \times_{\mathrm{Spec}(K)} \mathrm{Spec}(R/\mathfrak{m}_R)$$

is an isomorphism of BT-groups over $R/\mathfrak{m}_R$. Denote by $\mathrm{Def}(X_0/K)$ the restriction of the functor $\mathrm{Def}(X_0/W(K))$ to the faithful subcategory Art_K of $\mathrm{Art}_{W(K)}$.

Suppose that λ_0 is a polarization on X_0, then the deformation functor of (X_0,λ_0) is the functor $\mathrm{Def}((X_0,\lambda_0)/W(K))$ on $\mathrm{Art}_{W(K)}$ which sends an object (R,ϵ) of $\mathrm{Art}_{W(K)}$ to the set of isomorphism classes of pairs $((X,\lambda) \to \mathrm{Spec}(R),\epsilon)$, where $(X,\lambda) \to \mathrm{Spec}(R)$ is a polarized BT-group over $\mathrm{Spec}(R)$, and

$$\epsilon : (X,\lambda) \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R/\mathfrak{m}_R) \xrightarrow{\sim} (X_0,\lambda) \times_{\mathrm{Spec}(k)} \mathrm{Spec}(R/\mathfrak{m}_R)$$

is an isomorphism of polarized BT-groups over $R/\mathfrak{m}_R$. Denote by $\mathrm{Def}((X_0,\lambda_0)/K)$ the restriction of $\mathrm{Def}((X_0,\lambda_0)/W(K))$ to Art_K.

(2.2) Definition. 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 *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 *nilpotent* DP *extension* of a commutative ring R_0 is a nilpotent DP structure $(R,I,(\gamma_i)_{i\in\mathbb{N}})$ together with an isomorphism $R/I \xrightarrow{\sim} R_0$.

(2.3) Remark. 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. An extension of a ring R_0 by a square-zero ideal I is forms a standard "input data" in deformation theory. So we can feed such input data into the crystalline deformation theory summarized in Thm. 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.

(2.4) Theorem $\boxed{\textbf{BB}}$ (Grothendieck-Messing). *Let $X_0 \to \mathrm{Spec}(R_0)$ be an Barsotti-Tate group over a commutative ring R_0.*

(i) *To every nilpotent* DP *extension $(R, I, (\gamma_i)_{i\in\mathbb{N}})$ of R_0 there is a functorially attached locally free R-module $\mathbb{D}(X_0)_R$ 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 nilpotent* DP *extension of R_0. Suppose that $X \to \mathrm{Spec}(R)$ is an Barsotti-Tate 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 BT-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 nilpotent* DP *extension of R_0. Suppose that $A \to \mathrm{Spec}(R)$ is an abelian scheme such that there exist an isomorphism $\beta : A[p^\infty] \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R_0) \xrightarrow{\sim} X_0$ of BT-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 nilpotent* DP *extension of R_0. Denote by $\mathfrak{E}$ the category of 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 and 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 is isomorphic 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 BT-group $X_0 \to \mathrm{Spec}(R_0)$ as a special case of (ii) *above. Then the functor from the category of BT-groups over R lifting X_0 to the category $\mathfrak{E}$ described in* (ii) *is an equivalence of categories.*

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

Proof. Apply Thm. 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 $W(K)$. Apply Thm. 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. □

Remark. From the definition of $\mathrm{Def}(A_0/W(K))$, there is a natural action of $\mathrm{Aut}(A_0)$ on the smooth formal scheme $\mathrm{Def}(A_0/W(K)) \cong \mathrm{Spf}(W(K)[[x_1,\ldots,x_{g^2}]])$.

(2.6) We set up notation for the Serre-Tate theorem 2.7. 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 $S_0 = \underline{\mathrm{Spec}}(\mathcal{O}_S/I)$. 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 Barsotti-Tate group over S, and $\epsilon : X \times_S S_0 \to A_0[p^\infty]$ is an isomorphism of BT-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, $f : X \to X'$ is a homomorphism of BT-groups over S, such that $h[p^\infty] \circ \epsilon) = \epsilon' \circ (f \times_S S_0)$. Let

$$\mathfrak{F} : \mathrm{AV}_S \to \mathrm{AVBT}_{S_0,S}$$

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 $A[p^\infty] \times_S S_0 \xrightarrow{\sim} (A \times_S S_0)[p^\infty]$.

(2.7) Theorem $\boxed{\textbf{BB}}$ (Serre-Tate). *Notation and assumptions as in the above paragraph. Then the functor $\mathfrak{F}$ is an equivalence of categories.*

Remark. A proof of Thm. 2.7 first appeared in print in [52]. See also [46].

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

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

be the functor which sends any object

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

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

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

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

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

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

PROOF. We have $\mathrm{Def}(A_0/W(K)) \cong \mathrm{Def}(A_0[p^\infty]/W(K))$ by by Thm. 2.7. Cor. 2.9 now follows from Cor. 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.

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

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

(2.11) Theorem *We have a canonical isomorphism*

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

with the following properties.

(1) *The composition*

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

is equal to

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

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 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*

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Lie}(A/R)^\vee \arrow[r] \arrow[d, "\cong"] & \mathbb{D}(A_0)_R^\vee \arrow[r] \arrow[d, "\phi_{A_0}"] & (\mathrm{Lie}(A^t/R)^\vee)^\vee \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & \mathrm{Lie}((A^t)^t/R)^\vee \arrow[r] & \mathbb{D}(A_0^t)_R \arrow[r] & \mathrm{Lie}(A^t/R) \arrow[r] & 0
\end{tikzcd}$$

commutes. Here the horizontal exact sequences are as in 2.4, and the left vertical isomorphism is induced by the canonical isomorphism $A \xrightarrow{\sim} (A^t)^t$.

(2.12) Corollary *Let (A_0, λ_0) be a g-dimensional principally polarized abelian variety over a perfect field $K \supset \mathbb{F}_p$. Then deformation functor* $\mathrm{Def}((A_0, \lambda)/W(K))$ *of A_0 is representable by a smooth formal scheme over $W(K)$ of dimensional $g(g{+}1)/2$. This statement 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 $x_0 = [(A_0, \lambda_0, \eta_0)] \in \mathcal{A}_{g,1,n}(K)$. Then the formal completion $\mathcal{A}_{g,1,n}^{/x_0}$ of the moduli space $\mathcal{A}_{g,1,n}^{/x_0} \to \mathrm{Spec}(W(K))$ is non-canonically isomorphic to* $\mathrm{Spf}\,\big(W(K)[[x_1, \ldots, x_{g(g+1)/2}]]\big)$.

The proof follows quickly from Thm. 2.4 and Thm. 2.11, and is left as an exercise.

(2.13) Corollary *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* $x_0 = [(A_0, \lambda_0, \eta_0)] \in \mathcal{A}_{g,d,n}(K)$. *Then 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* $\mathrm{Def}((A_0, \lambda_0)/W(K))$.

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

(2.15) Corollary *Let* (A_0, λ_0) *be a polarized abelian variety over a perfect field* $K \supset \mathbb{F}$. *Let* $\mathrm{Aut}((A_0, \lambda_0)[p^\infty])$ *be 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* $\lambda_0[p^\infty]$. *Then the natural action in* Cor. 2.14 *induces a natural action of on the closed formal subscheme* $\mathrm{Def}(A_0, \lambda_0)$ *of* $\mathrm{Def}(A_0)$.

(2.16) ETALE AND MULTIPLICATIVE BT-GROUPS: NOTATION

Remark. Let $E \to S$ be an Barsotti-Tate group, where S is a scheme. Then 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_{et} whose rank is equal to $\mathrm{ht}(E/S)$. When S is the spectrum of a field K, $\mathrm{T}_p(E)$ "is" a free $\mathbb{Z}_p$-module with an action by $\mathrm{Gal}(K^{\mathrm{sep}}/K)$.

Remark. Attached to any multiplicative Barsotti-Tate 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 Barsotti-Tate group over S. Both $X^*(T)$ and $X_*(T)$ are smooth $\mathbb{Z}_p$-sheaves of rank $\dim(T/S)$ on S_{et}, and they are naturally dual to each other.

(2.17) Definition. 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 $\mathcal{O}_S$. An Barsotti-Tate 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) Barsotti-Tate group. Such an exact sequence is unique up to unique isomorphisms.

Remark. If $S = \mathrm{Spec}(K)$, K is a perfect field of characteristic p, and X is an ordinary Barsotti-Tate group over K, then there exists a unique splitting of the short exact sequence $0 \to T \to X \to E \to 0$ over K.

(2.18) Proposition $\boxed{\text{BB}}$ *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 BT-group such that $X \times_S S_0$ is ordinary, then $X \to S$ is ordinary.*

(2.19) We set up notation for Thm. 2.20 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 Barsotti-Tate 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) Barsotti-Tate group over K. Let $T_i \to \mathrm{Spec}(W(K)/p^iW(K))$ (resp. $E_i \to \mathrm{Spec}(W(K)/p^iW(K)))$ be the multiplicative (resp. étale) BT-group over $\mathrm{Spec}(W(K)/p^iW(K))$ 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 $\tilde{T} \to \mathrm{Spec}(W(K))$ (resp. $\tilde{E} \to \mathrm{Spec}(W(K)))$ over $W(K)$. Denote by $\hat{T}$ the formal torus over $W(K)$ attached to T_0; i.e. $\hat{T} = X_*(T_0) \otimes_{\mathbb{Z}_p} \widehat{\mathbb{G}_m}$, where $\widehat{\mathbb{G}_m}$ is the formal completion of $\mathbb{G}_m \to \mathrm{Spec}(W(K))$ along its unit section.

(2.20) Theorem *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 BT-group over R. Therefore X sits in the middle of an exact sequence*

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

(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 BT-group*

$$\left(\tilde{T} \times_{\mathrm{Spec}(W(K))} \tilde{E}\right) \times_{\mathrm{Spec}(W(K))} \mathrm{Spec}(R)$$

over R.

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

$$\begin{aligned}\mathrm{Def}(X_0/W(K)) \xleftarrow{\sim} \underline{\mathrm{Hom}}_{\mathbb{Z}_p}(\mathrm{T}_p(E_0), \hat{T}) &= \mathrm{T}_p(E)^\vee \otimes_{\mathbb{Z}_p} X_*(T_0) \otimes_{\mathbb{Z}_p} \widehat{\mathbb{G}_m} \\ &= \underline{\mathrm{Hom}}_{\mathbb{Z}_p}\left(\mathrm{T}_p(E_0) \otimes_{\mathbb{Z}_p} X^*(T_0), \widehat{\mathbb{G}_m}\right)\,.\end{aligned}$$

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 Prop. 2.18, 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, $\mathfrak{Def}(X_0/W(K))(R)$ is the set of isomorphism classes of extensions of $\tilde{E} \times_{W(K)} \mathrm{Spec}(R)$ by $\tilde{T} \times_{W(K)} \mathrm{Spec}(R)$. 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 $\varprojlim_n \mathrm{Ext}^1_{\mathrm{Spec}(R)}(p^{-n}\mathbb{Z}/\mathbb{Z}, \mu_{p^n})$. By Kummer theory, we have

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

the second equality follows from the hypothesis that K is perfect. 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

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

is an isomorphism. □

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

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

(2.22) Exercise 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 Barsotti-Tate group such that the closed fiber $X_0 := X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(k)$ is an ordinary BT-group over k. Denote by $q(X/R;\cdot,\cdot)$ the $\mathbb{Z}_p$-bilinear map

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

correspond to the deformation $X \to \mathrm{Spec}(R)$ of the BT-group X_0 as in Cor. 2.21. Here we have used the natural isomorphism $X^*(X_{0\mathrm{mult}}) \cong \mathrm{T}_p(X^t_{0\mathrm{et}})$, so that the Serre-Tate coordinates for the BT-group $X \to \mathrm{Spec}(R)$ is a $\mathbb{Z}_p$-bilinear map $q(X/R;\cdot,\cdot)$ on $\mathrm{T}_p(X_{0\mathrm{et}}) \times \mathrm{T}_p(X^t_{0\mathrm{et}})$. The 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 $\mathrm{can}_* : \mathrm{T}_p(X_{0\mathrm{et}}) \xrightarrow{\sim} \mathrm{T}_p((X_0^t)^t_{\mathrm{et}})$ 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 2.23. The proof is left as an exercise.

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

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

The same statement hold when the ordinary BT-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 2.20, it is not difficult to verify the following.

(2.24) Proposition *Let X_0, Y_0 be ordinary BT-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*

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

(2.25) Corollary *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*

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

where

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

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

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

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

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 $X = \mathrm{Hom}_k(\widehat{\mathbb{G}}_m, T) \cong \mathbb{Z}_p^n$ be the cocharacter group of T; notice that $\mathrm{GL}(X)$ operates naturally on T. Let G be a reductive linear algebraic subgroup of $\mathrm{GL}(X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \cong \mathrm{GL}_n$ 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 Thm. 6.6 of [12] for a proof of 2.27; see also [11].

(2.28) Corollary *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 $\mathcal{H}^{(p)}_{\mathrm{Sp_{2g}}}(x_0)$ on $\mathcal{A}_{g,1,n}$. Then 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 2.27 and the local stabilizer principal; see 9.5 for the statement of the local stabilizer principal.

§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 like to tell more than we really need.
Basic references: [88] and [37]; [87], [41], [66].

(3.1) let A be an abelian variety over a field K. The ring $\mathrm{End}(A)$ is an algebra over $\mathbb{Z}$, which has no torsion, and which is free of finite rank as $\mathbb{Z}$-module. We write $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. 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

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

called the *Rosati-involution.* In case μ is a principal polarization this maps $\mathrm{End}(A)$ into itself.

The Rosati involution is *positive definite* on $D := \mathrm{End}^0(A)$, meaning that $x \mapsto \mathrm{Tr}(x \cdot x^\dagger)$ is positive definite quadratic form on $\mathrm{End}^0(A)$. Such algebras have been classified by Albert, see 10.4.

(3.2) Definition. *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), *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 $\psi(L) \not\subset \mathbb{R}$).
Remark. The quadratic extension L/L_0 gives an involution $\iota \in \mathrm{Aut}(L/L_0)$. For every embedding $\psi : L \to \mathbb{C}$ this involution corresponds with the restriction of complex conjugation on $\mathbb{C}$ to $\psi(L)$.

See 10.5 for details on the definition "sufficiently many Complex Multiplications".

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

(3.3) Theorem (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* $\mathrm{End}^0(A)$.
See [87], [88], see 10.7. In particular this implies the following.

Let A be an abelian variety over $\mathbb{F} = \overline{\mathbb{F}_p}$. Suppose that A is simple, and hence that $\mathrm{End}^0(A)$ is a division algebra; this algebra has finite rank over $\mathbb{Q}$. Then

- either A is a supersingular elliptic curve, and $D := \mathrm{End}^0(A) = \mathbb{Q}_{p,\infty}$, 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).

(3.4) Corollary. *Let A be an abelian variety over $\mathbb{F} = \overline{\mathbb{F}_p}$. Then 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 $\dim_{\mathbb{Q}}(E) = \dim(A)$.*

Some 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 $\mathrm{IV}(e_0, d)$ with $e_0 > 1$ can appear. For example, see [88], page 67: for any prime number $p > 0$, and for any $g > 1$ 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) 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 $\dagger : D \to D$ anti-involution. Suppose a characteristic is given. Then there exists a field k of that characteristic, and an abelian variety A over k such that $\mathrm{End}^0(A) \cong D$, 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 [86], Theorem 5. In general this was proved by Gerritzen, see [31], for more references see [68].

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 properties of $\dim(A)$. However the answer to this question in positive characteristic is not yet complete.

(3.6) Weil numbers and CM-fields. Definition. *Let p be a prime number, $n \in \mathbb{Z}_{>0}$; write $q = p^n$. A q-Weil 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: $\pi \quad \sim \quad \pi'$. We write $W(q)$ for the set conjugacy classes of q-Weil numbers.

