Zariski density of CM points on products of modular curves

Masami Ohta

Abstract

We prove the Zariski density of certain set of CM points lying in self-products of elliptic modular curves, considered by Hida. A new ingredient in our argument is a finiteness result on irreducible components for the inverse images in infinite coverings of self-products of modular curves.

Introduction.

The purpose of this paper is to prove the Zariski density of CM points on products of elliptic modular curves, as formulated and announced by Hida [H1], [H3]. (Hida considered general Hilbert modular varieties, but we only treat the elliptic modular case in this paper.) It was one of the key result for the proof of the non-vanishing modulo p result for special values of Hecke L-functions twisted by anti-cyclotomic characters; [H1]-[H3]. Aside from its own interest, Vatsal [V] applied the non-vanishing modulo p result to the study of μ-type subgroups of the modular Jacobian variety $J_0(N)$, together with an application to a conjecture of Stevens. The author [O], following Vatsal's method, studied μ-type subgroups of $J_1(N)$, and applied it to a conjecture of Sharifi.

Unfortunately, the original proof of the Zariski density was incomplete, as pointed out by Venkatesh; cf. [H4]. Hida, in the same paper, recovered his results under an additional assumption (also in the Hilbert modular case), but the Zariski density in the full generality seems remained open so far. We will supply a proof for this lacuna.

We now explain the main result. Let us fix an imaginary quadratic field K, a prime number p which splits in K, and a prime number ℓ different from p. Let Cl_n be the proper ideal class group of conductor ℓ^n of K and set $\mathrm{Cl}_\infty := \varprojlim_n \mathrm{Cl}_n$. Each class $\mathrm{cl}(\mathfrak{a}) \in \mathrm{Cl}_n$ determines an isomorphism class of a CM elliptic curve over $\overline{\mathbb{Q}}$, and then an ordinary elliptic curve over an algebraic closure $\mathbb{F}$ of the prime field $\mathbb{Z}/p\mathbb{Z}$, by reduction. This determines a closed point $x(\mathfrak{a})_{/\mathbb{F}}$ of the coarse moduli scheme $Y(1)_{/\mathbb{F}}$ of elliptic curves over $\mathbb{F}$. The group Cl_∞ acts on the set of $x(\mathfrak{a})_{/\mathbb{F}}$ through its projections to Cl_n. On the other hand, Hida introduced a certain subgroup $\mathrm{Cl}^{\mathrm{alg}}$ of Cl_∞.

2020 *Mathematics Subject Classification.* Primary 11G18; Secondary 14G35.
Key Words and Phrases. modular curves, CM points, Zariski density.

Take and fix an infinite sequence of non-negative integers $\underline{n} := \{n_0 < n_1 < \cdots\}$, and set

$$\xi(1;\underline{n})_{/\mathbb{F}} := \{x(\mathfrak{a})_{/\mathbb{F}} \mid \mathrm{cl}(\mathfrak{a}) \in \mathrm{Ker}(\mathrm{Cl}_{n_j} \to \mathrm{Cl}_{n_0}), n_j \in \underline{n}\} \subset Y(1)_{/\mathbb{F}}.$$

Then take $\delta_1, \cdots, \delta_m \in \mathrm{Ker}(\mathrm{Cl}_\infty \to \mathrm{Cl}_{n_0})$ which give different classes in $\mathrm{Cl}_\infty/\mathrm{Cl}^{\mathrm{alg}}$. Define

$$\Xi(1;\underline{n})_{/\mathbb{F}} := \{(x(\delta_1\mathfrak{a})_{/\mathbb{F}}, \cdots, x(\delta_m\mathfrak{a})_{/\mathbb{F}}) \mid x(\mathfrak{a})_{/\mathbb{F}} \in \xi(1;\underline{n})_{/\mathbb{F}}\}$$

which is a set consisting of closed points of $(Y(1)_{/\mathbb{F}})^m$, the self-product of m copies of $Y(1)_{/\mathbb{F}}$ over $\mathbb{F}$.

Let $Y(M)_{/\mathbb{F}}$ be the modular curve classifying elliptic curves with a $\Gamma(M)$-structure (in the terminology of Katz and Mazur [KM]) over $\mathbb{F}$-schemes, for M prime to p. We set $Y^{(p)}(\infty)_{/\mathbb{F}} := \varprojlim_{p\nmid M} Y(M)_{/\mathbb{F}}$ and take its one irreducible component $Y^{(p)}(\infty)^0_{/\mathbb{F}}$. This determines an irreducible component $Y(M)^0_{/\mathbb{F}}$ of each $Y(M)_{/\mathbb{F}}$ so that $Y^{(p)}(\infty)^0_{/\mathbb{F}} = \varprojlim_{p\nmid M} Y(M)^0_{/\mathbb{F}}$. With these terminologies, the main result of this paper, which is equivalent to [H3, Proposition 8.28], can be stated as follows:

Theorem 1 *Let M be a positive integer prime to p (resp. $M = \infty$), and let $\Lambda(M)$ be a set of closed point of $(Y(M)^0_{/\mathbb{F}})^m$ (resp. $(Y^{(p)}(\infty)^0_{/\mathbb{F}})^m$) mapping surjectively onto $\Xi(1;\underline{n})_{/\mathbb{F}}$. Then $\Lambda(M)$ is a Zariski dense subset of $(Y(M)^0_{/\mathbb{F}})^m$ (resp. $(Y^{(p)}(\infty)^0_{/\mathbb{F}})^m$).*

As in Hida's argument, it is necessary to use infinite coverings of $(Y(1)_{/\mathbb{F}})^m$ like $(Y^{(p)}(\infty)^0_{/\mathbb{F}})^m$ to prove the theorem. A new point of our argument is the following finiteness result for the irreducible components, which allows us to avoid the situation described by an example of Venkatesh:

Theorem 2 *Take and fix an integer $N_0 \geq 3$ prime to p, and Let Z be an irreducible closed subvariety of $(Y(N_0)^0_{/\mathbb{F}})^m$ defined over $\mathbb{F}$ such that:*

i) *The composite of $Z \hookrightarrow (Y(N_0)^0_{/\mathbb{F}})^m \xrightarrow{p_i} Y(N_0)^0_{/\mathbb{F}}$ is dominant for each i $(1 \leq i \leq m)$, where p_i is the projection to the i-th direct factor.*

ii) *Let $E_{Z,i}$ be the pull-back of the universal elliptic curve on $Y(N_0)^0_{/\mathbb{F}}$ to Z by the above morphism $(1 \leq i \leq m)$. Then if $i \neq j$, the generic geometric fibres of $E_{Z,i}$ and $E_{Z,j}$ are not isogenous.*

Then the inverse image of Z to $(Y^{(p)}(\infty)^0_{/\mathbb{F}})^m$ has only a finite number of irreducible components.

Note that $\dim Z > 0$ by the condition i).

Here is a rough sketch of the proof of Theorem 2:

• If M is a positive multiple of N_0 prime to p, the étale covering $Y(M)^0_{/\mathbb{F}}$ of $Y(N_0)^0_{/\mathbb{F}}$ is a torsor under a subgroup of $SL_2(\mathbb{Z}/M\mathbb{Z})$, described in terms of the universal elliptic curve $\mathcal{E}$ on $Y(N_0)^0_{/\mathbb{F}}$. (For example, when $M = N_0M'$ with

M' prime to N_0, $Y(M)^0_{/\mathbb{F}}$ is $Y(N_0)^0_{/\mathbb{F}}$-isomorphic to the $SL_2(\mathbb{Z}/M'\mathbb{Z})$-torsor classifying isomorphisms $\underline{\mathbb{Z}/M'\mathbb{Z}} \times \underline{\mathbb{Z}/M'\mathbb{Z}} \xrightarrow{\sim} \mathcal{E}[M']$ of prescribed determinant.)

• It follows that the inverse image of Z to $(Y(M)^0_{/\mathbb{F}})^m$ is a torsor over Z described in terms of the elliptic curves $E_{Z,i}$ $(1 \leq i \leq m)$. The set of its irreducible components can be then studied in terms of the Galois representation on the M-division points of the generic fibre of $E_{Z,1} \times_Z \cdots \times_Z E_{Z,m}$.

• The finiteness claimed in the theorem ultimately reduces to a function field analogue of the open image theorem proved by Serre [Se3] and extended by Ribet [R] for products of elliptic curves over number fields.

When Z is a positive dimensional irreducible component of the Zariski closure $\overline{\Lambda(N_0)}$ of $\Lambda(N_0)$ as in Theorem 1, (the condition i) is easy and) the condition ii) in Theorem 2 is a consequence of our assumption that $\delta_1, \cdots, \delta_m$ give different classes in $\mathrm{Cl}_\infty/\mathrm{Cl}^{\mathrm{alg}}$. After Theorem 2, the proof of Theorem 1 basically goes along the track as in Hida's work, based on fundamental works of Chai [C1], [C2]. The notion of *Tate-linearlity* studied by Chai is indispensable in this part.

The organization of this paper is as follows:

Section 1 is preliminaries on modular curves. In this paper, we only consider (open) modular curves classifying (isomorphism classes of) elliptic curves with a $\Gamma(M)$-structure and their irreducible components, or the projective limits of these curves, such as $Y(M)_{/\mathbb{F}}$, $Y(M)^0_{/\mathbb{F}}$, $Y^{(p)}(\infty)_{/\mathbb{F}}$ or $Y^{(p)}(\infty)^0_{/\mathbb{F}}$ that already appeared. After fixing basic terminologies on them, we describe at some length the action of the adelic group, e.g. the action of $GL_2((\varprojlim_{p\nmid M} \mathbb{Z}/M\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q})$ extending the natural action of $GL_2(\varprojlim_{p\nmid M} \mathbb{Z}/M\mathbb{Z})$ on $Y^{(p)}(\infty)_{/\mathbb{F}}$, following Deligne's moduli theoretic description [D2]. We will need such action, via Subsection 2.4, in the proof of the Tate-linearity in the final Subsection 4.2.

In Section 2, we study the CM points on modular curves attached to K, p and ℓ as mentioned above. In Subsection 2.2, we recall Hida's definition of $\mathrm{Cl}^{\mathrm{alg}}$, and study its properties. Proposition (2.2.6) is a key to the proof of the property ii) in Theorem 2 for $Z \subseteq \overline{\Lambda(N_0)}$, to be given later in Subsection 4.1. After this, we state our main result Theorem (2.3.4) (= Theorem 1 above).

In the course of the proof of the Tate-linearity, we will consider special points on $Y^{(p,\ell)}(\infty)_{/\mathbb{F}} := \varprojlim_{p,\ell\nmid M} Y(M)_{/\mathbb{F}}$, the modular curve of infinite prime-to-$p\ell$ level, called *admissible CM points* specifying the level structures on CM elliptic curves. We study the properties of these points in detail in Subsection 2.4.

Section 3 is devoted to the proof of Theorem 2. In Subsections 3.2-3.3, we state and prove an analogue of Serre's open image theorem for products of two elliptic curves over function fields of one variable over $\mathbb{F}$ or its finite subfield. The method is completely due to Serre. We then use Ribet's group theoretic lemma to give its generalization for products of more than two elliptic curves over general function fields; cf. Theorem (3.4.2). After preliminary consideration on torsors attached to elliptic curves, we prove Theorem (3.6.4) (= Theorem 2

above) as an application of the open image theorem. Another application of this result, a consequence of Čebotarev density theorem, which will be used at the final step of the proof of our main theorem, is given at the end of this section.

In the final Section 4, we complete the proof of the main theorem. We prove a key result Proposition (4.2.2) on Tate-linearity (at appropriate points for suitably chosen $\Lambda(N_0)$ and Z, to be precise) using results from Sections 2 and 3, and finally deduce from it the main theorem.

§1. Preliminaries on modular curves.

1.1. Modular curves $Y(N)$. In this paper, we will exclusively consider modular curves with respect to the "naive" $\Gamma(N)$-moduli problems. For an elliptic curve E over a $\mathbb{Z}[1/N]$-scheme S, we thus consider its $\Gamma(N)$-*structures*, i.e. isomorphisms

$$\alpha_N : \underline{\mathbb{Z}/N\mathbb{Z}} \times \underline{\mathbb{Z}/N\mathbb{Z}} \xrightarrow{\sim} E[N] \tag{1.1.1}$$

of group schemes over S, where $E[N]$ denotes the kernel of multiplication by N on E, and we indicated by the underline the corresponding constant group scheme. We denote by

$$\boldsymbol{\mu}_N^{\mathrm{prim}} = \mathrm{Spec}(\mathbb{Z}[X]/\Phi_N(X)) \tag{1.1.2}$$

with $\Phi_N(X)$ the N-th cyclotomic polynomial, the scheme of primitive N-th roots of unity. If α_N is a $\Gamma(N)$-structure on E/S, we define its *determinant* by:

$$\det(\alpha_N) := e_{N,E}(\alpha_N \begin{pmatrix}1\\0\end{pmatrix}, \alpha_N \begin{pmatrix}0\\1\end{pmatrix}) \in \boldsymbol{\mu}_N^{\mathrm{prim}}(S) \tag{1.1.3}$$

using the e_N-pairing on E.

There is a natural right action of the group $GL_2(\mathbb{Z}/N\mathbb{Z})$ on the set of $\Gamma(N)$-structures on E/S:

$$\alpha_N \mapsto \alpha_N \circ g \text{ for } g \in GL_2(\mathbb{Z}/N\mathbb{Z}), \tag{1.1.4}$$

and we have

$$\det(\alpha_N \circ g) = \det(\alpha_N)^{\det(g)}. \tag{1.1.5}$$

Definition (1.1.6) We denote by $Y(N)$ the (coarse) moduli scheme classifying the (isomorphism classes of) pairs (E, α_N) as above over $\mathbb{Z}[1/N]$-schemes.

$Y(N)$ is an irreducible affine curve smooth over $\mathbb{Z}[1/N]$, and it is in fact the fine moduli scheme when $N \geq 3$. The correspondence $(E, \alpha_N) \mapsto \det(\alpha_N)$ gives a morphism $Y(N) \to \boldsymbol{\mu}_N^{\mathrm{prim}}$ over $\mathbb{Z}[1/N]$. Let μ_N be the group of N-th roots of unity in $\overline{\mathbb{Q}}$. Then the correspondences $X \mapsto \zeta_N$ for $\zeta_N \in \boldsymbol{\mu}_N^{\mathrm{prim}}(\overline{\mathbb{Q}})$ give us an isomorphism

$$\mathbb{Z}[X]/(\Phi_N(X)) \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \mu_N] \xrightarrow{\sim} \bigoplus_{\zeta_N} \mathbb{Z}[1/N, \zeta_N, \mu_N] = \bigoplus_{\zeta_N} \mathbb{Z}[1/N, \mu_N]$$

of $\mathbb{Z}[1/N,\mu_N]$-algebras. Therefore if we denote by $Y(N)^{(\zeta_N)}$ the base change of $Y(N)\to \boldsymbol{\mu}_N^{\mathrm{prim}}$ by the homomorphism given by $X\mapsto \zeta_N$, we obtain

$$Y(N)\otimes_{\mathbb{Z}[1/N]}\mathbb{Z}[1/N,\mu_N]\cong \coprod_{\zeta_N} Y(N)^{(\zeta_N)}\to \mathrm{Spec}(\mathbb{Z}[1/N,\mu_N]). \tag{1.1.7}$$

$Y(N)^{(\zeta_N)}$ is the moduli scheme classifying (E,α_N) with $\det(\alpha_N)=\zeta_N$ over $\mathbb{Z}[1/N,\mu_N]$-schemes, and it is geometrically irreducible over $\mathbb{Z}[1/N,\mu_N]$.

If M is a positive divisor of N, α_N above gives rise to a $\Gamma(M)$-structure α_M defined by the commutativity of the diagram:

$$\begin{array}{ccc} \underline{\mathbb{Z}/N\mathbb{Z}}\times\underline{\mathbb{Z}/N\mathbb{Z}} & \xrightarrow[\sim]{\alpha_N} & E[N] \\ {\scriptstyle\text{canon.}}\downarrow & & \downarrow{\scriptstyle N/M} \\ \underline{\mathbb{Z}/M\mathbb{Z}}\times\underline{\mathbb{Z}/M\mathbb{Z}} & \xrightarrow[\alpha_M]{\sim} & E[M]. \end{array} \tag{1.1.8}$$

We have

$$\det(\alpha_M)=\det(\alpha_N)^{N/M} \tag{1.1.9}$$

in this case. The association $(E,\alpha_N)\mapsto(E,\alpha_M)$ given by (1.1.8) induces natural morphisms

$$\begin{cases} Y(N)\to Y(M) \text{ over } \mathbb{Z}[1/N], \text{ and} \\ Y(N)^{(\zeta_N)}\to Y(M)^{(\zeta_N^{N/M})} \text{ over } \mathbb{Z}[1/N,\zeta_N^{N/M}]. \end{cases} \tag{1.1.10}$$