(3.7) Proposition. *Let π be a q-Weil number. Then*
(I) *either for at least one $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\psi(\pi) \in \mathbb{R}$; in this case we have:*
(Ie) *a is even, $\sqrt{q} \in \mathbb{Q}$, and $\pi = +p^{n/2}$, or $\pi = -p^{n/2}$; or*
(Io) *a 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.

(3.8) Remark. We see a characterization of q-Weil numbers:

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

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 q-Weil numbers.

(3.9) Let K be a finite field, let A be an abelian variety over K. Suppose $K = \mathbb{F}_q$ with $q = p^n$. We have $F : A \to A^{(p)}$. 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.

(3.10) Theorem $\boxed{\textbf{Extra}}$ (Weil). *Let $K = \mathbb{F}_q$ be a finite field, let A be a simple abelian variety over K. Then π is a q-Weil number.*
This is the famous "Weil conjecture" for an abelian variety over a finite field.
See [93], page 70; [94], page 138; [59], Theorem 4 on page 206.

(3.11) Exercise. We indicate in which way this theorem, part of *the Weil conjecture for an abelian variety* can be proved.

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

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

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

One proof can be found in [59], formula (i) on page 206; also see [16], Coroll. 19.2 on page 144.

Another proof of (I) can be given by duality:

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

From this we see that

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

where we make the shorthand notation F^n for the n times iterated 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 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 [59], Th. 1 on page 192, see [16], Th. 17.3 on page 138.

Give a proof of Theorem 3.10. Suggestion: use Proposition I and Proposition II.

Note that part of the exercise is: *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 induces complex conjugation on L (on every embedding $L \hookrightarrow \mathbb{C}$).*

(3.12) Remark. 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 [88], Th. 1. See 10.7.

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

$$\{\textit{abelian variety over } \mathbb{F}_q\}/{\sim_{\mathbb{F}_q}} \quad \xrightarrow{\sim} \quad W_q/\sim$$

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

(3.14) Let π be a Weil q-number. Let $\mathbb{Q} \subset L \subset D$ be the central algebra determined by π. We remind the reader that

$$[L : \mathbb{Q}] =: e, \quad [D : L] =: d^2, \quad 2g := e{\cdot}d. \qquad \text{See 10.2.}$$

As we have seen in Proposition 3.7 there are three possibilities:

($\mathbb{R}$e) *Either $\sqrt{q} \in \mathbb{Q}$, 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, $\mathrm{End}^0(A)$ 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

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

($\mathbb{R}$o) *Or $q = p^n$ with n an* **odd** *positive integer and $\sqrt{q} \notin \mathbb{Q}$.* $\boxed{\text{Type III(2)}, \quad g = 2}$
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 $\mathrm{End}(A) = \mathrm{End}(A \otimes K')$. If $K \subset K'$ is an extension of even degree $A \otimes K'$ is non-simple, it is K'-isogenous with a product of two supersingular elliptic curves, and $\mathrm{End}^0(A \otimes K')$ is a 2×2 matrix algebra over $\mathbb{Q}_{p,\infty}$, and

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

($\mathbb{C}$) *For at least one embedding $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $\psi(\pi) \notin \mathbb{R}$.* $\boxed{\mathrm{IV}(e_0, d), \quad g := e_0{\cdot}d}$
In this case all conjugates of $\psi(\pi)$ are non-real. We can determine $[D : L]$ knowing all $v(\pi)$ by 10.7 (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 $\mathrm{IV}(e_0, d)$. For $K = \mathbb{F}_q \subset K' = \mathbb{F}_{q^m}$ we have

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

(3.15) Exercise/Remark. 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 [88], page 98. *This gives a proof of a conjecture by Manin,* see 5.19.

(3.16) ℓ-adic monodromy. (Any characteristic.) Let K be a base field, 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 $T_\ell(A) = \lim_{\leftarrow j} A[\ell^j]$ can be considered as a group isomorphic with $(\mathbb{Z}_\ell)^{2g}$ with a continuous G_K-action.

(3.17) Theorem $\boxed{\textbf{Extra}}$ (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 [87]. The case of function field in characteristic p was proved by Zarhin and by Mori, see [98], [99], [56]; also see [55], 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 [25]. For the case of a function field in characteristic zero, see [28], Th. 1 on page 204.

(3.18) Remark. $\boxed{\textbf{Extra}}$ 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.XXcheck this, give example:XX
Example. *There exists a finite extension $L \supset \mathbb{Q}_p$ and anabelian variety over L such that*

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

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 [54].

(3.19) We like to have a p-adic analogue of 3.17. 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.

(3.20) Theorem $\boxed{\textbf{Th}}$ & $\boxed{\textbf{BB}}$ (Tate, 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 (uniquely) $\beta : X \to Y$ 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 [41], 1.2 and [42], Th. 2 on page 261.

(3.21) Theorem (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*

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

is an isomorphism.
This was proved by Tate in case K is a finite field; a proof was written up in [92]. The case of a function field over $\mathbb{F}_p$ was proved by Johan de Jong, see [41], Th. 2.6. We will see that this case follows from the result by Tate and from the proceeding result on extending homomorphisms 3.20.

(3.22) Ekedahl-Oort strata. $\boxed{\textbf{BB}}$ In [71] a new technique is developed, which will be used below. We sketch some of the datails of that method. we will only indicate detaios relevant for the polarized case (and leaving 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 Barsotti-Tate group scheme trucated 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 isomorphisms classes of BT_1 group schemes is finite. Any $A[p]$, for an abelian variety is a BT_1 groups 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 (there are subtleties in case $p = 2$), see [71], Section 9.

3.22.1 *The number of isomorphism classes of polarized BT_1 group schemes* $(N, [,])$ *over k of given rank is finite; see the classification in* [71], 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 $(A, \lambda)[p]$ is geometrically belongs to the isomorphism class φ.

3.22.2 *It can be shown that this is a locally closed set*, called an EO-stratum. We obtain $\mathcal{A}_{g,1} \otimes \sqcup_\varphi \ \ S_\varphi$, a disjoint union of local closed sets. *This is a stratification*, in the sense that *the boundary of a stratum is a union of lowwer dimensional strata.*

On of the main theorems of this theory is that
3.22.3 *for every φ the set S_φ is* quasi-affine (i.e. open in an affine scheme), see [71], 1.2.

The finite set Φ_g of such isomorphism types has two partial orderings, see [71], 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 $S_{\varphi'}$.

(3.23) An application. *Let $x \in \mathcal{A}g, 1$. Let*

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

be the Zariski closure. This closed set $\mathcal{A}_{g,1}$ in contains a supersingular point.
Use 3.22 and 1.17.

§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 Barsotti-Tate 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 Barsotti-Tate groups, which are apparently non-linear in nature, are translated into questions in linear algebras 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 Barsotti-Tate 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.

Remarks on notation: (i) In the first part of this section, on Cartier theory, k denotes a commutative ring with 1, or a commutative $\mathbb{Z}_{(p)}$-algebra with 1. This differs from the convention in the rest of this article that k stands for an algebraically closed field.
(ii) In this section, we used V and F as elements in the Cartier ring $\mathrm{Cart}_p(k)$ or the smaller Dieudonné ring $R_K \subset \mathrm{Cart}_p(K)$ for a perfect field K. In the rest of this article, the notation $\mathcal{V}$ 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 Barsotti-Tate groups over K.

A synopsis of Cartier theory

Let k be a commutative ring with 1 over $\mathbb{Z}_{(p)}$. The main theorem of Cartier theory says that there is an equivalence between the category of commutative smooth formal groups over k and the category of left modules over a non-commutative ring $\mathrm{Cart}_p(k)$ satisfying certain conditions. See 4.27 for a precise statement.

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

$$\sum_{m,n\geq 0} V^m\langle a_{mn}\rangle F^n\,, \quad a_{mn} \in k\,, \forall\, m\ \exists\, C_m > 0 \text{ s.t. } a_{mn} = 0 \text{ if } n \geq C_m\,.$$

These topological generators satisfy the following commutation relations.

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

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

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

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

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

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

If so, then $\mathrm{Lie}(G/k) \cong M/VM$, and M is a finitely generated $\mathrm{Cart}_p(k)$-module. See 4.18 for the definition of $\mathrm{Cart}_p(k)$, 4.19 for the commutation relations in $\mathrm{Cart}_p(k)$, and 4.23 for some other properties of k. We strongly advice the readers with no prior experience with Cartier theory to accept the "big black box" as described in the previous paragraph and use the materials in 4.1 – 4.27 as a dictionary only when necessary. Instead, it would be more helpful to get familiar first with the structure of the ring $\mathrm{Cart}_p(k)$ in the case when $k \supset$ is a perfect field and 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.

References for Cartier theory. We highly recommend [100], where the approach in §2 of [83] is fully developed. Other references for Cartier theory are [49] and [36].

(4.1) Definition. Let k be a commutative ring with 1.

(1) Let $\mathfrak{Nilp}_k$ be the category of all nilpotent k-algebras, consisting of all commutative k-algebras N without unit such that $N^n = (0)$ for some positive integer n.

(2) A *commutative smooth formal group* over k is a covariant functor $G : \mathfrak{Nilp}_k \to \mathfrak{Ab}$ from $\mathfrak{Nilp}_k$ 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 $\mathfrak{Nilp}_k$ 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 $\mathfrak{Nilp}_k$ whose underlying k-module is k, and $N_0^2 = (0)$.

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

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

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

Then the functor which sends an object N in $\mathfrak{Nilp}_k$ to the abelian group

$$\operatorname{Ker}\left(A(k \oplus N) \to A(k)\right)$$

is a commutative smooth formal group over k, denoted by $\widehat{A}$. For instance we have

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

for all $N \in \operatorname{Ob}(\mathfrak{Nilp}_k)$.

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

$$\Lambda_k(N) = 1 + t\, k[t] \otimes_k N \subset ((k \oplus N)[t])^\times \qquad \forall\; N \in \operatorname{Ob}(\mathfrak{Nilp}_k)\,.$$

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 $(k \oplus N)[t]$ in one variable t.

Remark. (i) The formal group Λ will play the role of a free generator in the category of (smooth) formal groups.
(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 $\lambda(1 + \sum_{i \geq 1} u_i\, t^i)$.

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

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

(4.4) Theorem $\boxed{\textbf{BB}}$ *Let $H : \mathfrak{Nilp}_k \to \mathfrak{Ab}$ be a commutative smooth formal group over k. Let $\Lambda = \Lambda_k$ be the functor defined in 4.2. Then the map*

$$Y_H : \operatorname{Hom}(\Lambda_k, H) \to H(k[[X]]^+)$$

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

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

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 Thm. 4.4.

(4.5) Definition. (i) Define $\mathrm{Cart}(k)$ to be $(\mathrm{End}(\Lambda_k))^{\mathrm{op}}$, the opposite ring of the endomorphism ring of the smooth formal group Λ_k. According to Thm. 4.4, for every weakly symmetric functor $H : \mathfrak{Nilp}_k \to \mathfrak{Ab}$, the abelian group $H(k[[X]]^+) = \mathrm{Hom}(\Lambda_k, H)$ is a *left* module over $\mathrm{Cart}(k)$.
(ii) We define some special elements of the Cartier ring $\mathrm{Cart}(k)$, naturally identified with $\Lambda(k[[X]])$ via the bijection $Y = Y_\Lambda : \mathrm{End}(\Lambda) \xrightarrow{\sim} \Lambda(k[[X]]^+)$ in Thm. 4.4.

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

Corollary. For every commutative ring with 1 we have

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

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

(1) $V_1 = F_1 = 1,\ F_n\,V_n = n.$

(2) $[a]\,[b] = [ab]$ *for all* $a, b \in k$

(3) $[c]\,V_n = V_n\,[c^n],\ F_n\,[c] = [c^n]\,F_n$ *for all* $c \in k,$ *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* $a, b \in k,\ m, n \geq 1.$

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

$$\mathrm{Fil}^j\mathrm{Cart}(k) = \left\{ \sum_{m\geq j}\sum_{n\geq 1} V_m[a_{mn}]F_n \mid a_{mn} \in k,\ \forall\, m \geq j,\ \exists\, C_m > 0 \text{ s.t. } a_{mn} = 0 \text{ if } n \geq C_m \right\}$$

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

Remark. The definition of the Cartier ring gives a functor

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

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

(4.8) Definition. Let k be a commutative ring with 1.

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

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

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 $c \in k$ 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 $\mathrm{Cart}(k)$-module $(M, \mathrm{Fil}^\bullet M)$ is *V-flat* if $M/\mathrm{Fil}^2 M$ is a flat k-module. The k-module $M/\mathrm{Fil}^2 M$ is defined to be the *tangent space* of $(M, \mathrm{Fil}^\bullet M)$.

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

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

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

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

(i) For every integer $m \geq 1$, let $Q_m := \mathrm{Ann}_Q(\mathrm{Fil}^m \mathrm{Cart}(k))$ be the subgroup of Q consisting of all elements $x \in Q$ such that $x \cdot \mathrm{Fil}^m \mathrm{Cart}(k) = (0)$. 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 $Q \otimes_{\mathrm{Cart}(k)} M$.

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* $Q \overline{\otimes}_{\mathrm{Cart}(k)} M$ by

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

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

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

$$\begin{array}{ccc} \{\text{smooth formal groups over } k\} & \xrightarrow{\sim} & \{V\text{-flat } V\text{-reduced left } \mathrm{Cart}(k)\text{-mod}\} \\ G & \longmapsto & \mathrm{M}(G) = \mathrm{Hom}(\Lambda, G) \\ \Lambda \overline{\otimes}_{\mathrm{Cart}(k)} M & \longleftarrow & M \end{array}$$

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

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

(4.12) Definition. (1) The *universal Witt vector group* $\widetilde{W}$ is defined as the functor from the category of all commutative algebras with 1 to the category of abelian groups such that

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

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 $\widetilde{W}(R)$, we use the notation $\omega(1 + \sum_{m\geq 1} u_m\, T^m)$. It is easy to see that every element of $\widetilde{W}(R)$ has a unique expression as

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

Hence $\widetilde{W}$ is isomorphic to $\mathrm{Spec}\,\mathbb{Z}[x_1, x_2, x_3, \ldots]$ 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 $(a_1, a_2, a_3, \ldots)$. In other words, $\omega(\underline{a}) = \omega(\prod_{m\geq 1} (1 - a_m\, T^m))$

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

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

(3) There are two families of endomorphisms of the group scheme $\widetilde{W}$: 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 $\widetilde{W} \times_{\mathrm{Spec}\,\mathbb{Z}} \mathrm{Spec}\, R$. These operators make $\widetilde{W}(k)$ a left $\mathrm{Cart}(k)$-module; they are defined as follows

$$\begin{array}{lclcl} V_n & : & \omega(f(T)) & \mapsto & \omega(f(T^n)) \\ F_n & : & \omega(f(T)) & \mapsto & \sum_{\zeta\in\mu_n} \omega(f(\zeta\, T^{\frac{1}{n}})) \qquad (\text{formally}) \\ [c] & : & \omega(f(T)) & \mapsto & \omega(f(cT)) \end{array}$$

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

(4.13) Exercise. Show that the Cartier module of $\widehat{\mathbb{G}_m}$ over k is naturally isomorphic to $\widetilde{W}(k)$ as a module over $\mathrm{Cart}(k)$.

(4.14) Proposition $\boxed{\textbf{BB}}$ *Let k be a commutative ring with 1.*

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

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

form a subring of $\mathrm{Cart}(k)$.

(ii) *The injective map*

$$\widetilde{W}(k) \hookrightarrow \mathrm{Cart}(k), \qquad \omega(\underline{a}) \mapsto \sum_{n\geq 1} V_n\,[a_n]\,F_n$$

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

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

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

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 $\mathrm{Cart}(k)$ under the canonical ring homomorphism $\mathrm{Cart}(\mathbb{Z}_{(p)}) \to \mathrm{Cart}(k)$ is also denoted by ϵ_p.

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

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

in $\tilde{W}(k)$, 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.