The action of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on $Y(N)$ gives isomorphisms

$$\begin{cases} GL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm1\}\xrightarrow{\sim}\mathrm{Aut}(Y(N)/Y(1)), \\ SL_2(\mathbb{Z}/N\mathbb{Z})/\{\pm1\}\xrightarrow{\sim}\mathrm{Aut}(Y(N)^{(\zeta_N)}/(Y(1)\otimes_{\mathbb{Z}}\mathbb{Z}[1/N,\mu_N])). \end{cases} \tag{1.1.11}$$

1.2. Towers of modular curves. We set

$$\begin{cases} \widehat{\mathbb{Z}}:=\prod_{q:\mathrm{prime}}\mathbb{Z}_q, \text{ and} \\ \mathbb{A}_{\mathrm{f}}:=\widehat{\mathbb{Z}}\otimes_{\mathbb{Z}}\mathbb{Q}, \text{ the ring of finite adeles of } \mathbb{Q}. \end{cases} \tag{1.2.1}$$

Slightly more generally, we take a finite set $\mathcal{P}$ of prime numbers and consider

$$\begin{cases} \widehat{\mathbb{Z}}^{(\mathcal{P})}:=\prod_{q\notin\mathcal{P}}\mathbb{Z}_q, \\ \mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}:=\widehat{\mathbb{Z}}^{(\mathcal{P})}\otimes_{\mathbb{Z}}\mathbb{Q}. \end{cases} \tag{1.2.2}$$

(We will later need these symbols only when $\mathcal{P}=\{p\}$ or $\{p,\ell\}$ with prime numbers p and $\ell\neq p$; but the general treatment requires no extra effort.)

We also consider the semilocal ring

$$\mathbb{Z}_{(\mathcal{P})}:=\{a/b\in\mathbb{Q}\mid a,b\in\mathbb{Z},\ b \text{ is not divisible by any element of } \mathcal{P}\} \tag{1.2.3}$$

(thus $\mathbb{Z}_{(\mathcal{P})} = \mathbb{Q}$ if $\mathcal{P}$ is empty). We say that a positive integer N is *prime to* $\mathcal{P}$ if N is not divisible by primes in $\mathcal{P}$; equivalently, if N is a unit in $\mathbb{Z}_{(\mathcal{P})}$. In this case, we can consider $Y(N)_{/\mathbb{Z}_{(\mathcal{P})}} := Y(N) \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}_{(\mathcal{P})}$.

When E is an elliptic curve over a $\mathbb{Z}_{(\mathcal{P})}$-scheme S, we set

$$\begin{cases} \widehat{T}^{(\mathcal{P})}(E) := (E[N])_{N:\text{prime to } \mathcal{P}}, \\ \widehat{V}^{(\mathcal{P})}(E) := \widehat{T}^{(\mathcal{P})}(E) \otimes \mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}. \end{cases} \tag{1.2.4}$$

Here, we consider $\widehat{T}^{(\mathcal{P})}(E)$ as a projective system of finite étale group schemes over S (with respect to $E[N] \overset{N/M}{\to} E[M]$ whenever M divides N), and also identify it with the associated smooth $\widehat{\mathbb{Z}}^{(\mathcal{P})}$-sheaf on the étale site $S_{\text{ét}}$ of S; and denote by $\widehat{V}^{(\mathcal{P})}(E)$ the $\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}$-sheaf on $S_{\text{ét}}$ associated with it: In [D2, N° 3], Deligne considered $\widehat{\mathbb{Z}}$-sheaves and $\mathbb{A}_{\mathrm{f}}$-sheaves (when $\mathcal{P} = \phi$), and we are using here the similar terminology for objects without q-components for $q \in \mathcal{P}$. When S is the spectrum of a field k, we will identify them with the usual ("physical") Tate module over $\widehat{\mathbb{Z}}^{(\mathcal{P})}$ or $\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}$ on which the absolute Galois group of k acts continuously.

Now we form the projective limit

$$Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}} := \varprojlim_{N:\text{prime to } \mathcal{P}} Y(N)_{/\mathbb{Z}_{(\mathcal{P})}} \tag{1.2.5}$$

which exists because transition morphisms $Y(N)_{/\mathbb{Z}_{(\mathcal{P})}} \to Y(M)_{/\mathbb{Z}_{(\mathcal{P})}}$ are all finite. For any $\mathbb{Z}_{(\mathcal{P})}$-scheme S, the set

$$Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}}(S) = \varprojlim_{N:\text{prime to } \mathcal{P}} Y(N)_{/\mathbb{Z}_{(\mathcal{P})}}(S)$$

corresponds bijectively with the set of isomorphism classes of the pairs consisting of an elliptic curve E/S together with an isomorphism of smooth $\widehat{\mathbb{Z}}^{(\mathcal{P})}$-sheaves on $S_{\text{ét}}$

$$\alpha_\infty^{(\mathcal{P})} : \underline{\widehat{\mathbb{Z}}}^{(\mathcal{P})} \times \underline{\widehat{\mathbb{Z}}}^{(\mathcal{P})} \overset{\sim}{\to} \widehat{T}^{(\mathcal{P})}(E). \tag{1.2.6}$$

(Here the underlined $\underline{\widehat{\mathbb{Z}}}^{(\mathcal{P})}$ means the constant $\widehat{\mathbb{Z}}^{(\mathcal{P})}$-sheaf on $S_{\text{ét}}$.) Such an isomorphism $\alpha_\infty^{(\mathcal{P})}$ will be called a $\Gamma^{(\mathcal{P})}(\infty)$-*structure* on E. We can naturally define its determinant

$$\det(\alpha_\infty^{(\mathcal{P})}) \in \boldsymbol{\mu}_\infty^{(\mathcal{P})\text{prim}}(\overline{\mathbb{Q}}) := \varprojlim_{N:\text{prim to } \mathcal{P}} \boldsymbol{\mu}_N^{\text{prim}}(\overline{\mathbb{Q}}). \tag{1.2.7}$$

On the other hand, if we denote by $\mu_\infty^{(\mathcal{P})}$ the set of all N-th roots of unity in $\overline{\mathbb{Q}}$ with N prime to $\mathcal{P}$, the set of irreducible components of $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]} := Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}} \otimes_{\mathbb{Z}_{(\mathcal{P})}} \mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]$ corresponds bijectively , via "det", with $\boldsymbol{\mu}_\infty^{(\mathcal{P})\text{prim}}(\overline{\mathbb{Q}})$

(cf. Appendix (A.2.1)). More precisely, if $(\zeta_N)_{N:\,\text{prime to}\,\mathcal{P}} =: \zeta_\infty$ is in this latter set, the corresponding component is given by

$$(1.2.8) \qquad Y^{(\mathcal{P})}(\infty)^{(\zeta_\infty)}_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]} := \varprojlim_{N:\,\text{prime to}\,\mathcal{P}} (Y(N)^{(\zeta_N)} \otimes_{\mathbb{Z}[1/N,\mu_N]} \mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}])$$

and this scheme represents the functor: $(\text{Schemes}/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]) \to (\text{Sets})$ associating with each S the isomorphism classes of the pairs $(E, \alpha_\infty^{(\mathcal{P})})$ of determinant ζ_∞ over S.

The group $GL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})/\{\pm 1\}$ acts faithfully on $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}}$ by the rule $(E, \alpha_\infty^{(\mathcal{P})}) \mapsto (E, \alpha_\infty^{(\mathcal{P})} \circ g)$. The action of $g \in GL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})/\{\pm 1\}$ on the set of irreducible components of $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]}$ then corresponds to the map: $\zeta_\infty \mapsto \zeta_\infty^{\det(g)}$, in the obvious sense, by (1.1.5). Especially, an element $g \in GL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})/\{\pm 1\}$ leaves each irreducible component stable if and only if $g \in SL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})/\{\pm 1\}$.

1.3. Action of $GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$. Let $\mathcal{P}$ be as in 1.2. In this subsection we consider the action of $GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$ on $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}}$ extending that of $GL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})$ following Deligne [D2, N° 3]. The existence of such an extension is a common feature of general Shimura varieties (cf. Shimura [Sh, 6.6] in the elliptic modular case). The following moduli theoretic description seems to be originally due to Shafarevich (according to [D2, loc. cit.]).

We call a morphism $E \to E'$ of elliptic curves over S a *prime-to-$\mathcal{P}$ isogeny* if it is an isogeny over S whose degree is (fibre-by-fibre) prime to $\mathcal{P}$. In the following, we let S be a scheme over $\mathbb{Z}_{(\mathcal{P})}$. We consider the *category of elliptic curves up to prime-to-$\mathcal{P}$ isogenies* over S, which for the moment will be denoted by $\mathcal{C}'_S$. Thus if we denote by $\mathcal{C}_S$ the category of elliptic curves over S, there is a functor

$$(1.3.1) \qquad \otimes\mathbb{Z}_{(\mathcal{P})} : \mathcal{C}_S \to \mathcal{C}'_S;\ E \mapsto E \otimes \mathbb{Z}_{(\mathcal{P})}$$

such that: (i) if f is a prime-to-$\mathcal{P}$ isogeny in $\mathcal{C}_S$, then it is sent to an isomorphism in $\mathcal{C}'_S$; and (ii) if $F : \mathcal{C}_S \to \mathcal{D}$ is a functor having the property (i), then it factors uniquely through $\otimes\mathbb{Z}_{(\mathcal{P})}$. When S is quasi-compact, we in fact have:

$$(1.3.2) \qquad \mathrm{Hom}_{\mathcal{C}'_S}(E \otimes \mathbb{Z}_{(\mathcal{P})}, E' \otimes \mathbb{Z}_{(\mathcal{P})}) = \mathrm{Hom}_{\mathcal{C}_S}(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_{(\mathcal{P})}$$

for E and E' in $\mathrm{Ob}(\mathcal{C}_S)$. An isomorphism in $\mathcal{C}'_S$ is often called a prime-to-$\mathcal{P}$ quasi-isogeny.

The functor on $\mathcal{C}_S$: $E \mapsto \widehat{V}^{(\mathcal{P})}(E)$ clearly factors through $\mathcal{C}'_S$. Thus we can consider, for each object F in $\mathcal{C}'_S$, the smooth $\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}$-sheaf $\widehat{V}^{(\mathcal{P})}(F)$, and also an isomorphism of smooth $\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}$-sheaves on $S_{\text{ét}}$, called a $\Gamma^{(\mathcal{P})}(\infty) \otimes \mathbb{Z}_{(\mathcal{P})}$-*structure* on F:

$$(1.3.3) \qquad \beta_\infty^{(\mathcal{P})} : \underline{\mathbb{A}}_{\mathrm{f}}^{(\mathcal{P})} \times \underline{\mathbb{A}}_{\mathrm{f}}^{(\mathcal{P})} \xrightarrow{\sim} \widehat{V}^{(\mathcal{P})}(F).$$

If $\alpha_\infty^{(\mathcal{P})}$ is a $\Gamma(\infty)^{(\mathcal{P})}$-structure on $E \in \mathrm{Ob}(\mathcal{C}_S)$, we can associate with it a $\Gamma(\infty)^{(\mathcal{P})} \otimes \mathbb{Z}_{(\mathcal{P})}$- structure $\alpha_\infty^{(\mathcal{P})} \otimes \mathbb{Z}_{(\mathcal{P})}$ on $E \otimes \mathbb{Z}_{(\mathcal{P})}$ naturally.

Proposition (1.3.4) (cf. [D2, Corollaire 3.5]) *Let $\mathcal{F}$ be the functor* (Schemes/$\mathbb{Z}_{(\mathcal{P})}$) $\to$ (Sets) *assigning to each $\mathbb{Z}_{(\mathcal{P})}$-scheme S the S-isomorphism classes of the pairs $(F, \beta_\infty^{(\mathcal{P})})$ consisting of $F \in \mathrm{Ob}(\mathcal{C}'_S)$ and a $\Gamma^{(\mathcal{P})}(\infty) \otimes \mathbb{Z}_{(\mathcal{P})}$-structure $\beta_\infty^{(\mathcal{P})}$ on it. Then the association: $(E, \alpha_\infty^{(\mathcal{P})}) \mapsto (E \otimes \mathbb{Z}_{(\mathcal{P})}, \alpha_\infty^{(\mathcal{P})} \otimes \mathbb{Z}_{(\mathcal{P})})$ gives an isomorphism $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}} \xrightarrow{\sim} \mathcal{F}$ of functors.*

Proof Deligne proved this fact when $\mathcal{P}$ is empty; but his proof applies to general $\mathcal{P}$ as well. (We recall below the argument showing the essential surjectivity.) □

We will identify the above two functors, which enables us to let $GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$ act on $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}}$ as $\mathbb{Z}_{(\mathcal{P})}$-automorphisms by the rule $(F, \beta_\infty^{(\mathcal{P})}) \mapsto (F, \beta_\infty^{(\mathcal{P})} \circ g)$.

Let us now describe what the effect of the action of $g \in GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$ on the original pair $(E, \alpha_\infty^{(\mathcal{P})})$ is: First assume that $g^{-1} \in GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}) \cap M_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})$. Then there is a positive integer N prime to $\mathcal{P}$ such that $(1/N) \cdot \widehat{\mathbb{Z}}^{(\mathcal{P})\oplus 2} \supseteq g \cdot \widehat{\mathbb{Z}}^{(\mathcal{P})\oplus 2} \supseteq \widehat{\mathbb{Z}}^{(\mathcal{P})\oplus 2}$. In this case, we obtain a finite étale subgroup scheme K_g of prime-to-$\mathcal{P}$ order of E/S, as the image of:

$$(1.3.5) \qquad g\cdot\underline{\widehat{\mathbb{Z}}}^{(\mathcal{P})\oplus 2}/\underline{\widehat{\mathbb{Z}}}^{(\mathcal{P})\oplus 2} \hookrightarrow (1/N)\cdot\underline{\widehat{\mathbb{Z}}}^{(\mathcal{P})\oplus 2}/\underline{\widehat{\mathbb{Z}}}^{(\mathcal{P})\oplus 2} \overset{\alpha_\infty^{(\mathcal{P})}}{\underset{\sim}{\to}} (1/N)\widehat{T}^{(\mathcal{P})}(E)/\widehat{T}^{(\mathcal{P})}(E) \cong E[N]$$

which does not depend on the choice of N. Set $E' := E/K_g$, and let $\pi : E \to E'$ be the quotient homomorphism. Then it is easy to see that the composite of:

$$\underline{\mathbb{A}}_{\mathrm{f}}^{(\mathcal{P})\oplus 2} \xrightarrow{g} \underline{\mathbb{A}}_{\mathrm{f}}^{(\mathcal{P})\oplus 2} \xrightarrow{\alpha_\infty^{(\mathcal{P})} \otimes \mathbb{Z}_{(\mathcal{P})}} \widehat{V}^{(\mathcal{P})}(E) \xrightarrow{\widehat{V}^{(\mathcal{P})}(\pi)} \widehat{V}^{(\mathcal{P})}(E')$$

in fact arises from an isomorphism $\alpha_\infty^{(\mathcal{P})\prime} : \underline{\widehat{\mathbb{Z}}}^{(\mathcal{P})\oplus 2} \xrightarrow{\sim} \widehat{T}^{(\mathcal{P})}(E')$. Thus using these symbols, we have:

$$(1.3.6) \qquad (E \otimes \mathbb{Z}_{(\mathcal{P})}, (\alpha_\infty^{(\mathcal{P})} \otimes \mathbb{Z}_{(\mathcal{P})}) \circ g) \cong (E', \alpha_\infty^{(\mathcal{P})\prime}) \otimes \mathbb{Z}_{(\mathcal{P})}.$$

As a special case of this, if N is a positive integer prime to $\mathcal{P}$, we see that multiplication by N on E induces an isomorphism

$$(1.3.7) \qquad (E \otimes \mathbb{Z}_{(\mathcal{P})}, (\alpha_\infty^{(\mathcal{P})} \otimes \mathbb{Z}_{(\mathcal{P})}) \circ \left(\begin{smallmatrix} 1/N & 0 \\ 0 & 1/N \end{smallmatrix}\right)) \xrightarrow{\sim} (E, \alpha_\infty^{(\mathcal{P})}) \otimes \mathbb{Z}_{(\mathcal{P})}.$$

If we set

(1.3.8)

$$\begin{cases} \mathbb{Q}_+^{(\mathcal{P})\times} := (\text{the subgroup of } \mathbb{Q}^\times \text{ generated by all prime numbers prime to } \mathcal{P}), \\ \mathbb{Q}^{(\mathcal{P})\times} := \{\pm 1\} \cdot \mathbb{Q}_+^{(\mathcal{P})\times}, \end{cases}$$

this relation means that the action of scalar matrices $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$ with $a \in \mathbb{Q}^{(\mathcal{P})\times}$ (embedded diagonally in $\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})\times}$) is trivial. Especially, the description of the action of general $g \in GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$ reduces to the first case.

We next consider the effect of the action of $GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$ on the set of irreducible components of $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]}$. For this, decompose $\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})\times}$ as a direct product:

$$\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})\times} = \widehat{\mathbb{Z}}^{(\mathcal{P})\times} \times \mathbb{Q}_+^{(\mathcal{P})\times}. \tag{1.3.9}$$

An element $c \in \mathbb{A}_{\mathrm{f}}^{(\mathcal{P})\times}$ is then expressed as $c = (c_0, c_1)$ with $c_0 \in \widehat{\mathbb{Z}}^{(\mathcal{P})\times}$ and $c_1 \in \mathbb{Q}_+^{(\mathcal{P})\times}$.