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

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

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

(iii) $\epsilon_p V_n = 0,\ F_n \epsilon_p = 0$ *for all n with $(n,p) = 1$.*

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

(v) $\epsilon_{p,n}\, \epsilon_{p,m} = 0$ *for all $m \neq n$ with $(mn,p) = 1$.*

(vi) $[c]\, \epsilon_p = \epsilon_p\, [c]$ *and* $[c]\, \epsilon_{p,n} = \epsilon_{p,n}\, [c]$ *for all $c \in k$ and all n with $(n,p) = 1$.*

(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 $(n,p) = 1$.*

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

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

(ii) Define elements $F, V \in \mathrm{Cart}_p(k)$ 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 $c \in k$, denote by $\langle c \rangle$ the element $\epsilon_p[c]\epsilon_p = \epsilon_p[c] = [c]\epsilon_p \in \mathrm{Cart}_p(k)$.

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

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

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

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

(4) $FV = p$.

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

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

(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 $a, b \in k$ and all $m, n \in \mathbb{N}$, where $r = \min\{m, n\}$.

(4.20) Definition. Let k 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 $\mathfrak{Nilp}_k$ to $\mathfrak{Ab}$ such that

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

for any nilpotent k-algebra N.

(4.21) Definition. (1) Denote by W_p the image of ϵ_p, i.e. $W_p(R) := \epsilon_p(\widetilde{W}(R))$ 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 $\widetilde{W}(R)$, 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 $\widetilde{W}$ 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 $\widetilde{W}$; 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 $\underline{c} = (c_0, c_1, c_2, \ldots)$.

(4.22) Exercise. Let k 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 k-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 k.

(iii) Prove that every element of $W_p(k)$ 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 $W_p(k)$ to the product ring $\prod_0^\infty k$ defined by

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

is a ring homomorphism.

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

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

$$\sum_{m,n\geq 0} V^m \langle a_{mn} \rangle F^n\,, \quad a_{mn} \in k\,, \forall\, m\ \exists\, C_m > 0 \text{ s.t. } a_{mn} = 0 \text{ if } n \geq C_m$$

in a unique way.

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

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

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

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

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

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

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

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

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

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

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

$$\begin{array}{ccc}
\{\ V\text{-reduced left } \mathrm{Cart}(k)\text{-mod}\} & \xrightarrow{\sim} & \{\ V\text{-reduced left } \mathrm{Cart}_p(k)\text{-mod}\} \\
M & \longmapsto & \epsilon_p M \\
\mathrm{Cart}(k)\epsilon_p\widehat{\otimes}_{\mathrm{Cart}_p(k)}M_p & \longleftarrow & M_p
\end{array}$$

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

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

$$\begin{array}{ccc}
\{\text{smooth formal groups over } k\} & \xrightarrow{\sim} & \{\,V\text{-flat } V\text{-reduced left } \mathrm{Cart}_p(k)\text{-mod}\} \\
G & \longmapsto & M_p(G)=\epsilon_p\,\mathrm{Hom}(\Lambda,G) \\
\Lambda_p\otimes_{\mathrm{Cart}_p(k)}M & \longleftarrow & M
\end{array}$$

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 $W(K)$.

(4.28) Definition. Denote by R_K the 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

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

i.e. elements of $W(K)[V,F]$ are sums of the form $\sum_{i\in\mathbb{Z}} a_iV^i$, 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.

(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 $\sum_{i\in\mathbb{Z}} a_iV^i$ 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 multiplication on $W(K)[V,F]$ extends to $W(K)[[V,F\rangle\rangle$ by continuity.

(4.29) Definition. (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 $a(M) = \dim_K(M/(VM + FM)$.

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

(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 $(\mathbb{Z}/n\mathbb{Z})_S$.

(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 is induced by $X \mapsto X \otimes X$.

(4.31) Theorem $\boxed{\textbf{BB}}$

(1) *There is an equivalence of categories between the category of Barsotti-Tate groups over K and the category of Dieudonné modules over R_K. Denote by $\mathrm{M}_p(X)$ the covariant Dieudonné module attached to a Barsotti-Tate group over K.*

(2) *Let X be a Barsotti-Tate 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 $\hat{X}$ the formal group attached to X, i.e. $\hat{X}$ is the formal completion of X along the zero section of X. Then there is a canonical isomorphism $\mathrm{M}_p(X) \xrightarrow{\sim} \mathrm{M}_p(\hat{X})$ between the Dieudonné module of X and the Cartier module of $\hat{X}$.*

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

(4) *Let X^t be the Serre-dual of the Barsotti-Tate group of X. Then the Dieudonné module $\mathrm{M}_p(X^t)$ can be described in terms of $\mathrm{M}_p(X)$ as follows. The underlying $W(K)$-module is the linear dual $\mathrm{Hom}_{W(K)}(\mathrm{M}_p(X), W(K))$ of $\mathrm{M}_p(X)$. The action of V and F are defined as follows.*

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

for all $h \in \mathrm{Hom}_{W(K)}(\mathrm{M}_p(X), W(K))$ and all $m \in \mathrm{M}_p(X)$.

(5) *A Barsotti-Tate group X over K is étale if and only if $V : \mathrm{M}_p(X) \to \mathrm{M}_p(X)$ is bijective, or equivalently, $F : \mathrm{M}_p(X) \to \mathrm{M}_p(X)$ is divisible by p. A Barsotti-Tate group X over K is multiplicative if and only if $V : \mathrm{M}_p(X) \to \mathrm{M}_p(X)$ is divisible by p, or equivalently, $F : \mathrm{M}_p(X) \to \mathrm{M}_p(X)$ is bijective.*

Remark. See [64] for Thm. 4.31.

(4.32) Proposition $\boxed{\textbf{BB}}$ *Let X be a Barsotti-Tate group over K. We have a natural isomorphism*

$$\mathrm{Hom}_K(\alpha_p, X[p]) \cong \mathrm{M}_p(X)/(V\mathrm{M}_p(X) + F\mathrm{M}_p(X))\,.$$

In particular $\dim_K(\mathrm{Hom}_K(\alpha_p, X[p])) = a(\mathrm{M}_p(X))$. The natural number $a(\mathrm{M}_p(X))$ of a BT-group X over K is zero if and only if X is an extension of an étale BT-group by a multiplicative BT-group.

Definition. The a-number of a Barsotti-Tate group X over K is the natural number

$$a(X) := \dim_K(\mathrm{Hom}_K(\alpha_p, X[p])) = a(\mathrm{M}_p(X))\,.$$

(4.33) Proposition $\boxed{\text{BB}}$ *Let X be a Barsotti-Tate group over a perfect field $K \supset \mathbb{F}_p$. Then there exists a canonical splitting*

$$X \cong X_{\mathrm{mult}} \times_{\mathrm{Spec}(K)} X_{\mathrm{ll}} \times_{\mathrm{Spec}(K)} X_{\mathrm{et}}$$

where X_{et} is the maximal étale quotient of X, X_{mult} is the maximal multiplicative Barsotti-Tate subgroup of X, and X_{ll} is a Barsotti-Tate group with no non-trivial étale quotient nor non-trivial multiplicative Barsotti-Tate subgroup.

Remark. The analogous statement for finite group schemes over K can be found in [51, Chap. 1], from which 4.33 follows. See also [21], [22].

(4.34) Definition. 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 Barsotti-Tate group whose Dieudonné module is

$$\mathrm{M}_p(G_{m,n}) = R_K/R_K \cdot (V^n - F^m)\,.$$

(4.35) Exercise. (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 Barsotti-Tate group $\mathbb{Q}_p/\mathbb{Z}_p$, and $G_{1,0}$ is isomorphic to the multiplicative Barsotti-Tate 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.

(4.36) Theorem $\boxed{\text{BB}}$ *Let $k \supset \mathbb{F}_p$ be an algebraically closed field. Let X be a simple Barsotti-Tate group over k, i.e. X has no non-trivial quotient Barsotti-Tate 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.*

(4.37) Definition. (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 on the plane from $(0, 0)$ to $m + n, m$. The slope sequence of $G_{m,n}$ is the finite sequence $(m/(m + n), \ldots, m/(m + n))$ with $m + n$ entries.
(ii) Let X be a Barsotti-Tate 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 $m_i/(m_i + n_i) \le m_{i+1}/(m_{i+1} + n_{i+1})$ 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 Barsotti-Tate group X over K is étale (resp. multiplicative) if and only if all of its slopes are equal to 0 (resp. 1).

(4.38) Exercise. Suppose that X is a Barsotti-Tate 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. $G_{m,1}$).

(4.39) Exercise. Show that there are infinitely many non-isomorphic Barsotti-Tate groups with slope sequence $(1/2, 1/2, 1/2, 1/2)$. Same for the slope sequence $(1/3, 1/3, 1/3, 2/3, 2/3, 2/3)$.

(4.40) Exercise. Determine all Newton polygons attached to a Barsotti-Tate group of height 6, and the symmetric Newton polygons among them.

Recall that the set of all Newton polygons is a 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.

(4.41) "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 [22]. We will need this theory only in the commutative case. For more general statements see [22], 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 $(F : N \to N^{(p)}) = 0$ is 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. $\boxed{\textbf{BB}}$ *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: $\mathcal{D}_K = \mathrm{M}_p$, with $\mathrm{M}_p(V) = g$.
See [22], II.7.4

Exercise. *Classify all commutative group schemes of rank p over k, an algebraically closed field of characteristic p.*

Classify all commutative group schemes of rank p over a perfect field $K \supset \mathbb{F}_p$.

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

Main reference: [70].

(5.1) For a matrix $\mathcal{F}$ over a *commutative* integral domain R we have the Cayley-Hamilton theorem: *let*

$$\det(\mathcal{F} - T{\cdot}I) =: g \in R[T]$$

be the characteristic polynomial of this matrix; then $g(\mathcal{F}) = 0$, i.e. "a matrix is a zero of its own characteristic polynomial".

(5.2) Exercise. Show the classical Cayley-Hamilton theorem for a matrix over a commutative ring R:

$$\text{let } X \text{ be a } n \times n \text{ matrix with entries in } R;$$
$$\text{let } g = \mathrm{Det}(X - T{\cdot}\mathbf{1}_n) \in R[T]; \text{ the matrix } g(X) \text{ is the zero matrix.}$$

Here are some suggestions for a proof:
(a) For any commutative ring R, and a $n \times n$ matrix X with entries in R there exists a ring homomorphism $\mathbb{Z}[t_{1,1}, \cdots, t_{i,j}, \cdots t_{n,n}] \to R$ such that the matrix $(t) = (t_{i,j} \mid 1 \leq i, j \leq n)$ is mapped to X.
(b) Construct $\mathbb{Z}[t_{i,j} \mid 1 \leq i, j \leq n] \hookrightarrow \mathbb{C}$. Show that the matrix (t) considered over $\mathbb{C}$ has mutually different eigenvalues.
(c) Conclude the theorem for (t), over $\mathbb{C}$ and for (t) over $\mathbb{Z}[t_{i,j} \mid 1 \leq i, j \leq n]$. Conclude the theorem for X over R.
Here are suggestions for a different proof:
(1) Show it suffices to prove this for an algebraically closed field of characteristic zero.
(2) Show 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 very useful analog of this over the Dieudonné ring. Note that over a non-commutative ring there is no reason any straight 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. In general $g(\mathcal{F})$ does not annihilate other elements.

(5.4) Notation. 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 possible.

The group scheme $\alpha_{p,K}$ over a field K corresponds under refnonperfect (in any case) or by Diedonné 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 5.6 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.

(5.5) Exercise. 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.*

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

$$\mathcal{W}_{\mathcal{N}(X_0)}(\mathrm{Def}(X_0)) \textit{ is non-singular.}$$

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 $n \geq 3$).

We see that we can a priori consider a set of points in which we know the Newton polygon stratum is 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.

(5.6) Remark/Exercise. We give an example where $\dim_K(\mathrm{Hom}(\alpha_p, G)) < a(G)$; we see that the condition "L is perfect" is necessary in 5.4 .
(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 4.41. *Show*:

$$\dim_K(\mathrm{Hom}(\alpha_p, N)) = 1, \quad a(N) = 2.$$

(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*

$$N \not\cong_K (\alpha_p \oplus W_2[F]) \otimes K \quad \text{and} \quad N \otimes L \cong_L (\alpha_p \oplus W_2[F]) \otimes L.$$

Remark. In [50], 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.

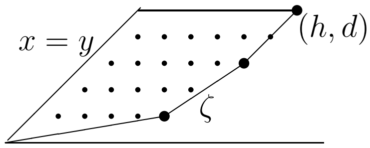
(5.7) We fix integers $h \geq d \geq 0$, and we write $c := h - d$. We consider Newton polygons ending at (h, d). For such a Newton polygon β we write:

$$\diamondsuit(\beta) = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y < d, \quad y < x, \quad (x, y) \prec \beta\};$$

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

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

Example:



$\zeta = 2 \times (1,0) + (2,1) + (1,5) =$
$= 6 \times \frac{1}{6} + 3 \times \frac{2}{3} + 2 \times \frac{1}{1}; \quad h = 11.$
Here $\dim(\zeta) = \#(\diamond(\zeta)) = 22.$

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

(5.8) Theorem (Newton polygon-strata for p-divisible groups). *Suppose $a(X_0) \leq 1$. For every $\beta \succ \gamma = \mathcal{N}(X_0)$ we have: $\dim(V_\beta) = \dim(\beta)$. The strata V_β are nested as given by the partial ordering on Newton polygon, i.e.*

$$V_\beta \subset V_\delta \Longleftrightarrow \diamond(\beta) \subset \diamond(\delta) \Longleftrightarrow \beta \prec \delta.$$

Generically on V_β the fibers have Newton polygon equal to β.
For the notion "generic" for a p-divisible group over a formal scheme, see 10.15.

(5.9) 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

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

We show that

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

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:

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

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 (see the talks by Messing), and by using the following tools.

(5.10) Definition. 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:

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

$a_{i,j} \in W, \quad a_{1,h} \in W^*$; i.e. it consists of blocks of sizes (d or c) $\times$ (d or c); in the left hand upper corner, which is of size $d \times d$, there are entries on 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 element unequal to zero, and it is 1; the right hand upper corner is unspecified, entries are called $pa_{i,j}$; 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 is defined by a matrix in displayed normal form then either the p-rank f is maximal, $f = d$, and this happens iff $a_{1,d}$ is not divisible by p, or $f < d$, and in that case $a = 1$. The p-rank is zero iff $a_{i,d} \equiv 0 \pmod{p}, \quad \forall 1 \leq i \leq d$.

(5.11) Lemma. $\boxed{\textbf{BB}}$ *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 $a_{1,d}, \cdots, a_{d,d}$ are divisible by p, they can be chosen to be equal to zero.

(5.12) Lemma (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 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* 5.10. *We write $e = X_1 = e_1$ for the first base vector. Then for the expression*

$$P := \sum_{i=1}^{d} \sum_{j=d}^{h} p^{j-d} a_{i,j}^{\sigma^{h-j}} \mathcal{F}^{h+i-j-1} \quad \textit{we have} \quad \mathcal{F}^h \cdot e = P \cdot e.$$

Note that we take powers of $\mathcal{F}$ in the σ-linear sense, i.e. if the display matrix is (a), i.e. $\mathcal{F}$ is given by the matrix (pa) as above,

$$\mathcal{F}^n \quad \text{is given by the matrix} \quad (pa) \cdot (pa^\sigma) \cdot \cdots \cdot (pa^{\sigma^{n-1}}).$$

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 $\mathcal{F}e_{s+1} = \left(\sum_{i=1}^{d} p\ a_{i,s+1} F^{i-1} \right) X + pe_{s+2}$. This proves the claim. Computing $\mathcal{F}(\mathcal{F}^{h-1}X)$ gives the desired formula. $\square$

(5.13) Proposition. *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 $W[F]$-sub-module $M' \subset M$ generated by $X = e_1$. Note that M' contains $X = e_1, e_2, \cdots, e_d$. 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 $M' \subset M = \oplus_{i \leq h}\ W{\cdot}e_i$ 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 [51], II.1. also see [21], pp. 82-84. By [21], 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. $\square$

(5.14) Corollary. *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 $d \le h-d$):*

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

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 5.8 proves the following statement.
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 for a closed fiber.*
However we will prove a much stronger result later.

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

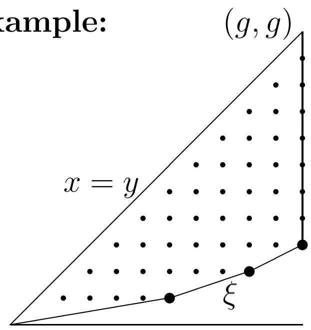
(5.16) We fix an integer g. For every *symmetric* Newton polygon ξ of height $2g$ we define:

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

and we write

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

Example:



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

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

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

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

Suppose given a p-divisible group X_0 over k of dimension g with a principal quasi-polarization. We write $\mathcal{N}(X_0) = \gamma$; this is a symmetric Newton polygon. We write $\mathcal{D} = \mathrm{Def}(X_0, \lambda)$ for the universal deformation space. For every symmetric Newton polygon ξ with $\xi \succ \gamma$ we define $W_\xi \subset \mathcal{D}$ as the maximal closed, reduced formal subscheme carrying all fibers with Newton polygon equal or above ξ; this space exists by Grothendieck-Katz, see [48], Th. 2.3.1 on page 143. Note that $W_\rho = \mathcal{D}$, where $\rho = g{\cdot}((1,0) + (0,1))$.

(5.17) Theorem (NP-strata for principally quasi-polarized formal groups). *Suppose $a(X_0) \leq 1$. For every symmetric $\xi \succ \gamma := \mathcal{N}(G_0)$ we have:* $\dim(W_\xi) = \mathrm{sdim}(\xi)$. *The strata W_ξ 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 $\mathcal{D}$ in which all W_ξ are given by linear equations.

(5.18) Corollary. *Suppose given a principally polarized abelian variety (A_0, λ_0) over k. Strata in $\mathcal{D}ef(X_0, \lambda_0)$ according to Newton polygons are exactly as in 5.17. 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* (for B_ξ, see the proof of 5.17 below; for the notion "generic point of W_ξ " see the proof of 5.18 below; also see 10.15).

Proof. We write $(A_0, \lambda_0)[p^\infty] =: (X_0, \lambda_0)$. By Serre-Tate theory, see [47], 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 [33], 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 over $\mathrm{Spec}(R)$, and we can consider the generic point of $W_\xi \subset \mathrm{Spec}(R)$. Hence the Newton polygon of fibers can be read off from the fibers in $(\mathcal{X}, \lambda) \to \mathrm{Spec}(R)$. This proves that 5.18 follows from 5.17. $\square$

Proof of 5.17. The proof of this theorem is analogous to the proof of 5.8. We use the diagram

$$\begin{array}{ccccccc}
 & & & & & & -1 \\
 & & & T_{g,g} & \cdots & T_{1,g} & \\
 & & . & \vdots & . & & \\
1 & T_{g,1} & \cdots & T_{1,1} & & &
\end{array}$$

Here $X_{i,j}$, $1 \leq i, j \leq g$, 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 5.12 and 5.14 we finish the proof of 5.17 as we did in the proof of 5.8 above. $\square$

(5.19) A conjecture by Manin. Let A be an abelian variety. The Newton polygon $\mathcal{N}(A)$ is symmetric 1.23. A conjecture by Manin expects the converse to hold:
Conjecture, see [51], 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 3.13. *We sketch a pure characteristic p proof.* It is not difficult to show that there exists a principally polarized supersingular abelian variety (A_0, λ_0), see [70], Section 4; this also follows from [50], 4.9. By 5.17 it follows that $\mathcal{W}^0_\xi(\mathrm{Def}(A_0, \lambda_0))$ is non-empty, *which proves the Manin conjecture.* $\square$

§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 $\mathcal{O}_F \hookrightarrow \mathrm{End}(A)$; the terminology "fake elliptic curve" was used by some authors. The moduli space of such objects behave 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 $\mathrm{SL}_2(F \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)})$ or $\mathrm{GL}_2(\mathbb{A}_f^{(p)})$ 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 plays 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 a 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. [80], [19], [29] Chap X, [20], [32], [96].

Let $F_1, \ldots, F_r$ are 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 ring 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 $\mathcal{L} = \mathcal{L}_1 \times \cdots \times \mathcal{L}_r$.

(6.1) Definition. Notation as above. A *notion of positivity* on an invertible $\mathcal{O}_E$-module $\mathcal{L}$ 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 $-\mathcal{L}^+$.

(6.2) Definition. (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 $\iota(1) = \mathrm{Id}_A$. Notice 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 $u \in \mathcal{O}_E$.

(6.3) Exercise. 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 $i = 1, \ldots, r$.

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

(6.5) Definition. 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 BT-group is a pair $(X \to S, \iota)$, where $X \to S$ is a BT-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 BT-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 BT-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 BT-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 BT-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 BT-group $(X \to S, \iota)$ is of HB-type if it admits an $\mathcal{O}_{E_p}$-linear polarization.

(6.6) Exercise. 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 BT-group $(A[p^\infty], \iota[p^\infty])$ is of HB-type.

(6.7) Definition. 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 5-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) $\lambda : \mathcal{L} \to \mathrm{Hom}^{\mathrm{sym}}_{\mathcal{O}_E}(A, A^t)$ 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 $(\mathcal{O}_E/n\mathcal{O}_E)^2_S$ to $A[n]$.

(6.8) Remark. 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 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 characterized by $\Xi_{E,\mathcal{L},n}(k) := \mathrm{Isom}(\mathcal{O}_E/n\mathcal{O}_E, \mathcal{L}^{-1}\mathcal{D}_E^{-1} \otimes_{\mathbb{Z}} \mu_n)$ 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 $\Xi_{E,\mathcal{L},n} := \underline{\mathrm{Isom}}(\mathcal{O}_E/n\mathcal{O}_E, \mathcal{L}^{-1}\mathcal{D}_E^{-1} \otimes_{\mathbb{Z}} \mu_n)$ 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 $\mathbb{F}_p$.

(6.9) Remark. (i) We have followed [19] 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 [19].
(ii) The product decompositions $\mathcal{O}_E = \mathcal{O}_{F_1} \times \cdots \times \mathcal{O}_{F_r}$ and $(\mathcal{L}, \mathcal{L}^+) = (\mathcal{L}_1, \mathcal{L}_1^+) \times (\mathcal{L}_r, \mathcal{L}_r^+)$ induces a natural isomorphism

$$\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n} \xrightarrow{\sim} \mathcal{M}_{F_1,\mathcal{L}_1,\mathcal{L}_1^+,n} \times \cdots \times \mathcal{M}_{F_r,\mathcal{L}_r,\mathcal{L}_r^+ n}\,.$$

(6.10) Remark. 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, not just one polarization: every element $u \in \mathcal{L}\cap^+$ 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 $\mathrm{Card}(\mathcal{L}/\mathcal{O}_E \cdot u)$ is not divisible by p. In [95] and [96] 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 $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$.

(6.11) Theorem $\boxed{\text{BB}}$ *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 [19] and for a proof of Thm. 6.11 which uses the arithmetic toroidal compactification constructed in [80].
(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 $\widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}}$ the projective system $(\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n})_n$ of Hilbert modular varieties over $\mathbb{F}$, where n runs through all positive integer such that $n \geq 3$ and $\gcd(n,p) = 1$. It is clear that the profinite group $\mathrm{SL}_2(\mathcal{O}_E \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{(p)})$ operates on the tower $\widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}}$, by pre-composing with the $\mathcal{O}_E$-linear level structures. Here $\widehat{\mathbb{Z}}^{(p)} = \prod_{\ell \neq p} \mathbb{Z}_\ell$. 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 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 $\widetilde{\Xi_E}$ be the projective system $(\Xi_{E,n})_n$, where n also runs through all positive integer 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 $\tilde{f} : \widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}} \to \widetilde{\Xi_E}$ between projective systems.

It is clear that the profinite group $\mathrm{SL}_2(\mathcal{O}_E \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{(p)})$ operates on right of the tower $\widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}}$, by pre-composing with the $\mathcal{O}_E$-linear level structures. Moreover this action is compatible with the map $\tilde{f} : \widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}} \to \widetilde{\Xi_E}$ between projective systems.

The above right action of the compact group $\mathrm{SL}_2(\mathcal{O}_E \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{(p)})$ on the projective system $\widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}}$ extends to a right action of $\mathrm{SL}_2(E \otimes_{\mathbb{Q}} \mathbb{A}_f^{(p)})$ on $\widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}}$. Again this action is compatible with $\tilde{f} : \widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}} \to \widetilde{\Xi_E}$. This action can be described as follows. A geometric point of $\widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}}$ is a quadruple $(A, \iota_A, \lambda_A, \tilde{\eta}_A)$, where the infinite prime-to-p level structure

$$\tilde{\eta}_A : \coprod_{\ell \neq p} (\mathcal{O}_E[1/\ell]/\mathcal{O}_E) \xrightarrow{\sim} \coprod_{\ell \neq p} A[\ell^\infty]$$

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 an element $\gamma\in \mathrm{SL}_2(E\otimes_{\mathbb{Q}}\mathbb{A}_f^{(p)})$ belongs to $\mathrm{M}_2(\mathcal{O}_E\otimes_{\mathbb{Z}}\widehat{\mathbb{Z}}^{(p)})$. Then the image of the point $(A,\iota_A,\lambda_A,\tilde{\eta}_A)$ under γ is a quadruple $(B,\iota_B,\lambda_B,\tilde{\eta}_B)$ such that there exists an $\mathcal{O}_E$-linear prime-to-p isogeny $\beta: B\to A$ such that the diagram

$$\begin{tikzcd}
\coprod_{\ell\neq p}(\mathcal{O}_E[1/\ell]/\mathcal{O}_E)^2 \arrow[r, "\tilde{\eta}_A"] & \coprod_{\ell\neq p} A[\ell^\infty] \\
\coprod_{\ell\neq p}(\mathcal{O}_E[1/\ell]/\mathcal{O}_E)^2 \arrow[r, "\tilde{\eta}_B"'] \arrow[u, "\gamma"] & \coprod_{\ell\neq p} B[\ell^\infty] \arrow[u, "\beta"']
\end{tikzcd}$$

commutes.

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 $\widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}}$ induce 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 $\tilde{x}$ is point of $\widetilde{\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+}}$ lifting x_0. Then the prime-to-p SL_2-Hecke orbit of x_0, denoted $\mathcal{H}^{(p)}_{\mathrm{SL}_2}(x_0)$, is the image in $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}$ of the orbit $\mathrm{SL}_2(E\otimes_{\mathbb{Q}}\mathbb{A}_f^{(p)})\cdot x_0$. The set $\mathcal{H}^{(p)}_{\mathrm{SL}_2}(x_0)$ is countable.

(6.13) Theorem *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 $\Sigma_{E,p}=\{\wp_1,\dots,\wp_s\}$ be the set of all prime ideals of $\mathcal{O}_E$ containing p. Then we have a natural isomorphism*

$$\mathcal{M}^{/x_0}_{E,\mathcal{L},\mathcal{L}^+,n}\cong\prod_{j=1}^{s}\underline{\mathrm{Hom}}_{\mathbb{Z}_p}\left(\mathrm{T}_p(A_0[\wp_j^\infty]_{\mathrm{et}})\otimes_{(\mathcal{O}_E\otimes\mathbb{Z}_p)}\mathrm{T}_p(A_0^t[\wp_j^\infty]_{\mathrm{et}}),\,\widehat{\mathbb{G}_m}\right).$$

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 $(\mathcal{O}_E\otimes_{\mathbb{Z}}\mathbb{Z}_p)\otimes_{\mathbb{Z}_p}\widehat{\mathbb{G}_m}$.

PROOF. By the Serre-Tate theorem, we have

$$\mathcal{M}^{/x_0}_{E,\mathcal{L},\mathcal{L}^+,n}\cong\prod_{j=1}^{s}\underline{\mathrm{Hom}}_{\mathcal{O}_E\otimes\mathbb{Z}_p}\left(\mathrm{T}_p(A_0[\wp_j^\infty]_{\mathrm{et}}),\,\widehat{A_0[\wp_j^\infty]_{\mathrm{mult}}}\right),$$

where $\widehat{A_0[\wp_j^\infty]_{\mathrm{mult}}}$ is the formal torus attached to $A_0[\wp_j^\infty]_{\mathrm{mult}}$, 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 $\mathrm{T}_p(A_0^t[\wp_j^\infty]_{\mathrm{et}})$ attached to the maximal étale quotient of $A_0^t[\wp_j^\infty]_{\mathrm{et}})$. $\square$

(6.14) Proposition *Notation as in 6.13. Assume that $k=\mathbb{F}$, so $x_0=[(A_0,\iota_0,\lambda_0,\eta_0)]\in\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(\mathbb{F})$ and A_0 is an ordinary $\mathcal{O}_E$-linear abelian variety of HB-type over $\mathbb{F}$.*

(i) *There exists totally imaginary quadratic extensions K_i of F_i, $i=1,\dots,r$ such that $\mathrm{End}^0_{\mathcal{O}_E}(A_0)\cong K_1\times\cdots\times K_r=:K$. Moreover, for every prime ideal $\wp_j$ of $\mathcal{O}_E$ containing*

p, we have

$$\operatorname{End}_{\mathcal{O}_E}(A_0)\otimes_{\mathcal{O}_E}\mathcal{O}_{E_{\wp_j}} \xrightarrow{\sim} \operatorname{End}_{\mathcal{O}_{E_{\wp_j}}}(A_0[\wp_j^\infty]_{\mathrm{mult}})\times \operatorname{End}_{\mathcal{O}_{E_{\wp_j}}}(A_0[\wp_j^\infty]_{\mathrm{et}})$$
$$\cong \mathcal{O}_{E_{\wp_j}}\times\mathcal{O}_{E_{\wp_j}} \xleftarrow{\sim} \mathcal{O}_K\otimes_{\mathcal{O}_E}\mathcal{O}_{E_{\wp_j}}\,.$$

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 $H_{x_0}=\{u\in(\mathcal{O}_E\otimes\mathbb{Z}_p)^\times \mid u\cdot\bar{u}=1\}$. Then both projections*

$$\mathrm{pr}_1: H_{x_0}\to \prod_{\wp\in\Sigma_{E,p}}\Big(\operatorname{End}_{\mathcal{O}_{E_\wp}}(A_0[\wp_j^\infty]_{\mathrm{mult}})\Big)^\times \cong \prod_{\wp\in\Sigma_{E,p}}\mathcal{O}_{E_\wp}^\times$$

and

$$\mathrm{pr}_2: H_{x_0}\to \prod_{\wp\in\Sigma_{E,p}}\Big(\operatorname{End}_{\mathcal{O}_{E_\wp}}(A_0[\wp^\infty]_{\mathrm{et}})\Big)^\times \cong \prod_{\wp\in\Sigma_{E,p}}\mathcal{O}_{E_\wp}^\times$$

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 operates on the $(\mathcal{O}_E\otimes_{\mathbb{Z}}\mathbb{Z}_p)$-linear formal torus $\mathcal{M}^{/x_0}_{E,\mathcal{L},\mathcal{L}^+,n}$ through the character*

$$H\ \ni t\longmapsto \mathrm{pr}_1(t)^2\in(\mathcal{O}_E\otimes_{\mathbb{Z}}\mathbb{Z}_p)^\times\,.$$

(iv) *Notation as in* (ii) *above. Let Z be a reduced, irreducible closed formal subscheme of the formal scheme $\mathcal{M}^{/x_0}_{E,\mathcal{L},\mathcal{L}^+,n}$ which is stable under the natural action of an open subgroup U_{x_0} of H_{x_0} on $\mathcal{M}^{/x_0}_{E,\mathcal{L},\mathcal{L}^+,n}$. Then there exists a subset $S\subset\Sigma_{E,p}$ such that*

$$Z=\prod_{\wp\in S}\underline{\operatorname{Hom}}_{\mathbb{Z}_p}\Big(\mathrm{T}_p(A_0[\wp^\infty]_{\mathrm{et}})\otimes_{(\mathcal{O}_E\otimes\mathbb{Z}_p)}\mathrm{T}_p(A_0^t[\wp^\infty]_{\mathrm{et}}),\,\widehat{\mathbb{G}_m}\Big)$$

Proof. The statement (i) is a consequence of Tate's theorem on endomorphisms of abelian varieties over finite field, see [88]. The statement (ii) follows from (i). The statement (iii) is immediate from the displayed canonical isomorphism in Thm. 6.13. It remains to prove (iv).