Proposition (1.3.10) *Let g be an element of $GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$. Let $(E', \alpha_\infty^{(\mathcal{P})\prime})$ be obtained from $(E, \alpha_\infty^{(\mathcal{P})})$ by* (1.3.6)*. Then we have*

$$\det(\alpha_\infty^{(\mathcal{P})\prime}) = \det(\alpha_\infty^{(\mathcal{P})})^{\det(g)_0}.$$

Especially, the action of g preserves each irreducible component of $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]}$ if and only if $\det(g) \in \mathbb{Q}_+^{(\mathcal{P})\times}$.

Proof We may assume that $g^{-1} \in M_2(\widehat{\mathbb{Z}}_{(\mathcal{P})})$. Using the above symbols, we see that the degree of the isogeny π is equal to:

$$\mid g\widehat{\mathbb{Z}}^{(\mathcal{P})\oplus 2} : \widehat{\mathbb{Z}}^{(\mathcal{P})\oplus 2} \mid = \det(g^{-1})_1.$$

On the other hand, it is easy to see that

$$\det(\alpha_\infty^{(\mathcal{P})})^{\deg(\pi)} = \det(\alpha_\infty^{(\mathcal{P})\prime})^{\det(g^{-1})}$$

from which the first assertion follows; and the rest is clear. □

We set:

$$\mathcal{G}^{(\mathcal{P})} := \{g \in GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}) \mid \det(g) \in \mathbb{Q}_+^{(\mathcal{P})\times}\}. \tag{1.3.11}$$

Fix an irreducible component $Y^{(\mathcal{P})}(\infty)^{(\zeta_\infty)}_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]}$ of $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]}$. We have obtained two homomorphisms

$$\begin{cases} GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}) \to \mathrm{Aut}(Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(\mathcal{P})}}/\mathbb{Z}_{(\mathcal{P})}), \\ \mathcal{G}^{(\mathcal{P})} \to \mathrm{Aut}(Y^{(\mathcal{P})}(\infty)^{(\zeta_\infty)}_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]}/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]). \end{cases} \tag{1.3.12}$$

Proposition (1.3.13) *The kernels of these two homomorphisms are both equal to:*

$$\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q}^{(\mathcal{P})\times}\}.$$

Proof It is enough to show the assertion for the second homomorphism. We need to show that an element $g \in \mathcal{G}^{(\mathcal{P})}$ lying in the kernel belongs to the above group of scalar matrices. We may assume that $g^{-1} \in M_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})$ to do this.

Let η be the generic point of $Y^{(\mathcal{P})}(\infty)^{(\zeta_\infty)}_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]}$, and $\kappa(\eta)$ the residue field at η. Let $(\mathcal{E}, \alpha^{(\mathcal{P})}_{\infty,\mathrm{univ}})$ be the universal pair on $Y^{(\mathcal{P})}(\infty)^{(\zeta_\infty)}_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]}$. We are going to apply the argument above describing the action of g to its generic fibre $(\mathcal{E}_\eta, (\alpha^{(\mathcal{P})}_{\infty,\mathrm{univ}})_\eta)$. Then we obtain a finite subgroup scheme K_g of $\mathcal{E}_\eta$ as in (1.3.5), and a prime-to-$\mathcal{P}$ isogeny $\mathcal{E}_\eta \to \mathcal{E}_\eta/K_g \cong \mathcal{E}_\eta$ over $\kappa(\eta)$. However, the endomorphism ring of $\mathcal{E}_\eta/\kappa(\eta)$ is isomorphic to $\mathbb{Z}$, so that $K_g = \mathcal{E}_\eta[N]$ with an integer N prime to $\mathcal{P}$; and hence $g = N^{-1}g_0$ with $g_0 \in GL_2(\widehat{\mathbb{Z}}_{(\mathcal{P})}) \cap \mathcal{G}^{(\mathcal{P})}$. But the image of g_0 in $\mathrm{Aut}(Y^{(\mathcal{P})}(\infty)^{(\zeta_\infty)}_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]}/Y(1)_{/\mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]})$ is trivial, and so $g_0 = \pm 1$. $\square$

1.4. Modular curves over $\mathbb{Z}_{(p)}$ and its strict localization. In the rest of this paper, we will mainly consider modular curves in characteristic p; and some objects obtained by "reduction modulo $\mathfrak{P}$" from characteristic zero. We fix here our notation for later use, including some repetitions.

We thus fix a prime number p, and consider curves over $\mathbb{Z}_{(p)}$-algebras. We henceforth assume that $\mathcal{P} \ni p$, and consider

$$Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(p)}} := \varprojlim_{N:\text{prime to } \mathcal{P}} Y(N)_{/\mathbb{Z}_{(p)}}. \tag{1.4.1}$$

The curve $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(p)}}$ is irreducible and it is a Galois covering of $Y(1)_{/\mathbb{Z}_{(p)}}$ with Galois group $GL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})/\{\pm 1\}$. It is an étale Galois covering of $Y(N)_{/\mathbb{Z}_{(p)}}$ if N is prime $\mathcal{P}$ and $N \geq 3$.

The case where $\mathcal{P} = \{p\}$ is the "largest" tower, and there is a natural morphism: $Y^{(p)}(\infty)_{/\mathbb{Z}_{(p)}} \to Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(p)}}$ over $\mathbb{Z}_{(p)}$ for general $\mathcal{P}$. The action of $GL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})$ on $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(p)}}$ is of course compatible with the action of $GL_2(\widehat{\mathbb{Z}}^{(p)})$ on $Y^{(p)}(\infty)_{/\mathbb{Z}_{(p)}}$ through this morphism and the projection $GL_2(\widehat{\mathbb{Z}}^{(p)}) \twoheadrightarrow GL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})$.

The action of $GL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})$ on $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(p)}}$ can be naturally extended to the action of the bigger group $GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$. Its subgroup acting trivially on $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(p)}}$ is the subgroup of diagonal matrices with entries in $\mathbb{Q}^{(\mathcal{P})\times}$. (We note however that the morphism $Y^{(p)}(\infty)_{/\mathbb{Z}_{(p)}} \to Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(p)}}$ considered above is not compatible with the action of adelic groups via the projection $GL_2(\mathbb{A}_{\mathrm{f}}^{(p)}) \twoheadrightarrow GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$. For example, if $q \in \mathcal{P} - \{p\}$, the action of $\begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix} \in GL_2(\mathbb{A}_{\mathrm{f}}^{(p)})$ on $Y^{(p)}(\infty)_{/\mathbb{Z}_{(p)}}$ is trivial, but $\begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix} \in GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$ acts non-trivially on $Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(p)}}$. If we consider $GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$ as a subgroup of $GL_2(\mathbb{A}_{\mathrm{f}}^{(p)})$ whose components at all $q \in \mathcal{P} - \{p\}$ are trivial, $Y^{(p)}(\infty)_{/\mathbb{Z}_{(p)}} \to Y^{(\mathcal{P})}(\infty)_{/\mathbb{Z}_{(p)}}$ is $GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})})$-equivariant.)

From now on, we fix embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and $\overline{\mathbb{Q}}_p$ once and for all. We denote by $\mathfrak{P}$ the prime of $\overline{\mathbb{Q}}$ induced by this embedding, and set

$$\begin{cases} \mathcal{K} := \text{ (the fixed field of the inertia group at } \mathfrak{P}) \subseteq \overline{\mathbb{Q}}, \\ \mathcal{W} := \text{(the ring of } \mathfrak{P}\text{-integers in } \mathcal{K}), \\ \mathbb{F} := \text{(the residue field of } \mathcal{W}). \end{cases} \tag{1.4.2}$$

Thus $\mathcal{W}$ is a strict Henselization of $\mathbb{Z}_{(p)}$, and $\mathbb{F}$ is an algebraic closure of the prime field $\mathbb{Z}/p\mathbb{Z}$. We consider the base extensions of the curves in (1.4.1) from $\mathbb{Z}_{(p)}$ to $\mathcal{W}$:

$$Y^{(\mathcal{P})}(\infty)_{/\mathcal{W}} := \varprojlim_{N:\text{prime to } \mathcal{P}} Y(N)_{/\mathcal{W}} \tag{1.4.3}$$

and similarly for the further base extensions to $\mathbb{C}$ and $\mathbb{F}$ etc. We have the group actions as above having the same properties on such curves. But these curves are not irreducible: According to our convention, we have $\mathcal{W}^\times \supseteq \mu_\infty^{(\mathcal{P})}$, $\boldsymbol{\mu}_\infty^{(\mathcal{P})\mathrm{prim}}(\overline{\mathbb{Q}})$, and $\mathcal{W} \supseteq \mathbb{Z}_{(\mathcal{P})}[\mu_\infty^{(\mathcal{P})}]$ (cf. 1.2 for notation). Irreducible components of $Y^{(\mathcal{P})}(\infty)_{/\mathcal{W}}$ correspond bijectively with $\boldsymbol{\mu}_\infty^{(\mathcal{P})\mathrm{prim}}(\overline{\mathbb{Q}})$ and are given by

$$Y^{(\mathcal{P})}(\infty)^{(\zeta_\infty)}_{/\mathcal{W}} := \varprojlim_{N:\text{prime to } \mathcal{P}} Y(N)^{(\zeta_N)}_{/\mathcal{W}} \tag{1.4.4}$$

for each $\zeta_\infty = (\zeta_N)_N \in \boldsymbol{\mu}_\infty^{(\mathcal{P})\mathrm{prim}}(\overline{\mathbb{Q}})$ with $Y(N)^{(\zeta_N)}_{/\mathcal{W}} = Y(N)^{(\zeta_N)} \otimes_{\mathbb{Z}[1/N,\mu_N]} \mathcal{W}$.