By Thm. 2.27 and Thm. 6.13, we know that Z is a formal subtorus of the formal torus

$$\mathcal{M}^{/x_0}_{E,\mathcal{L},\mathcal{L}^+,n}=\prod_{\wp\in\Sigma_{E,p}}\underline{\operatorname{Hom}}_{\mathbb{Z}_p}\Big(\mathrm{T}_p(A_0[\wp^\infty]_{\mathrm{et}})\otimes_{(\mathcal{O}_E\otimes\mathbb{Z}_p)}\mathrm{T}_p(A_0^t[\wp^\infty]_{\mathrm{et}}),\,\widehat{\mathbb{G}_m}\Big)\,.$$

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

$$\prod_{\wp\in\Sigma_{E,p}}(\mathrm{T}_p(A_0[\wp^\infty]_{\mathrm{et}}))^\vee\otimes_{(\mathcal{O}_E\otimes\mathbb{Z}_p)}\big(\mathrm{T}_p(A_0^t[\wp^\infty]_{\mathrm{et}})\big)^\vee$$

of $\mathcal{M}^{/x_0}_{E,\mathcal{L},\mathcal{L}^+,n}$, which is co-torsion free. Moreover $X_*(Z)$ is stable under the action of U_{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 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

$$\left(\prod_{\wp\in S} (\mathrm{T}_p(A_0[\wp^\infty]_{\mathrm{et}}))^\vee \otimes_{\mathcal{O}_E\otimes\mathbb{Z}_p} \left(\mathrm{T}_p(A_0^t[\wp^\infty]_{\mathrm{et}})\right)^\vee\right)\otimes_{\mathbb{Z}_p} .$$

Since $X_*(Z)$ is a co-torsion free $\mathbb{Z}_p$-submodule of

$$\prod_{\wp\in\Sigma_{E,p}} (\mathrm{T}_p(A_0[\wp^\infty]_{\mathrm{et}}))^\vee \otimes_{(\mathcal{O}_E\otimes\mathbb{Z}_p)} \left(\mathrm{T}_p(A_0^t[\wp^\infty]_{\mathrm{et}})\right)^\vee ,$$

we see that $X_*(Z)$ is equal to $\left(\prod_{\wp\in S} (\mathrm{T}_p(A_0[\wp^\infty]_{\mathrm{et}}))^\vee \otimes_{\mathcal{O}_E\otimes\mathbb{Z}_p} (\mathrm{T}_p(A_0^t[\wp^\infty]_{\mathrm{et}}))^\vee\right)$. □

(6.15) Corollary *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*

$$Z^{/x_0} = \prod_{\wp\in S} \underline{\mathrm{Hom}}_{\mathbb{Z}_p}\left(\mathrm{T}_p(A_0[\wp^\infty]_{\mathrm{et}})\otimes_{(\mathcal{O}_E\otimes\mathbb{Z}_p)}\mathrm{T}_p(A_0^t[\wp^\infty]_{\mathrm{et}}),\, \widehat{\mathbb{G}_m}\right) .$$

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 $K^\times$. Denote by $\mathrm{U}_K(\mathbb{Z}_p)$ the compact open subgroup of $\mathrm{U}_K(\mathbb{Q}_p)$ corresponding to the subgroup $\mathbb{Z}_p^\times\subset\mathbb{Q}_p^\times$. This group $\mathrm{U}_K(\mathbb{Z}_p)$ is naturally isomorphic to the group H_{x_0} in 6.14 (ii). We have a natural action of $\mathrm{U}_K(\mathbb{Z}_p)$ on

$$\mathrm{Def}((\mathrm{A}_0,\iota_0,\lambda_0)[\mathrm{p}^\infty])/\mathbb{F}) \cong \mathcal{M}^{/\mathrm{x}_0}_{\mathrm{E},\mathcal{L},\mathcal{L}^+,\mathrm{n}}$$

by the deformation of the deformation functor $\mathrm{Def}((\mathrm{A}_0,\iota_0,\lambda_0)[\mathrm{p}^\infty])$

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 $Z\subset\mathcal{M}^{/x_0}_{E,\mathcal{L},\mathcal{L}^+,n}$ 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 [79], 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 $Z^{/x_0}\subset\mathcal{M}^{/x_0}_{E,\mathcal{L},\mathcal{L}^+,n}$ 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). □

(6.16) Exercise. 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.

(6.17) Exercise. 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.

(6.18) Exercise. 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 $(A, \iota, \lambda, \eta)] \in \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,n}(k)$.

(6.19) Exercise. 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: [43], [72]
In this course we will prove and use the following rather technical result.

(7.1) Theorem *Defoa1* $\boxed{\textbf{Th}}$ (**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 with X_0, and for the generic point $\eta \in S$ we have:*

$$\mathcal{N}(X_0) = \mathcal{N}(X_\eta) \quad \textit{and} \quad a(X_\eta) \leq 1.$$

See [43], 5.12 and [72], 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 Lecture 9, that once we have the theorem in this special case, 7.1 and 7.13 will follow without much trouble.

The proof of this special case given here (and the only one I know) is a combination of general theory, and a computation. We start with one of the tools.

(7.3) Theorem *Purity* $\boxed{\textbf{BB}}$ (**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 $S \supset D = S_{\neq\gamma} := \{s \mid \mathcal{N}(A_s) \npreceq \gamma\}$* (Note that D is closed in S by Grothendieck-Katz.) *Then either D is empty or* $\mathrm{codim}(D \subset S) = 1$.

I know two proofs of this theorem, and both proofs are non-trivial. See [43], Th. 4.1. Also see [89], th. 6.1; this proof was analyzed in [73].

When this result was first mentioned, it met unbelief. Why? If you follow the proof by Katz, see [48], 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 my 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 complete a intersection, or locally a set-theoretic complete intersection).

(7.4) The simple case, notation. We follow [43], §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 define the p-divisible group $H_{m,n}$, see [43], 5.3. Let K be a perfect field, $W = W_\infty(K)$. Consider symbols $\{e_i \mid i \in \mathbb{Z}_{\geq 0}\}$. Define

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

This is a Dieudonné module, and the p-divisible group determined by this we write as $H_{m,n}$. Note that if $K \supset \mathbb{F}_{p^{m+n}}$ then $D := \mathrm{End}^0(H_{m,n})$ is a division algebra of rank $(m+n)^2$ over $\mathbb{Q}_p$, and $R := \mathrm{End}(H_{m,n})$ is the maximal order in $\mathrm{End}^0(H_{m,n})$; note that $\pi \in \mathrm{End}(H_{m,n})$ defined by $\pi(e_i) = e_{i+1}$ indeed is an endomorphism, it is a "uniformizer" in R, and R is a "non-commutative discrete valuation ring".
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. For properties of minimal p-divisible groups see [76]. Such groups are of importance in understanding various stratifications of $\mathcal{A}_g$.

We want to understand all p-divisible groups isogenous with $H := H_{m,n}$ (m and n will remain fixed).

(7.5) Lemma $\boxed{\textbf{BB}}$ *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. **Exercise:** give a proof.

(7.6) Construction. For every scheme S over $\mathbb{F}_p$ consider

$$S \quad \mapsto \quad \{(\varphi, X) \mid \varphi : H \times S \to X, \;\; \deg(\varphi) = p^r\}.$$

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 constructed is just a special case of the theory of Rapoport-Zink spaces, see [82], Th. 2.16. In the special case considered here, the space T is a connected component of the reduction-mod-p fiber of a Rapoport-Zink space.

(7.7) Theorem $\boxed{\textbf{Th}}$ *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 [43], Th. 5.11. *Note that* 7.1 *follows from this theorem in case* $X_0 \sim H_{m,n}$. We now focus on a proof of 7.7.
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 $m \geq n > 0$.

(7.8) Definition. We say that $A \subset \mathbb{Z}$ is a *semi-module* or more precisely, a (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 $A = \{a_1, a_2, \cdots\}$ 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) $A = \{a_1, \cdots, a_r\} \cup [2r, \infty)$;
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 "$(-m,-n)$-semimodule". Hence $\{y \mid y \notin A\}$ is a semi-module; then normalize.

Example. Write $< 0 >$ 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 $< 0 >$ indeed is normalized. Show that $2r - 1 \notin < 0 >$.*
(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: $A = < 0 > \iff 0 \in A \iff 2r - 1 \notin A$.*

(7.9) 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

$$\mathbb{D}(X) \quad \hookrightarrow \quad \mathbb{D}(H) = M = \oplus_{0 \leq i < m+n} W{\cdot}e_i.$$

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 as* Type(X) .

We denote by $U_A \subset T$ the set where the semi-module A is realized:

$$U_A \quad = \quad \{t \in T \mid \mathrm{Type}(\mathcal{G}_t) = A\}.$$

(7.10) Proposition (1) *$U_A \hookrightarrow T$ is locally closed, $T = \sqcup_A U_A$.*
(2) *$A =< 0 > \iff a(X) = 1$.*
(3) *$U_{<0>}$ is geometrically irreducible and has dimension r.*
(4) *If $A \neq< 0 >$ then every component of U_A has dimension strictly less than r.*

(7.11) $\boxed{\textbf{BB}}$ 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 with $\mathrm{Spf}(K[[t_1, \cdots, t_{cd}]])$ 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 [39], 4.8, [43], 5.15.

(7.12) We prove 7.7, using 7.3 and 7.10. Note that the Zariski closure $(U_{<0>})^{\mathrm{Zar}} \subset T$ is geometrically irreducible, and has dimension r; we want to show equality $(U_{<0>})^{\mathrm{Zar}} = T$. Suppose there would be an irreducible component T' of T not contained in $(U_{<0>})^{\mathrm{Zar}}$. By 7.10 (3) and (4) we see that $\dim(T') < r$. Let $y \in T'$, with corresponding p-divisible group Y_0.

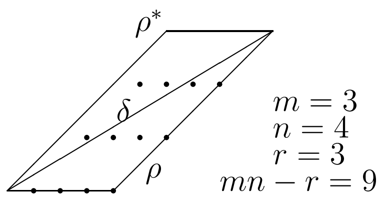
Consider the formal completion $T^{/y}$ of T at y. Write $D = \mathrm{Def}(Y_0)$ for the universal deformation space of Y_0. The moduli map $T^{/y} \to D = \mathrm{Def}(Y_0)$ is an immersion, see [43], 5.19. Let $T'' \subset D$ be the image of $(T')^{/y}$ in D; we conclude that no irreducible component 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 $\leq mn - r$.



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 beginning and end point. 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 $\delta \precneqq (i,j)$ for the property "(i,j) is strictly below δ", and $(i,j) \prec \rho$ for "(i,j) is upon or above ρ". We see:

$$\#\left(\{(i,j) \mid \delta \precneqq (i,j) \prec \rho\}\right) \quad = \quad (m-1)(n-1)/2 + (m+n-1) \quad = \quad mn - r. \qquad \square$$

We used the fact: If $\zeta_1 \precneqq \zeta_2$, 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

$$\#\left(\{(i,j) \mid \delta \precneqq (i,j) \prec \rho\}\right).$$

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 with the assumption of the existence of T', i.e. $\dim(T') = \dim(T'') < r$. Hence $(U_{<0>})^{\mathrm{Zar}} = T$. This proves 7.7. Hence we have proved 7.1 in case X_0 is isogenous with $H_{m,n}$. $\square$

(7.13) Theorem $\boxed{\text{Th}}$ (**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:*

$$\mathcal{N}(X_0) = \mathcal{N}(X_\eta) \quad \textit{and} \quad a(X_\eta) \leq 1.$$

See [43], 5.12 and [72], 3.10.

(7.14) Corollary $\boxed{\text{Th}}$ (**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:*

$$\mathcal{N}(A_0) = \mathcal{N}(A_\eta) \quad \textit{and} \quad a(X_\eta) \leq 1.$$

(7.15) 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 [45], 6.10, and also see [50], 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 $(W^0_{\xi_2})^{\mathrm{Zar}} = W_{\xi_2}$ does not hold in general as is showed 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 [45], 6.10, there is a component of $\mathcal{W}_\sigma(\mathcal{A}_{g,p^2})$ of dimension 3; more generally see [50], Th. 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 [63], Th. 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.

§8. Proof of the Grothendieck conjecture

Main reference: [72].

(8.1) Definition. $\boxed{\textbf{Extra}}$ Let X be a p-divisible group over a base S. We say that $0 = X^{(0)} \subset X^{(1)} \subset \cdots \subset X^{(s)} = X$ is *the slope filtration* of X if $Y_i := X^{(i)}/X^{(i-1)}$ for $1 \leq i \leq s$ is isoclinic of slope τ_i with $\tau_1 < \tau_2 < \cdots < \tau_s$.
Remarks. 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 [103], Coroll. 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.

(8.2) Definition. We say that $0 = X^{(0)} \subset X^{(1)} \subset \cdots \subset X^{(s)} = X$ is a maximal filtration of $X \to S$ if $Y^{(i)} := X^{(i)}/X^{(i-1)}$ for $1 \leq i \leq s$ is *simple* and isoclinic of slope τ_i with $\tau_1 \leq \tau_2 \leq \cdots \leq \tau_s$.
Lemma. $\boxed{\textbf{BB}}$ *For every X over k a maximal filtration exists.*
See [72], 2.2

(8.3) Lemma. $\boxed{\textbf{BB}}$ *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 $1 \leq i \leq s$, such that $\{X^{(i)}\}_0 = \{X_0^{(i)}\}$ and such that for the generic point $\eta \in S$ we have $a(X_\eta) \leq 1$.*
See [72], Section 2. A proof of this lemma uses Theorem 7.7.

From this lemma we derive a proof for Theorem 7.1.

(8.4) Definition. We say that X_0 over a field K is a *specialization* of 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 sued for p-divisible groups, for abelian schemes, etc

(8.5) Proposition. *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 5.8 and Theorem 7.1 by the proposition above we derive a proof for the Grothendieck Conjecture Theorem 1.28. $\square$

(8.6) Corollary of Theorem 1.28. *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 $\Diamond(\beta)$.*

(8.7) Definition. Let (X, λ) be a principally polarized p-divisible group over S. We say that $0 = X^{(0)} \subset X^{(1)} \subset \cdots \subset X^{(s)} = X$ is *a maximal symplectic filtration* of (X, λ) if:

- $Y^{(i)} := X^{(i)}/X^{(i-1)}$ for $1 \leq i \leq s$ is simple of slope τ_i,
- $\tau_1 \leq \tau_2 \leq \cdots \leq \tau_s$, and
- $\lambda : X \to X^t$ induces an isomorphism

$$\lambda_i : Y^{(i)} \to (Y^{(s+1-i)})^t \quad \text{for} \quad 0 < i \leq (s+1)/2.$$

(8.8) Lemma. *For every principally polarized (X, λ) over k there exists a maximal symplectic filtration.* See [72], 3.5.