The group $SL_2(\widehat{\mathbb{Z}}^{(\mathcal{P})})/\{\pm 1\}$ acts on each irreducible component faithfully as its Galois group over $Y(1)_{/\mathcal{W}}$. The group defined by (1.3.11):

$$\mathcal{G}^{(\mathcal{P})} = \{g \in GL_2(\mathbb{A}_{\mathrm{f}}^{(\mathcal{P})}) \mid \det(g) \in \mathbb{Q}_+^{(\mathcal{P})\times}\}$$

also acts on each irreducible component as $\mathcal{W}$-automorphisms, and the subgroup acting trivially is the subgroup of diagonal matrices with entries in $\mathbb{Q}^{(\mathcal{P})\times}$.

These results stated so far for curves over $\mathcal{W}$ equally holds over $\mathbb{C}$ or over $\mathbb{F}$. (The proof of (1.3.13) also works for the base changed curves.)

§2. CM points on modular curves.

2.1. Preliminaries on imaginary quadratic fields. We hereafter fix an imaginary quadratic field K, and denote by $\mathfrak{o}$ its ring of integers. We also fix a prime number ℓ and let $\mathfrak{o}_n$ be the order of conductor ℓ^n of K,

$$\mathfrak{o}_n := \mathbb{Z} + \ell^n \mathfrak{o} \text{ for } n \geq 0. \tag{2.1.1}$$

If $\mathfrak{a}$ is a lattice in K, we set

$$\begin{cases} \mathfrak{a}_q := \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_q \text{ for each prime number } q, \\ \widehat{\mathfrak{a}} := \mathfrak{a} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} = \prod_{q:\text{prime}} \mathfrak{a}_q. \end{cases} \tag{2.1.2}$$

We also set

$$K_{\mathbb{A},\mathrm{f}} := K \otimes_{\mathbb{Q}} \mathbb{A}_{\mathrm{f}} = (\text{the ring of finite adeles of } K), \tag{2.1.3}$$

so that $K_{\mathbb{A},\mathrm{f}}$ is the restricted direct product of $K_q := K \otimes_{\mathbb{Q}} \mathbb{Q}_q$ with respect to $\mathfrak{o}_q$ for rational primes q.

For a lattice $\mathfrak{a}$ and $x = (x_q) \in K_{\mathbb{A},\mathrm{f}}^{\times}$, we set

$$x\mathfrak{a} := (\text{the unique lattice such that } (x\mathfrak{a})_q = x_q\mathfrak{a}_q \text{ for all } q) = x\widehat{\mathfrak{a}} \cap K. \tag{2.1.4}$$

When $\mathfrak{a}$ is a proper $\mathfrak{o}_n$-ideal, i.e. a locally free $\mathfrak{o}_n$-submodule of K of rank one, $x\mathfrak{a}$ is also a proper $\mathfrak{o}_n$-ideal, and conversely, every proper $\mathfrak{o}_n$-ideal is of the form $x\mathfrak{o}_n$ for some $x \in K_{\mathbb{A},\mathrm{f}}^{\times}$. Let

$$\mathrm{Cl}_n := (\text{the group of proper } \mathfrak{o}_n\text{-ideal classes}), \tag{2.1.5}$$

so that

$$K_{\mathbb{A},\mathrm{f}}^{\times}/K^{\times}\widehat{\mathfrak{o}}_n^{\times} \cong \mathrm{Cl}_n \text{ by } x \mapsto \mathrm{cl}(x\mathfrak{o}_n), \text{ the class of } x\mathfrak{o}_n. \tag{2.1.6}$$

When $m \geq n \geq 0$, there is a natural homomorphism $\mathrm{Cl}_m \to \mathrm{Cl}_n$ defined by: $\mathrm{cl}(\mathfrak{a}) \mapsto \mathrm{cl}(\mathfrak{a}\mathfrak{o}_n)$, or equivalently by $\mathrm{cl}(x\mathfrak{o}_m) \mapsto \mathrm{cl}(x\mathfrak{o}_n)$ $(x \in K_{\mathbb{A},\mathrm{f}}^{\times})$. We then obtain a profinite abelian group

$$\mathrm{Cl}_\infty := \varprojlim_{n \geq 0} \mathrm{Cl}_n. \tag{2.1.7}$$

Proposition (2.1.8) *Consider the homomorphism*

$$K_{\mathbb{A},\mathrm{f}}^{\times} \to \mathrm{Cl}_\infty \text{ defined by } x \mapsto (\mathrm{cl}(x\mathfrak{o}_n))_{n \geq 0}.$$

Then the kernel of this homomorphism is $K^{\times}\widehat{\mathfrak{o}}_\infty^{\times}$ where

$$\widehat{\mathfrak{o}}_\infty^{\times} := \prod_{q \neq \ell} \mathfrak{o}_q^{\times} \times \mathbb{Z}_\ell^{\times},$$

and we obtain an isomorphism:

$$K_{\mathbb{A},\mathrm{f}}^{\times}/K^{\times}\widehat{\mathfrak{o}}_\infty^{\times} \xrightarrow{\sim} \mathrm{Cl}_\infty.$$

Proof Since $\cap_{n \geq 0} (\mathbb{Z}_\ell + \ell^n \mathfrak{o}_\ell) = (\text{the closure of } \mathbb{Z}_\ell \text{ in } \mathfrak{o}_\ell) = \mathbb{Z}_\ell$, we have

$$\cap_{n \geq 0} \widehat{\mathfrak{o}}_n = \prod_{q \neq \ell} \mathfrak{o}_q \times \mathbb{Z}_\ell = \widehat{\mathfrak{o}}_\infty \text{ and } \cap_{n \geq 0} \widehat{\mathfrak{o}}_n^{\times} = \widehat{\mathfrak{o}}_\infty^{\times}.$$

The kernel in question is $\cap_{n \geq 0} K^{\times}\widehat{\mathfrak{o}}_n$, which clearly contains $K^{\times}\widehat{\mathfrak{o}}_\infty^{\times}$. Suppose conversely that $x \in K_{\mathbb{A},\mathrm{f}}^{\times}$ lies in the kernel, so that $x = \varepsilon_n \alpha_n$ with $\varepsilon_n \in K^{\times}$ and $\alpha_n \in \widehat{\mathfrak{o}}_n^{\times}$ for all $n \geq 0$. If $m \geq n \geq 1$, then since $K^{\times} \cap \widehat{\mathfrak{o}}_m^{\times} = K^{\times} \cap \widehat{\mathfrak{o}}_n^{\times} = \{\pm 1\}$, we have $\varepsilon_n^{-1}\varepsilon_m \in \{\pm 1\}$, and hence $\varepsilon_n^{-1}x = (\varepsilon_n^{-1}\varepsilon_m)\alpha_m \in \widehat{\mathfrak{o}}_m^{\times}$. This shows that $\varepsilon_n^{-1}x \in \cap_{m \geq n} \widehat{\mathfrak{o}}_m^{\times} = \widehat{\mathfrak{o}}_\infty^{\times}$, and hence $x \in K^{\times}\widehat{\mathfrak{o}}_\infty^{\times}$.

It remains to show the surjectivity of $K_{\mathbb{A},\mathrm{f}}^{\times}/K^{\times}\widehat{\mathfrak{o}}_\infty^{\times} \hookrightarrow \mathrm{Cl}_\infty$. It follows from (2.1.6) that the image is dense in Cl_∞, while it also follows from (2.1.6) and the finiteness of Cl_n that the group $K_{\mathbb{A},\mathrm{f}}^{\times}/K^{\times}\widehat{\mathfrak{o}}_\infty^{\times}$ is compact, which implies the surjectivity. □

We hereafter denote by

$$i_\ell : K^\times \hookrightarrow K_\ell^\times (\hookrightarrow K_{\mathbb{A},\mathrm{f}}^\times)$$

the natural embedding (to distinguish $i_\ell(K^\times)$ from the diagonal image $K^\times \subset K_{\mathbb{A},\mathrm{f}}^\times$).

Corollary (2.1.9) *The natural homomorphism sending $x \in \mathfrak{o}_{n,\ell}^\times \subseteq K_{\mathbb{A},\mathrm{f}}^\times$ to $(\mathrm{cl}(x\mathfrak{o}_m))_{m\geq 0}$ gives an isomorphism: $\mathfrak{o}_{n,\ell}^\times/\mathbb{Z}_\ell^\times \xrightarrow{\sim} \mathrm{Ker}(\mathrm{Cl}_\infty \to \mathrm{Cl}_n)$ when $n \geq 1$, while $\mathfrak{o}_\ell^\times/i_\ell(\mathfrak{o}^\times)\mathbb{Z}_\ell^\times \xrightarrow{\sim} \mathrm{Ker}(\mathrm{Cl}_\infty \to \mathrm{Cl}_0)$.*

Similarly if $m \geq n$, we have an isomorphism $\mathfrak{o}_{n,\ell}^\times/\mathfrak{o}_{m,\ell}^\times \xrightarrow{\sim} \mathrm{Ker}(\mathrm{Cl}_m \to \mathrm{Cl}_n)$ when $n \geq 1$, and $\mathfrak{o}_\ell^\times/i_\ell(\mathfrak{o}^\times)\mathfrak{o}_{m,\ell}^\times \xrightarrow{\sim} \mathrm{Ker}(\mathrm{Cl}_m \to \mathrm{Cl}_0)$.

Proof We only give a proof for the first assertion. By (2.1.6) and (2.1.8), we see that $\mathrm{Ker}(\mathrm{Cl}_\infty \to \mathrm{Cl}_n)$ is canonically isomorphic to

$$\frac{K^\times \widehat{\mathfrak{o}}_n^\times}{K^\times \widehat{\mathfrak{o}}_\infty^\times} \cong \frac{\widehat{\mathfrak{o}}_n^\times}{(K^\times \widehat{\mathfrak{o}}_\infty^\times) \cap \widehat{\mathfrak{o}}_n^\times} \twoheadleftarrow \mathfrak{o}_{n,\ell}^\times.$$

Our claim follows from this, noting that $K^\times \cap \widehat{\mathfrak{o}}_n^\times = \{\pm 1\}$ when $n \geq 1$. □

2.2. Subgroup $\mathrm{Cl}^{\mathrm{alg}}$ of Cl_∞. Hida introduced the subgroup $\mathrm{Cl}^{\mathrm{alg}}$ of Cl_∞ which plays a crucial role in the study of Zariski density of CM points; [H1, 2.3], [H3, 8.2.2]. We first recall its definition:

Definition (2.2.1) Let

$$K_{\mathbb{A},\mathrm{f}}^{(\ell)\times} := (\text{elements of } K_{\mathbb{A},\mathrm{f}}^\times \text{ whose } \ell\text{-component is one}) \subseteq K_{\mathbb{A},\mathrm{f}}^\times.$$

We denote by $\mathrm{Cl}^{\mathrm{alg}}$ the image of $K_{\mathbb{A},\mathrm{f}}^{(\ell)\times}$ under the homomorphism defined in (2.1.8):

$$\mathrm{Cl}^{\mathrm{alg}} := \{(\mathrm{cl}(x\mathfrak{o}_n))_{n\geq 0} \in \mathrm{Cl}_\infty \mid x \in K_{\mathbb{A},\mathrm{f}}^{(\ell)\times}\}.$$

Set $\mathfrak{o}_{(\ell)} := \mathfrak{o} \otimes_{\mathbb{Z}} \mathbb{Z}_{(\ell)}$ in the following.

Proposition (2.2.2) *The homomorphism: $K_{\mathbb{A},\mathrm{f}}^\times \supseteq \mathfrak{o}_\ell^\times \ni x \mapsto (\mathrm{cl}(x\mathfrak{o}_n))_{n\geq 0} \in \mathrm{Cl}_\infty$ induces an isomorphism:*

$$\frac{\mathfrak{o}_\ell^\times}{i_\ell(\mathfrak{o}_{(\ell)}^\times)\mathbb{Z}_\ell^\times} \xrightarrow{\sim} \frac{\mathrm{Cl}_\infty}{\mathrm{Cl}^{\mathrm{alg}}}.$$

Proof Consider the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K_{\mathbb{A},\mathrm{f}}^{(\ell)\times} \cap (K^\times \widehat{\mathfrak{o}}_\infty^\times) & \longrightarrow & K_{\mathbb{A},\mathrm{f}}^{(\ell)\times} & \longrightarrow & \mathrm{Cl}^{\mathrm{alg}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K^\times \widehat{\mathfrak{o}}_\infty^\times & \longrightarrow & K_{\mathbb{A},\mathrm{f}}^\times & \longrightarrow & \mathrm{Cl}_\infty & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{pr}_\ell} & & \downarrow{\scriptstyle \mathrm{pr}_\ell} & & \downarrow & & \\
 & & i_\ell(K^\times)\mathbb{Z}_\ell^\times & \longrightarrow & K_\ell^\times & \longrightarrow & \mathrm{Cl}_\infty/\mathrm{Cl}^{\mathrm{alg}} & \longrightarrow & 0
\end{array}$$

where pr_ℓ is the projection to the ℓ-factor. We obtain from this an isomorphism:

$$\frac{K_\ell^\times}{i_\ell(K^\times)\mathbb{Z}_\ell^\times} \xrightarrow{\sim} \frac{\mathrm{Cl}_\infty}{\mathrm{Cl}^{\mathrm{alg}}}.$$

Since $K_\ell^\times = i_\ell(K^\times)\mathfrak{o}_\ell^\times$, we see that the group in the left hand side is isomorphic to $\mathfrak{o}_\ell^\times / i_\ell(\mathfrak{o}_{(\ell)}^\times)\mathbb{Z}_\ell^\times$. □

Proposition (2.2.3) *Let a be an element of $\mathfrak{o}_\ell^\times$. The following conditions are equivalent:*

(1) $\cap_{n\geq 0} a\mathfrak{o}_n \neq \{0\}$;

(2) $a \in i_\ell(\mathfrak{o}_{(\ell)}^\times)\mathbb{Z}_\ell^\times$;

(3) *the element* $(\mathrm{cl}(a\mathfrak{o}_n))_{n\geq 0} \in \mathrm{Cl}_\infty$ *belongs to* $\mathrm{Cl}^{\mathrm{alg}}$.

Proof The equivalence of (2) and (3) is clear from (2.2.2).

On the other hand, we have:

$$\cap_{n\geq 0} a\mathfrak{o}_n = \cap_{n\geq 0}(a\widehat{\mathfrak{o}}_n \cap K) = a(\cap_{n\geq 0}\widehat{\mathfrak{o}}_n) \cap K.$$

By the first remark in the proof of (2.1.8), this is equal to

$$a\widehat{\mathfrak{o}}_\infty \cap K = (\prod_{q\neq\ell} \mathfrak{o}_q \times a\cdot\mathbb{Z}_\ell) \cap K = (\prod_{q\neq\ell} \mathfrak{o}_q \times a\cdot\mathbb{Z}_\ell) \cap \mathfrak{o}.$$

One then checks easily that this set contains a non-zero element if and only if $a \in i_\ell(\mathfrak{o}_{(\ell)}^\times)\mathbb{Z}_\ell^\times$. □

We next interpret this result in terms of complex elliptic curves. If $\mathbb{C}/L$ and $\mathbb{C}/L'$ are one-dimensional complex tori, recall that an analytic homomorphism between them is induced by multiplication by a complex number on $\mathbb{C}$:

$$\mathrm{Hom}(\mathbb{C}/L, \mathbb{C}/L') = \{\mu \in \mathbb{C} \mid \mu L \subseteq L'\}. \tag{2.2.4}$$

Lemma (2.2.5) *Fix $x \in K_{\mathbb{A},\mathrm{f}}^\times$ and $a \in \mathfrak{o}_\ell^\times$, and consider the complex elliptic curves $\mathbb{C}/x\mathfrak{o}_n$ and $\mathbb{C}/ax\mathfrak{o}_n$ for $n \geq 0$.*

(1) $\mathrm{Hom}(\mathbb{C}/x\mathfrak{o}_n, \mathbb{C}/ax\mathfrak{o}_n) = a\mathfrak{o}_n$ *for all n.*

(2) *When $\mu \in a\mathfrak{o}_n$, the degree of the corresponding homomorphism of $\mathbb{C}/x\mathfrak{o}_n$ to $\mathbb{C}/ax\mathfrak{o}_n$ is $N_{K/\mathbb{Q}}(\mu)$, the norm of μ.*

Proof (1) By (2.2.4), a homomorphism $\mathbb{C}/x\mathfrak{o}_n \to \mathbb{C}/ax\mathfrak{o}_n$ is given by multiplication by $\mu \in K$ satisfying $\mu x\mathfrak{o}_n \subseteq ax\mathfrak{o}_n$. This latter condition is satisfied if and only if $(\mu x\mathfrak{o}_n)_q \subseteq (ax\mathfrak{o}_n)_q$, equivalently $(\mu\mathfrak{o}_n)_q \subseteq (a\mathfrak{o}_n)_q$ for all rational primes q; i.e. $\mu\mathfrak{o}_n \subseteq a\mathfrak{o}_n$.