(8.9) Using this definition, and this lemma we show the principally polarized analog of 7.13, see [72], Section 3. Hence Corollary 7.14 follows. Using Theorem 5.17 we derive a proof for:

(8.10) Theorem (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. We write $\mathcal{N}(X_0) = \xi$ for its Newton polygon. Suppose given a Newton Polygon ζ "below" ξ, i.e. $\xi \prec \zeta$. Then there exists a deformation (X_η, λ_η) of (X_0, λ_0) such that $\mathcal{N}(\mathcal{X}_\eta) = \zeta$.*

(8.11) Corollary. *Let $K \supset \mathbb{F}_p$. Let (A_0, λ_0) be a* principally *polarized abelian variety over K. We write $\mathcal{N}(A_0) = \xi$ for its Newton polygon. Suppose given a Newton Polygon ζ "below" ξ, i.e. $\xi \prec \zeta$. Then there exists a deformation (A_η, λ_η) of (A_0, λ_0) such that $\mathcal{N}(\mathcal{X}_\eta) = \zeta$.*

(8.12) Corollary. *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 1.7 on density of ordinary Hecke orbits, restated as Theorem 9.1 below. To establish Thm. 1.7, 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 2.27.

(iv) Consequence of EO stratification, see 9.7.

(iv) Hilbert trick, see 9.10.

The logical structure of the proof of Theorem 1.7 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 point. Then we use the local stabilizer principle and the local rigidity to conclude the proof of 1.7

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 $E = F_1 \times \cdot \times F_r$ of totally real field 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 $\mathbb{F}_p$ and finite $\mathbb{F}_p$-morphisms $g : T \to \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$ and $f : T \to \mathcal{A}_{g,1,n}$ such that the pull-back by g of the universal abelian scheme over $\mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$ is isogenous to the pull-back 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, $\left(\mathcal{H}^{(p)}_{\mathrm{Sp}}(x)\right)^{\mathrm{Zar}}$ 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 $\left(\mathcal{H}^{(p)}_{\mathrm{Sp}}(x)\right)^{\mathrm{Zar}}$ is equal to $g(g+1)/2$, hence $\left(\mathcal{H}^{(p)}_{\mathrm{Sp}}(x)\right)^{\mathrm{Zar}} = \mathcal{A}_{g,1,n}$ because $\mathcal{A}_{g,1,n}$ is geometrically irreducible, see 10.16.

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 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 Barsotti-Tate groups. We follow the first approach here, see [12, §8] for the second approach.

(9.1) Theorem *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 $\mathbb{F}$, i.e.*

$$\left(\mathcal{H}^{(p)}_{\mathrm{Sp}}(x)\right)^{\mathrm{Zar}} = \mathcal{A}_{g,1,n}\,.$$

(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.*

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

(9.2) Theorem *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 $\mathbb{F}$.*

(9.3) Proposition *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 $\mathcal{H}^{(p)}_{\mathrm{Sp}_{2g}}(x)$ 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 be the Zariski closure of the prime-to-p Hecke orbit $\mathcal{H}^{(p)}_{\mathrm{SL}_2}(y)$ 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 $\mathcal{H}^{(p)}_{\mathrm{SL}_2}(y)$ 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. ∎

Remark. (i) Prop. 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 Prop. 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.

(9.4) Theorem $\boxed{\textbf{BB}}$ *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 [10, Prop. 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 consists 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 $\mathcal{A}^{/z}_{g,1,n}$ (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 $\mathfrak{Def}\,((A_z,\lambda_z)[p^\infty]/k)$. 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

$$\mathcal{A}_{g,1,n}^{/z} = \mathfrak{Def}\,((A_z,\lambda_z)/k) \xrightarrow[\sim]{\text{Serre-Tate}} \mathfrak{Def}\,((A_z,\lambda_z)[p^\infty])/k)\ .$$

(9.5) Theorem (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 $\widetilde{\mathcal{A}_{g,1}} = \varprojlim_m \mathcal{A}_{g,1,m}$ over k, where m runs through all integers $m \geq 1$ which are prime to p. The pro-scheme $\widetilde{\mathcal{A}_{g,1}}$ 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 representation of the symplectic group Sp_{2g}. Take $S_z = \mathcal{A}_{g,1,n}^{/z}$, let $(\hat{A},\hat{\lambda}) \to \mathcal{A}_{g,1,n}^{/z}$ be the restriction of the universal principally polarized abelian scheme to $\mathcal{A}_{g,1,n}^{/z}$, and let $\hat{\eta}$ be the tautological prime-to-p level structure, we get an S_z-point of the tower $\widetilde{\mathcal{A}_{g,1}}$ 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

$$\begin{tikzcd}
(\hat{A},\hat{\lambda})[p^\infty] \arrow[r, "{f_\gamma[p^\infty]}"] \arrow[d] & (\hat{A},\hat{\lambda})[p^\infty] \arrow[d] \\
\mathcal{A}_{g,1,n}^{/z} \arrow[r, "u_\gamma"] & \mathcal{A}_{g,1,n}^{/z}
\end{tikzcd}$$

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

$$\begin{tikzcd}
\hat{A} \arrow[r, "f_\gamma"] \arrow[d] & \hat{A} \arrow[d] \\
\mathcal{A}_{g,1,n}^{/z} \arrow[r, "u_\gamma"] & \mathcal{A}_{g,1,n}^{/z}
\end{tikzcd}$$

commutes and f_γ preserves the polarization $\hat{\lambda}$. 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 $\widetilde{\mathcal{A}_{g,1}}$. 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 [79], 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 $\mathrm{Aut}((A_z,\lambda_z)[p^\infty])$. $\square$

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 $\mathrm{End}^0_{\mathcal{O}_E}(A_y) = \mathrm{End}_{\mathcal{O}_E}(A_y) \otimes_{\mathcal{O}_E} E$. Denote by H_y the unitary group over $\mathbb{Q}$ attached to $(\mathrm{End}^0_{\mathcal{O}_E}(A_y), *_y)$, so

$$\mathrm{H}_y(R) = \left\{ u \in \left(\mathrm{End}^0_{\mathcal{O}_E}(A_y) \otimes_{\mathbb{Q}} R\right)^\times \mid u \cdot *_y(u) = *_y(u)\cdot u = \mathrm{Id}_{A_y} \right\}$$

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 induces 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 deformation space $\mathfrak{Def}((A_y,\iota_y,\lambda_y)[p^\infty]/k)$. 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 $\mathcal{M}^{/y}_{E,\mathcal{L},\mathcal{L}^+,m}$ via the canonical isomorphism

$$\mathcal{M}^{/y}_{E,\mathcal{L},\mathcal{L}^+,m} = \mathfrak{Def}((A_y,\iota_y,\lambda_y)/k) \xrightarrow[\sim]{\text{Serre-Tate}} \mathfrak{Def}((A_y,\iota_y,\lambda_y)[p^\infty]/k)\ .$$

(9.6) Theorem *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 $\mathcal{M}^{/y}_{E,\mathcal{L},\mathcal{L}^+,m}$ is stable under the action by elements of the subgroup $\mathrm{H}_y(\mathbb{Z}_p)$ of $\mathrm{Aut}(A_y[p^\infty], \iota_y[p^\infty], \lambda_y[p^\infty])$.*

PROOF. The proof of Thm. 9.6 is similar to that of Thm. 9.5, and is left as an exercise. $\square$

(9.7) Theorem $\boxed{\textbf{BB}}$ *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. Thm. 9.7 follows from the main theorem of [71] and Prop. 9.8 below. Also see 3.23.

(9.8) Proposition $\boxed{\textbf{BB}}$ *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 $\mathcal{H}^{(p)}_{\mathrm{Sp}_{2g}}(x)$ is finite. Conversely, if A_x is not supersingular, then the ℓ-adic Hecke orbit $\mathcal{H}^{\mathrm{Sp}_{2g}}_{\ell}(x)$ 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 is supersingular, then the prime-to-p Hecke orbit $\mathcal{H}^{(p)}_{\mathrm{SL}_{2,E}}(y)$ is finite. Conversely, if A_y is not supersingular, then the ℓ-adic Hecke orbit $\mathcal{H}^{\mathrm{SL}_{2,E}}_{v}(y)$ 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 Prop. 1, p. 448 of [8], see 1.17. The proof of (ii) is similar. The key to the proof of the second part of (i) is a bijection

$$\mathcal{H}^{\mathrm{Sp}_{2g}}_{\ell}(x) \xleftarrow{\sim} \left(\mathrm{H}_x(\mathbb{Q}) \cap \prod_{\ell' \neq \ell} K_\ell\right) \backslash \mathrm{Sp}_{2g}(\mathbb{Q}_\ell)/K_\ell$$

where ℓ' runs through all prime numbers not equal to ℓ or p, $\mathrm{H_x}$ is the unitary group attached to $(\mathrm{End}^0(A_x), *_x)$ as in Thm. 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 Thm. 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 $\mathcal{H}^{\mathrm{Sp}_{2g}}_{\ell}(x)$ (resp. $\mathcal{H}^{\mathrm{SL}_{2,E}}_{v}(y)$) is infinite.

The following irreducibility statement is handy for the proof of Thm. 9.2, in that it shortens the argument and simplifies the logical structure of the proof.

(9.9) Theorem $\boxed{\textbf{BB}}$ *Let W be a locally closed subscheme of $\mathcal{M}_{F,n}$ 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 operates 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 [10] works in the situation of 9.9. The following observations may be helpful.
(i) The linear algebraic group $\mathrm{Res}_{F/\mathbb{Q}}(\mathrm{SL}_2)$ over $\mathbb{Q}$ is a 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. Consequently $\mathrm{SL}_2(F \otimes \mathbb{A}_f^{(p)}$ has no proper subgroup of finite index.
(ii) The only part of the argument in [10] 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 $\ell \neq p$.

(9.10) Theorem (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 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 is a projective system $\widetilde{\mathcal{M}}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+;a}$ 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 $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$-action induces Hecke correspondences on $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$*

(ii) *The morphism g is equivariant w.r.t. Hecke correspondences coming from the group $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$. In other words, there is a $\mathrm{SL}_2(E \otimes \mathbb{A}_f^{(p)})$-equivariant morphism $\tilde{g}$ from the projective system $\widetilde{\mathcal{M}}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+;a}$ 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 w.r.t. 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 $\mathcal{A}^{\mathrm{ord}}_{g,n}(\mathbb{F})$.*

Lemma. Let A be a 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 the 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 [88]. $\square$

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 [8]. $\square$

Proof of Thm. 9.10 (Hilbert trick).

STEP 1. Consider the abelian variety A_0 attached to the given point $x_0 = [(A_0, \lambda_0, \eta_0)] \in \mathcal{A}_{g,1,n}^{\mathrm{ord}}(\mathbb{F})$. By the two lemmas above, Consequently 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 Thm. 3.17) 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 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 $\mathcal{L}_B := \mathrm{Hom}_{\mathcal{O}_E}^{\mathrm{sym}}(B, B^t)$ 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 Thm. 3.17, see 10.7) 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, $\lambda_A : \mathcal{L} \to \mathrm{Hom}_{\mathcal{O}_E}^{\mathrm{sym}}(A, A^t)$ 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 $\cap\mathcal{L}^+$ 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 $(m_1, p) = 1$ 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

$$\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} := \underline{\mathrm{Isom}}^{\mathcal{O}_E}_{\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}} \Big((B, \iota_B, \lambda_B)[p^a] \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m}, (A, \iota_A, \lambda_A)[p^a] \Big) \,.$$

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 Barsotti-Tate 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

$$\underline{\mathrm{Aut}}\left((B, \iota_B, \lambda_B)[p^a]\right) \times_{\mathrm{Spec}(\mathbb{F})} \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m} \,.$$

We have constructed the finite flat morphism g as promised in Thm. 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

$$0 \to \underline{\mathrm{Hom}}_{\mathcal{O}_E}\left(B[p^a]_{\mathrm{et}}, B[p^a]_{\mathrm{mult}}\right) \to \underline{\mathrm{Aut}}\left((B, \iota_B, \lambda_B)[p^a]\right) \to \underline{\mathrm{Aut}}\mathcal{O}_E\left(B[p^a]_{\mathrm{et}}\right) \to 0 \,.$$

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

$$\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \xrightarrow{g_1} \mathcal{M}^{\mathrm{ord,et}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \xrightarrow{g_2} \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m} \,,$$

where g_1 is defined as the push-forward by the surjection

$$\underline{\mathrm{Aut}}\,(B, \iota_B, \lambda_B)[p^a]) \twoheadrightarrow \underline{\mathrm{Aut}}\mathcal{O}_E\left(B[p^a]_{\mathrm{et}}\right)$$

of the $\underline{\mathrm{Aut}}\,(B, \iota_B, \lambda_B)[p^a])$-torsor $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$. Notice that the morphism g_1 is finite flat and purely inseparable, and $\mathcal{M}^{\mathrm{ord,et}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ is integral. Moreover $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ and $\mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ are irreducible by [81], [20], [80] and [19].

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 pull-back 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 pull-back 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 $A' \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ of $g^*A \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ by 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 subgroup of n-torsion $A'[n] \to \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a}$ 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 Thm. 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 $\widetilde{\mathcal{M}}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,a}$ 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 Thm. 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 Thm. 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 of $z \in \mathcal{M}^{\mathrm{ord}}_{F,\mathcal{L},\mathcal{L}^+,n}$ of a Hilbert modular variety $\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}$ admits a canonical decomposition

$$\mathcal{M}^{/z}_{F,\mathcal{L},\mathcal{L}^+,n} \cong \prod_{\wp \in \Sigma_{F,p}} \mathcal{M}^z_\wp, \qquad \mathcal{M}^z_\wp = \underline{\mathrm{Hom}}_{\mathcal{O}_{F,\wp}} \left(\mathrm{T}_p(A_z[\wp^\infty]_{\mathrm{et}}),\ e_\wp \cdot \widehat{A_z} \right),$$

where

- the indexing set $\Sigma_{F,p}$ is the finite set consisting of of all prime ideals of $\mathcal{O}_F$ above p,
- the $(\mathcal{O}_F \otimes \mathbb{Z}_p)$-linear formal torus$\widehat{A_z}$ 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 $e_\wp \widehat{A_z}$ is the formal torus attached to the multiplicative Barsotti-Tate group $A_z[\wp^\infty]_{\mathrm{mult}}$ 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 $\mathcal{M}^{/z}_{F,\mathcal{L},\mathcal{L}^+,n}$ into a product $\mathcal{M}^{/z}_{F,\mathcal{L},\mathcal{L}^+,n} = \prod_{\wp \in \Sigma_{F,p}} \mathcal{M}^z_\wp$ 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 Barsotti-Tate group attached to A, and each $A[\wp^\infty]$ is a deformation of $A \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R/\mathfrak{m})$ over $\mathrm{Spec}(R)$.

If z corresponds to an ordinary abelian variety A_z, then $\mathcal{M}^z_\wp$ is canonically isomorphic to the $\mathcal{O}_{F,\wp}$-linear formal torus $\underline{\mathrm{Hom}}_{\mathcal{O}_{F,\wp}}(A_z[\wp^\infty]_{\mathrm{et}}, e_\wp \cdot \widehat{A_z})$, which is the factor "cut out" in the $(\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p)$-linear formal torus

$$\mathcal{M}^{/z}_{F,\mathcal{L},\mathcal{L}^+,n} = \underline{\mathrm{Hom}}_{\mathcal{O}_F \otimes \mathbb{Z}_p} \left(\mathrm{T}_p(A_z[p^\infty],\ \widehat{A_z} \right)$$

by the idempotent $e_\wp$ in $\mathcal{O}_F \otimes \mathbb{Z}_p$. Each factor $\mathcal{M}^z_\wp$ in the above decomposition is a formal torus of dimension $[F_\wp : \mathbb{Q}_p]$, with a natural action by $\mathcal{O}^\times_{F,\wp}$; it is non-canonically isomorphic to the $\mathcal{O}_\wp$-linear formal torus $\widehat{A_z}$. $\square$

Step 2. (Linearization)

Claim. For every closed point $z \in Z_F^{\mathrm{ord}}(\mathbb{F})$ 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. The $\mathcal{O}_F$-linear abelian variety A_z is an ordinary abelian variety defined over $\mathbb{F}$. Therefore $\mathrm{End}^0_{\mathcal{O}_F}(A_z)$ 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 Thm. 3.17). 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 $\widehat{A_z}$. 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. an element $t \in U = \prod_{\wp\in\Sigma_{F,p}} \mathcal{O}_{F,\wp}^\times$ as 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

$$\mathcal{M}_{F,\mathcal{L},\mathcal{L}^+,n}^{/z} = \underline{\mathrm{Hom}}_{\mathcal{O}_F\otimes\mathbb{Z}_p}\left(\mathrm{T}_p(A_z[p^\infty]_{\mathrm{et}}),\ \widehat{A_z}\right),$$

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 $e_\wp\widehat{A_z}$ (resp. the $\mathcal{O}_F \otimes \mathbb{Z}_p$-linear Barsotti-Tate group $A_z[p^\infty]_{\mathrm{et}}$).

The local rigidity theorem 2.27 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 cotorsion 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 the 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 $\mathcal{H}^{(p)}_{\mathrm{SL}_2,F}(x)$ 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 $z \in Z_F(x)(\mathbb{F})$. $\square$

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 $\Delta_Z(\Delta_Z$, 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 $\mathcal{M}_\wp \to \mathcal{M}_{F,n}$ 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 point.

By Prop. 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 $\mathcal{P}_\wp \times_{\mathcal{M}_{F,n}} Z_F^{\mathrm{ord}} \to Z_F^{\mathrm{ord}}$, where $\wp$ runs through the subset $S \subseteq \Sigma_{F,p}$. □

Remark. (i) Without using Prop. 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 $\Omega^1_{\mathcal{M}^{\mathrm{ord}}_{F,\mathcal{L},\mathcal{L}^+,n}/\mathbb{F}}$ 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

$$\Omega^1_{Z_F^{\mathrm{ord}}/\mathbb{F}} \otimes_{\mathcal{O}_{Z_F,z}} \widehat{\mathcal{O}_{Z_F,z}} = \sum_{\wp \in S_z} e_\wp \cdot \Omega^1_{\mathcal{M}^{\mathrm{ord}}_{F,\mathcal{L},\mathcal{L}^+,n}/\mathbb{F}} \otimes_{\mathcal{O}_{\mathcal{M}^{\mathrm{ord}}_{F,\mathcal{L},\mathcal{L}^+,n}}} \widehat{\mathcal{O}_{Z_F,z}}$$

for every $z \in Z_F^{\mathrm{ord}}(\mathbb{F})$, where $\widehat{\mathcal{O}_{Z_F,z}}$ 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 [8]; see Prop. 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 Thm. 9.2 easier, as compared with the two-page proof of Prop. 7 on p. 474 of [8].

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 $\prod_{\wp \in S} \mathcal{M}_\wp^s$. By Thm. 9.7, Z_F contains a supersingular point s_0. Consider the formal completion $\hat{Z} := Z_F^{/s_0}$, which contains $\hat{W} := \prod_{\wp \in S} \mathcal{M}_\wp^{s_0}$, and the generic point $\eta_{\hat{W}}$ of $\mathrm{Spec}\left(\mathrm{H}^0(\hat{W}, \mathcal{O}_{\hat{W}})\right)$ is a maximal point of $\mathrm{Spec}\left(\mathrm{H}^0(\hat{Z}, \mathcal{O}_{\hat{Z}})\right)$. The restriction of the universal abelian scheme to $\eta_{\hat{W}}$ is an ordinary abelian variety. Hence $S = \Sigma_{F,p}$, otherwise $A_{\eta_{\hat{W}}}$ has slope $1/2$ with multiplicity at least $2\sum_{\wp \notin S}[F_\wp : \mathbb{Q}_p]$. Theorem 9.2 is proved. □

Remark. The proof of Thm. 9.2 can be finished without using Prop. 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 Thm. 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 Thm. 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 Thm. 9.10 to produce a finite flat flat morphism

$$g : \mathcal{M}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+,m;a} \to \mathcal{M}^{\mathrm{ord}}_{E,m}\,,$$

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 $y_0 \in \mathcal{M}^{\mathrm{ord}}_{E,m;a}(\mathbb{F})$ such that the following properties are satisfied.

(i) There is a projective system $\widetilde{\mathcal{M}}^{\mathrm{ord}}_{E,\mathcal{L},\mathcal{L}^+;a}$ of finite étale coverings of $\mathcal{M}_{E,m;a}$ on which the group $\mathrm{SL}_2(E\otimes\mathbb{A}_f^{(p)})$ operates. This $\mathrm{SL}_2(E\otimes\mathbb{A}_f^{(p)})$-action induces Hecke correspondences on $\mathcal{M}^{\mathrm{ord}}_{E,m;a}$

(ii) The morphism g is equivariant w.r.t. Hecke correspondences coming from the group $\mathrm{SL}_2(E\otimes \mathbb{A}_f^{(p)})$. In other words, there is a $\mathrm{SL}_2(E\otimes\mathbb{A}_f^{(p)})$-equivariant morphism $\tilde{g}$ from the projective system $\widetilde{\mathcal{M}}^{\mathrm{ord}}_{E,a}$ to the projective system $\left(\mathcal{M}^{\mathrm{ord}}_{E,mn}\right)_{n\in\mathbb{N}-p\mathbb{N}}$ which lifts g.

(iii) The finite morphism f is Hecke equivariant w.r.t. 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 $z \in \mathcal{M}^{\mathrm{ord}}_{E,m;a}$, 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 $\mathcal{A}^{\mathrm{ord}}_{g,n}(\mathbb{F})$.

(v) We have $f(y_0) = x_0$.

Let $y := g(y_0) \in \mathcal{M}^{\mathrm{ord}}_{E,m}$.

Step 2. Let Z_y be the Zariski closure of the $\mathrm{SL}_2(E\otimes\mathbb{A}_f^{(p)})$-Hecke orbit of y on $\mathcal{M}^{\mathrm{ord}}_{E,m;c}$, and let Z_{y_0} 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 Thm. 9.2, the $\mathrm{SL}_2(E\otimes\mathbb{A}_f^{(p)})$-Hecke orbits of $Z_y = \mathcal{M}_{E,\mathcal{L},\mathcal{L}^+,m}$. 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 $\mathcal{M}_{E,m}$ such that $A_{y_1} = E_1 \otimes_{\mathbb{Z}} \mathcal{O}_E$ and $\mathcal{L}_{y_1}$ contains the $\lambda_{E_1}\otimes\mathcal{O}_E$, and λ_{E_1} is 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 $\mathcal{O}_E$.

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 $\mathrm{SU}(\mathrm{End}^0(A_{x_1}), \lambda_{x_1})$ consisting of all elements $\gamma \in \mathrm{SU}(\mathrm{End}^0(A_{x_1}), \lambda_{x_1})(\mathbb{Q}_p)$ such that $\gamma(A_{x_1}[p^\infty]) = A_{x_1}[p^\infty]$. By Thm. 2.27, $Z(x)^{/x_1}$ is a formal subtorus of the formal torus $\mathcal{A}_{g,n}^{/x_1}$, 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 $\mathrm{SU}(\mathrm{End}^0(A_{x_1}), \lambda_{x_1})(\mathbb{Q}_p) \cong \mathrm{GL}_g(\mathbb{Q}_p)$ 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. $\square$

§10. Notations

(10.1) Warning. In most recent papers there is a distinction 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 a confusion between on the one hand A/K and "the same" abelian variety over any extension field. In such papers there is a confusion. 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 $\mathrm{End}(X \times_S T)$.

(10.2) We write $\mathrm{End}(A)$ for the endomorphism ring of A and $\mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ 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. We write:

$$[L_0 : \mathbb{Q}] = e_0, \quad [L : \mathbb{Q}] = e, \quad [D : L] = d^2.$$

(10.3) The Rosati involution $\dagger : D \to D$ is positive definite.
definition. *A simple division algebra of finite degree over $\mathbb{Q}$ with a positive definite anti-isomorphism which is positive definite is called an Albert algebra.*
Applications to abelian varieties and the classification have been described by Albert, [1], [2], [3].

(10.4) 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 an 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 $[D : L] = d^2$.

(10.5) 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 [18], page 63, see [58], 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 he notion "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 10.7. By Grothendieck we know that an abelian variety which admits smCM up to isogeny is defined over a finite field, see 10.9.

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 multplication 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. However 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.

(10.6) Exercise. *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.

(10.7) Theorem (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 10.5. *We have:*

$$f_A \quad = \quad (\mathrm{Irr}_{\pi_A})^{\sqrt{[D:L]}}.$$

(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*

$$\mathrm{inv}_v(D/L) = \frac{v(\pi_A)}{v(q)} \cdot [L_v : \mathbb{Q}_p] \mod 1,$$

where L_v is the local field obtained from L by completing at v.
See [87], [88].

(10.8) Remark. An abelian variety over a field of characteristic zero which admits smCM is defined over a number field.

(10.9) Remark. The converse of Tate's result 10.7 (2) is almost true. Grothendieck showed: *Let A be an abelian variety over a field which admits smCM; then A is isogenous with an abelian variety defined over a finite extension of the prime field*; see [66].

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.

(10.10) Exercise. *Give an example of a simple abelian variety A over a field K such that $A \otimes \overline{K}$ is not simple.*

(10.11) We 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 of characteristic p.

We write $\mathcal{A}_g$ for the moduli space of polarized abelian varieties of dimension g in characteristic p (this we write instead of $\mathcal{A}_g \otimes \mathbb{F}_p$). If we write "work over K" we mean that we consider $\mathcal{A}_g \otimes K$. We write $\mathcal{A}_{g,d}$ in case only polarizations of degree d^2 are considered. We write $\mathcal{A}_{g,d,n}$ by considering polarized abelian varieties with a symplectic level-n-structure; in this case it is assumed that n is not divisible by p.

The dimension of an abelian variety usually we will denote by g. If $m \in \mathbb{Z}_{>1}$ and A is an abelian variety we write $A[m]$ for the the group scheme of m-torsion. Note that if m is not divisible by p, then $A[m]$ is a group scheme étale over K; in this case it is uniquely determined by the Galois module $A[m](k)$. If p divides m, then $A[m]$ is a group scheme which is not reduced.

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, flat group scheme. We write $N^D \to S$ for its Cartier dual, see [67], I.2.

(10.12) For the definition of an abelian variety, an abelian scheme, see [59], II.4, [57], 6.1. The dual of an abelian scheme $A \to S$ will be denoted by $A^t \to S$, denoted by $\hat{A}$ in [57], 6.8.

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, [57], Lemma 6.12. This defines a dual isogeny $\varphi^t : B^t \to A^t$. And see 1.10.

A divisor D on an abelian scheme A/S defines a morphism $\varphi_D : A \to A^t$, see [59], theorem on page 125, see see [57], 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 [59], Application 1 on page 60, and [57], 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 canonical.

Writing $\varphi : (B, \mu) \to (A, \lambda)$ we mean that $\varphi : A \to A$ and $\varphi^*(\lambda) = \mu$, i.e.

$$\mu = \left(B \xrightarrow{\mu} A \xrightarrow{\lambda} A^t \xrightarrow{\mu^t} B^t\right).$$

(10.13) 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 [84], Exp. VII_A.4. The notation $A^{(p/S)}$ is (maybe) more correct.

Example. 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 given by $\sum_I a_I^p X^I$, 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 $(x_1^p, \cdots, x_n^p) \in A^{(p)}$, 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 $F_T = \mathrm{fr} : T \to T$.

(10.14) Verschiebung. Let A be a *commutative* group scheme over a characteristic p base scheme. In [84], 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 surjective, and $\mathrm{Ker}(F_A) \subset A[p]$. In this case we do not need the somewhat tricky construction of [84], Exp. VII_A.4, but we can define V_A by $V_A{\cdot}F_A = [p]_A$ and check that $F_A{\cdot}V_A = [p]_{A^{(p)}}$.

bf Remark. 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 [71], 15.3.

(10.15) Algebraization. (1) Suppose given a formal p-divisible group X_0 over k with $\mathcal{N}(X_0) = \gamma$ ending at (h, c). We write $D = \mathcal{D}ef(G_0)$ 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 $\mathcal{X}' \to \mathrm{Spf}(A)$. However "a finite group scheme over a formal scheme actually is already defined over an actual scheme". Indeed, by [40], 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 Spec(R). We will say that $\mathcal{X} \to \mathrm{Spec}(R) = D = \mathrm{Def}(X_0)$ is the universal deformation of X_0 if the corresponding $\mathcal{X}' \to \mathrm{Spf}(R) = \mathcal{D}^{\wedge}$ 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 $X/\mathrm{Spec}(R)$.

(2) Let A_0 be an abelian variety. The deformation functor $\mathrm{Def}(A_0)$ is prorepresentable. We obtain the universal 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. Then we can use the Chow-Grothendieck theorem, see [33], $\mathrm{III}^1.5.4$ (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 $\mathrm{Spec}(R)$.

The subtle differences between (1), (2) and (3) will be used without further mention.

(10.16) Theorem (Irreducibility of moduli spaces.) $\boxed{\textbf{BB}}$ *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 p[rime 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 [26], at the same time by Chai in his Harvard PhD-thesis; also see [27], IV.5.10. for a pure characteristic-p-proof see [71], 1.4.

(10.17) Etale 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 algebras etale and finite over K, 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 etale finite group schemes over K and the category of finite continuous G-modules.*
See [91], 6.4. Note that this equivalence also holds in the case of not necessarily commutative group schemes.

Naturally this can be generalized to: let S be a connected scheme, and let $s \in S$ be a base point; let $\pi = \pi_1(S, s)$. *There is an equivalence between the category of etale finite group schemes* (not necessarily commutative) *over S and the category of finite continuous π-sets.*

§11. A remark and a question

(11.1) In 1.16 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 [74]: Hecke-prime-to-p actions "move" a point in a central leave, and Hecke actions only involving compositions of isogenies with kernel isomorphic with α_p "move" a point in an isogeny leaf; 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 1.16 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 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 and see 1.17, and an isogeny leaf of a supersingular point is the whole supersingular locus.

In order to finish a proof of 1.16 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) In Section 5, in particular see the proofs of 5.8 and 5.14 we have seen a natural way of introducing coordinates in the formal completion at a point where $a \leq 1$ on an (open) Newton polygon stratum. It would be nice to have a better understanding and interpretation of these "coordinates".

In particular we could try to investigate whether a subset of these gives coordinates along a central leaf; note that the dimension of a leaf can be given by counting points in a certain Newton polygon region, see [77], 8.3 and 9.3; hence there is an obvious choice of a sub-coordinate-system, and we can wonder whether these coordinates are along the central leaf through this point.

References

[1] A. A. Albert – *On the construction of Riemann matrices, I, II.* Ann. Math. **35** (1934), 1 – 28; **36** (1935), 376 – 394.

[2] A. A. Albert – *A solution of the principal problem in the theory of Riemann matrices.* Ann. Math. **35** (1934), 500 – 515.

[3] A. A. Albert – *Involutorial simple algebras and real Riemann matrices.* Ann. Math. **36** (1935), 886 – 964.

[4] P. Berthelot, L. Breen & W. Messing – *Théorie de Dieudonné Cristalline II.* Lecture Notes Math. 930, Springer-Verlag, 1982.

[5] C. Birkenhake & H. Lange – *Complex tori.* Progr. Math. 177, Birkhäuser 1999.

[6] P. Cartier – *Groupes formels associés aux anneaux de Witt géneralisés.* Compt. Rend. Acad. Sc. Paris **265** (1967), 50 – 52.

[7] P. Cartier – *Modules associés à un groupe formel commutatif.* Compt. Rend. Acad. Sc. Paris **265** (1967), 129 – 132.

[8] C.-L. Chai - *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli space.* Invent. Math. **121** (1995), 439 – 479.

[9] C.-L. Chai - *Hecke orbits on Siegel modular varieties.* Progress in Mathematics **235**, Birkhäuser, 2004, pp. 71–107.

[10] C.-L. Chai - *Monodromy of Hecke-invariant subvarieties.* Pure Appl. Math. Quaterly **1** (Special issue: in memory of Armand Borel), 291 – 303.

[11] C.-L. Chai - *A rigidity result for p-divisible formal groups.* Preprint.

[12] C.-L. Chai - *Families of ordinary abelian varieties: canonical coordinates, p-adic monodromy, Tate-linear subvarieties and Hecke orbits.* Preprint.

[13] C.-L. Chai & F. Oort – *Hypersymmetric abelian varieties.* [To appear Quarterly Journal of Pure and Applied Mathematics]

[14] C.-L. Chai & F. Oort – *Monodromy and irreducibility of leaves.* Conference on abelian varieties, Amsterdam May 2006.

[15] C.-L. Chai & F. Oort – *Hecke orbits.* [In preparation]

[16] G. Cornell, J. H. Silverman (Editors) – *Arithmetic geometry.* Springer – Verlag 1986.

[17] P. Deligne – *Variétés abéliennes ordinaires sur un corps fini.* Invent. Math. **8** (1969), 238 – 243.

[18] P. Deligne – *Hodge cycles on abelian varieties.* Hodge cycles, motives and Shimura varieties (Eds P. Deligne et al). Lect. Notes Math. **900**, Springer – Verlag 1982; pp. 9 - 100.

[19] P. Deligne & G. Pappas – *Singularités des espaces de modules de Hilbert, en les caractéristiques divisant le discriminant.* Compos. Math. **90**, 59 – 79.

[20] P. Deligne & K. Ribet – *Values of abelian L-functions at negative integers over totally real fields.* Invent. Math. **59** (1980), 227 – 286.

[21] M. Demazure – *Lectures on p-divisible groups.* Lect. Notes Math. 302, Springer – Verlag, Berlin 1972.

[22] M. Demazure & P. Gabriel – *Groupes algébriques.* Tome 1: géométrie algébrique - généralités - groups commutatifs. Masson & Cie, North – Holland Publ. Cy, 1970.

[23] T. Ekedahl – *On supersingular curves and abelian varieties.* Math. Scand. **60** (1987), 151 – 178.

[24] T. Ekedahl & G. van der Geer – *Cycle classes of the E-O stratification on the moduli of abelian varieties.* Manuscript XII-2004; 60 pp.

[25] G. Faltings – *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), 349 – 366.

[26] G. Faltings – *Arithmetische Kompaktifizierung des Modulraums der Abelschen Varietäten.* Arbeitstagung Bonn 1984, Proceedings. Lecture Notes Math. 1111, Springer - Verlag 1984.

[27] G. Faltings & C.-L. Chai – *Degeneration of abelian varieties.* Ergebn. Math. 3 Folge, Bd 22, Springer - Verlag, 1990.

[28] G. Faltings & G. Wüstholz – *Rational points.* Seminar Bonn / Wuppertal 10983/84. Asp. Math. E6, Vieweg 1984.

[29] G. van der Geer – *Hilbert Modular Surfaces* Ergebnisse Bd 16, Springer-Verlag, 1988.

[30] G. van der Geer & B. Moonen – *Abelian varieties.* [In preparation]
See `http://staff.science.uva.nl/∼bmoonen/boek/BookAV.html`

[31] L. Gerritzen – *On multiplications of Riemann matrices.* Math. Ann **194** (1971), 109 – 122.

[32] E. Z. Goren & F. Oort - *Stratifications of Hilbert modular varieties.* Journ. Algebraic Geom. **9** (2000), 111-154.

[33] A. Grothendieck & J. Dieudonné - *Eléments de géométrie algébrique. Ch. III*[1]*: Etude cohomologique des faisceaux cohérents.* Publ. Math. **11**, IHES 1961.

[34] A. Grothendieck – *Groupes de Barsotti-Tate et cristaux de Dieudonné.* Sém. Math. Sup. **45**, Presses de l'Univ. de Montreal, 1970.

[35] A. Grothendieck – *Esquisse d'un programme,* 1972. Reproduced in: L. Schneps & P. Lochak – Geometric Galois actions, Vol 1. Around Grothendieck's Esquisse d'un programme. London Math. Soc. Lecture Note Series **242**, Cambridge Univ. Press, 1997, pp. 5 – 48.
In the same volume: Grothendieck – Brief an G. Faltings, 27 - VI - 1983, pp. 49 – 58.

[36] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, 1978.

[37] T. Honda – *Isogeny classes of abelian varieties over finite fields.* Journ. Math. Soc. Japan **20** (1968), 83 – 95.

[38] T. Ibukiyama, T. Katsura & F. Oort - *Supersingular curves of genus two and class numbers.* Compos. Math. **57** (1986), 127 – 152.

[39] L. Illusie – *Déformations de groupes de Barsotti-Tate.* Exp.VI in: Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell (L. Szpiro), Astérisque 127, Soc. Math. France 1985.

[40] A. J. de Jong - *Crystalline Dieudonné module theory via formal rigid geometry.* Publ. Math. IHES **82** (1995), 5 – 96.

[41] A. J. de Jong – *Homomorphisms of Barsotti-Tate groups and crystals in positive characteristics.* Invent. Math. **134** (1998) 301-333, Erratum **138** (1999), 225.

[42] A. J. de Jong – *Barsotti-Tate groups and crystals.* Documenta Mathematica, Extra Volume ICM 1998, II, 259 – 265.

[43] A. J. de Jong & F. Oort – *Purity of the stratification by Newton polygons.* Journ. A.M.S. **13** (2000), 209 – 241.

[44] T. Katsura & F. Oort - *Families of supersingular abelian surfaces.* Compos. Math. **62** (1987), 107 – 167.

[45] T. Katsura & F. Oort - *Supersingular abelian varieties of dimension two or three and class numbers.* Algebraic geometry, Sendai 1985 (Ed. T. Oda). Adv. Stud. in Pure Math. **10** (1987), Kinokuniya Cy Tokyo and North-Holland Cy Amsterdam, 1987 ; pp. 253 – 281.

[46] N. M. Katz – *Appendix to Expose V.* In: Surfaces algébriques (Ed. J. Giraud, L. Illusie, M. Raynaud). Lect. Notes Math. 868, Springer – Verlag, Berlin 1981; pp. 127 – 137.

[47] N. M. Katz – *Serre-Tate local moduli.* In: Surfaces algébriques (Ed. J. Giraud, L. Illusie, M. Raynaud). Lect. Notes Math. 868, Springer – Verlag, Berlin 1981; pp. 138 - 202.

[48] N. M. Katz – *Slope filtration of F–crystals.* Journ. Géom. Alg. Rennes, Vol. I, Astérisque **63** (1979), Soc. Math. France, 113 - 164.

[49] M. Lazard – *Commutative Formal Groups.* Lecture Notes in Math. 443, Springer, 1975.

[50] K.-Z. Li & F. Oort – *Moduli of supersingular abelian varieties.* Lecture Notes Math. 1680, Springer - Verlag 1998

[51] Yu. I. Manin - *The theory of commutative formal groups over fields of finite characteristic.* Usp. Math. **18** (1963), 3–90; Russ. Math. Surveys **18** (1963), 1–80.

[52] W. Messing – *The Crystals Associated to Barsotti-Tate Groups.* Lecture Notes Math. 264, Springer-Verlag, 1972.

[53] J. S. Milne – *Motives over finite fields.* Proc. Symp. Pure. Math. **55**, Part 1, 1994, 401–459.

[54] S. Mochizuki – *The local pro-p anabelian geometry of curves.* Invent. Math. **138** (1999), 319 – 423.

[55] B. Moonen – *Serre-tate theory for moduli spaces of* PEL *type.* Ann. sc. Ec. Norm. Sup. **37** (2004), 223-269.

[56] L. Moret-Bailly – *Pinceaux de variétés abéliennes.* Astérisque 129. Soc. Math. France 1985.

[57] S. Mori – *On Tate's conjecture concerning endomorphisms of abelian varieties.* Itl. Sympos. Algebr. Geom. Kyoto 1977 (Ed. M. Nagata). Kinokuniya Book-store, 1987, pp. 219 – 230.

[58] D. Mumford – *Geometric invariant theory.* Ergebn. Math. 34, Springer – Verlag, 1965. Second edition: D. Mumford & J. Fogarty, Springer – Verlag, 1982. Third enlarged edition: D. Mumford, J. Fogarty & F. Kirwan, Springer – Verlag, 1994.

[59] D. Mumford – *A note on Shimura's paper "Discontinuous groups and abelian varieties".* Math. Ann **181** (1969), 345 – 351.

[60] D. Mumford – *Abelian Varieties.* Tata Inst. Fund. Res. Studies in Math. **5**, Oxford University Press, 1974.

[61] D. Mumford – *Biextensions of formal groups.* In *Algebraic Geometry*, Proceedings of Internat. Coll. Bombay, 1968, Oxford Univ. Press, 1969, 307–322.

[62] P. Norman – *An algorithm for computing local moduli of abelian varieties.* Ann. Math. **101** (1975), 499 – 509.

[63] P. Norman – *Intersections of components of the moduli space of abelian varieties.* Journ. Pure Appl. Math. **13** (1978), 105 – 107. Norman-int

[64] P. Norman & F. Oort – *Moduli of abelian varieties.* Ann. Math. **112** (1980), 413 – 439. Norman-FO

[65] T. Oda & F. Oort – *Supersingular abelian varieties.* Itl. Sympos. Algebr. Geom. Kyoto 1977 (Ed. M. Nagata). Kinokuniya Book-store 1987, pp. 3 - 86. Oda.FO

[66] F. Oort – *Algebraic group schemes in characteristic zero are reduced.* Invent. Math. **2** (1966), 79 - 80.

[67] F. Oort – *The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field.* Journ. Pure Appl. Algebra **3** (1973), 399 - 408.

[68] F. Oort – *Commutative group schemes.* Lect. Notes Math. 15, Springer - Verlag 1966.

[69] F. Oort – *Endomorphism algebras of abelian varieties.* Algebraic Geometry and Commut. Algebra in honor of M. Nagata (Ed. H. Hijikata et al), Kinokuniya Cy Tokyo, Japan, 1988, Vol II; pp. 469–502.

[70] F. Oort – *Some questions in algebraic geometry,* preliminary version. Manuscript, June 1995. http://www.math.uu.nl/people/oort/

[71] F. Oort — *Newton polygons and formal groups: conjectures by Manin and Grothendieck.* Ann. Math. **152** (2000), 183 - 206.

[72] F. Oort – *A stratification of a moduli space of polarized abelian varieties.* In: *Moduli of abelian varieties.* (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. 195, Birkhäuser Verlag 2001; pp. 345 - 416.

[73] F. Oort – *Newton polygon strata in the moduli space of abelian varieties.* In: *Moduli of abelian varieties.* (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. 195, Birkhäuser Verlag 2001; pp. 417 - 440.

[74] F. Oort – *Purity reconsidered.* Talk, Amsterdam XII-2002, ms 9 pp. See: `http://www.math.uu.nl/people/oort/`

[75] F. Oort – *Foliations in moduli spaces of abelian varieties.* Journ. A. M. S. **17** (2004), 267–296.

[76] F. Oort – *Monodromy, Hecke orbits and Newton polygon strata* Manuscript. Seminar Algebraic Geometry, Bonn, 24 - II - 2003; 9 pp.
See: http://www.math.uu.nl/people/oort/

[77] F. Oort – *Minimal p-divisible groups.* Annals of Math **161** (2005), 1021 – 1036.

[78] *Foliations in moduli spaces of abelian varieties and dimension of leaves.* Felix-Klein-Kolloquium, Düsseldorf 2 - VII - 2005. Manuscript 20 pp. 2005
See: http://www.math.uu.nl/people/oort/

[79] F. Oort & T. Zink – *Families of p-divisible groups with constant Newton polygon.* Documenta Mathematica **7** (2002), 183 – 201.
See: http://www.mathematik.uni-bielefeld.de/ documenta/vol-07/09.html

[80] V. Platonov & A. Rapinchuk – *Algebraic groups and number theory.* Academic Press 1994.

[81] M. Rapoport – *Compactifications de l'espace de modules de Hilbert-Blumenthal.* Compos. Math. **36** (1978), 255 - 335.

[82] K. Ribet – *p-adic interpolation via Hilbert modular forms.* Proceed. Sympos. Pure Math. **29** (1975), 581 – 592.

[83] M. Rapoport & Th. Zink – *Period spaces for p-divisible groups.* Ann. Mat. Studies 141, Princeton University Press, 1996.

[84] M. Raynaud – *p-torsion du schéma de Picard.* Astérisque **64** (1973), 87–148.

[85] *Schémas en groupes, Séminaire de géométrie algébrique, SGA3.* M. Demazure & A. Grothendieck. Vol I: Lecture Notes Math. 151, Springer – Verlag 1970.

[86] G. Shimura & Y. Taniyama – *Complex multiplication of abelian varieties and its applications to number theory.* Publ. Math. Soc. Japan 6; 1961.

[87] G. Shimura – *On analytic families of polarized abelian varieties and automorphic functions.* Ann. Math. **78** (1963), 149 – 193.

[88] J. Tate – *Endomorphisms of abelian varieties over finite fields.* Invent. Math. **2** (1966), 134–144.

[89] J. Tate – *Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T. Honda).* Sém. Bourbaki, **21** , 1968/69, Exp. 352, Lect. Notes Math. **179**, 1971, pp. 95–110.

[90] A. Vasiu – *Crystaline boundedness principle.* Final version 15-XII-2005, 63 pp., arXiv:math.NT/-2-5199 v5, 4-I-2006.

[91] W. C. Waterhouse – *Abelian varieties over finite fields.* Ann. Sc. Ec. Norm. Sup. 4.Ser, **2** (1969), 521 – 560).

[92] W. C. Waterhouse – *Introduction to affine group schemes.* Grad. Texts Math. 66, Springer – Verlag, 1979. Waterhouse-Introd

[93] W. C. Waterhouse & J. S. Milne – *Abelian varieties over finite fields.* Proc. Sympos. Pure Math. Vol. **20**, 1969 Number Theory Institute (Stony Brook), AMS 1971, pp. 53 – 64.

[94] A. Weil – *Sur les courbes algébriques et les variétés qui s'en déduisent.* Hermann 1948.

[95] A. Weil – *Variétés abéliennes et courbes algébriques.* Hermann 1948.

[96] C.-F. Yu – *On the supersingular locus in the Hilbert-Blumenthal 4-folds.* J. Alg. Geom. **12** (2003), 653–698.

[97] C.-F. Yu – *On reduction of Hilbert-Blumenthal varieties.* Ann. Inst. Fourier Grenoble, **53** (2003), 2105–2154.

[98] C.-F. Yu – *Discrete Hecke orbit problem for Hilbert-Blumenthal varieties.* Preprint, 20 pp., Oct. 11, 2004.

[99] J. G. Zarhin – *Isogenies of abelian varieties over fields of finite characteristic.* Math. USSR Sbornik **24** (1974), 451 – 461.

[100] J. G. Zarhin – *A remark on endomorphisms of abelian varieties over function fields of finite characteristic.* Math. USSR Izv. **8** (1974), 477 – 480.

[101] T. Zink – *Cartiertheorie kommutativer formaler Gruppen.* Teubner-Texte Bd 68, Teubner 1984.

[102] T. Zink - *The display of a formal p-divisible group. Astérisque* **278**, 2002, 127–248.

[103] T. Zink - *A Dieudonné theory for p-divisible groups.* Manuscript, 23 pp., September 1998.

[104] T. Zink – *On the slope filtration.* Duke Math. Journ. **109** (2001), 79 - 95.

Ching-Li Chai
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
USA
email: chai@math.upenn.edu

Frans Oort
Mathematisch Instituut
Budapestlaan 6
NL - 3584 CD TA Utrecht
The Netherlands
email:oort@math.uu.nl

Postbus 80010
NL - 3508 TA Utrecht
The Netherlands