(2) Let μ be a non-zero element of $a\mathfrak{o}_n$.The degree in question is equal to:

$$\left|\frac{ax\mathfrak{o}_n}{\mu x\mathfrak{o}_n}\right| = \prod_q \left|\frac{(ax\mathfrak{o}_n)_q}{(\mu x\mathfrak{o}_n)_q}\right| = \prod_{q\neq\ell} \left|\frac{\mathfrak{o}_q}{\mu\mathfrak{o}_q}\right| \times \left|\frac{a\mathfrak{o}_{n,\ell}}{\mu\mathfrak{o}_{n,\ell}}\right|,$$

and hence it is enough to show that $|a\mathfrak{o}_{n,\ell}/\mu\mathfrak{o}_{n,\ell}| = |\mathfrak{o}_\ell/\mu\mathfrak{o}_\ell|$. Consider the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{o}_{n,\ell} & \longrightarrow & \mathfrak{o}_\ell & \longrightarrow & \mathfrak{o}_\ell/\mathfrak{o}_{n,\ell} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a^{-1}\mu} & & \downarrow{\scriptstyle a^{-1}\mu} & & \downarrow{\scriptstyle a^{-1}\mu} & & \\ 0 & \longrightarrow & \mathfrak{o}_{n,\ell} & \longrightarrow & \mathfrak{o}_\ell & \longrightarrow & \mathfrak{o}_\ell/\mathfrak{o}_{n,\ell} & \longrightarrow & 0. \end{array}$$

Since $\mathfrak{o}_\ell/\mathfrak{o}_{n,\ell}$ is finite, the kernel and the cokernel of the right vertical homomorphism have the same order; and the middle vertical homomorphism is injective. The snake lemma then implies that $|\mathfrak{o}_{n,\ell}/a^{-1}\mu\mathfrak{o}_{n,\ell}| = |\mathfrak{o}_\ell/a^{-1}\mu\mathfrak{o}_\ell| = |\mathfrak{o}_\ell/\mu\mathfrak{o}_\ell|$. □

Proposition (2.2.6) *Let the notation be as in the previous lemma. The minimal value of the degrees of non-zero elements of* $\mathrm{Hom}(\mathbb{C}/x\mathfrak{o}_n, \mathbb{C}/ax\mathfrak{o}_n)$ *is independent of* $x \in K^\times_{\mathbb{A},\mathrm{f}}$. *Call this value* c_n. *If* $(\mathrm{cl}(a\mathfrak{o}_n))_{n\geq 0} \in \mathrm{Cl}_\infty$ *does not belong to* $\mathrm{Cl}^{\mathrm{alg}}$, *then we have* $c_n \to \infty$ *as* $n \to \infty$.

Proof The first assertion is clear from (2.2.5).

To prove the second part, take one n. Since there are only a finite number of elements of $a\mathfrak{o}_n$ whose norm is c_n, none of such elements are contained in $a\mathfrak{o}_m$ for m large, because $\cap_{m\geq 0} a\mathfrak{o}_m = \{0\}$ by (2.2.3). Again by (2.2.5), this means that $c_m > c_n$ for such m. □

Remark (2.2.7) Let the notation be as above, and assume to the contrary that $(\mathrm{cl}(a\mathfrak{o}_n))_{n\geq 0} \in \mathrm{Cl}^{\mathrm{alg}}$. Then it follows from (2.2.3) that the set of values c_n $(n \geq 0)$ is bounded. This means that the set of closed points of $Y(1)_{/\mathbb{C}} \times_{\mathbb{C}} Y(1)_{/\mathbb{C}}$ provided by the pairs $(\mathbb{C}/x\mathfrak{o}_n, \mathbb{C}/ax\mathfrak{o}_n)$ $(n \geq 0)$ is contained in a union of finite number of modular correspondences.

2.3. CM points on modular curves and our main result. We henceforth fix a prime number p $(p \neq \ell)$, which *splits* in K.

Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal. The complex torus $\mathbb{C}/\mathfrak{a}$ is isomorphic to the complex points of an elliptic curve defined over $\overline{\mathbb{Q}}$ whose field of moduli is the ring class field of K of conductor ℓ^n. Therefore the complex point $x(\mathfrak{a})_{/\mathbb{C}}$ it determines is in fact a $\mathcal{K}$-rational point $x(\mathfrak{a})_{/\mathcal{K}}$ of the coarse moduli scheme $Y(1)_{/\mathcal{K}}$. It further uniquely extends to a $\mathcal{W}$-valued point $x(\mathfrak{a})_{/\mathcal{W}}$ of $Y(1)_{/\mathcal{W}}$.

This in turn gives an $\mathbb{F}$-valued point $x(\mathfrak{a})_{/\mathbb{F}}$ of $Y(1)_{/\mathbb{F}}$; cf (1.4.2) for these symbols. These points actually depend only on the class $\mathrm{cl}(\mathfrak{a}) \in \mathrm{Cl}_n$. When there is no fear of confusion, we simply write $x(\mathfrak{a})$ for them.

Let us take and fix an infinite increasing sequence of integers:

$$\underline{n} = \{0 \leq n_0 < n_1 < \cdots\}. \tag{2.3.1}$$

For each n_j, we set

$$R_{n_j} := \mathrm{Ker}(\mathrm{Cl}_{n_j} \to \mathrm{Cl}_{n_0}). \tag{2.3.2}$$

We consider the set of $\mathcal{R}$-valued points of $Y(1)_{/\mathcal{R}}$ defined by:

$$\xi(1;\underline{n})_{/\mathcal{R}} := \{x(\mathfrak{a})_{/\mathcal{R}} \mid \mathrm{cl}(\mathfrak{a}) \in R_{n_j} \text{ for some } n_j \in \underline{n}\} \tag{2.3.3}$$

where $\mathcal{R}$ denotes one of $\mathbb{C}$, $\mathcal{K}$, $\mathcal{W}$ or $\mathbb{F}$.

Our main concern is such points in characteristic p, and we will consider $\xi(1;\underline{n})_{/\mathbb{F}}$ also as a set of closed points of $Y(1)_{/\mathbb{F}}$ below. To state the following theorem, we fix an irreducible component of $Y^{(p)}(\infty)_{/\mathbb{F}}$ which we call $Y^{(p)}(\infty)^0_{/\mathbb{F}} = \varprojlim_{p\nmid N} Y(N)^0_{/\mathbb{F}}$ (cf. (1.4.4)). For a positive integer m, we indicate by the superscript m the m-fold fibre product over the base scheme under consideration.

The following theorem had been announced by Hida, in a slightly different formulation; cf. [H3, Proposition 8.28], [H1, Proposition 2.8] in a much more general situation treating Hilbert modular varieties:

Theorem (2.3.4) *Let the notation be as above. Take and fix $\delta_1, \cdots, \delta_m \in \mathrm{Ker}(\mathrm{Cl}_\infty \to \mathrm{Cl}_{n_0})$ whose classes in $\mathrm{Cl}_\infty/\mathrm{Cl}^{\mathrm{alg}}$ are all distinct, and choose $\alpha_i \in K^\times_{\mathbb{A},\mathrm{f}}$ satisfying $\delta_i = (\mathrm{cl}(\alpha_i \mathfrak{o}_n))_{n\geq 0}$ (cf. (2.1.8)) for $1 \leq i \leq m$. We consider the following set of closed points of $(Y(1)_{/\mathbb{F}})^m$:*

$$\Xi(1;\underline{n})_{/\mathbb{F}} = \Xi(1)_{/\mathbb{F}} := \{(x(\alpha_1\mathfrak{a}), \cdots, x(\alpha_m\mathfrak{a})) \in (Y(1)_{/\mathbb{F}})^m \mid x(\mathfrak{a}) \in \xi(1;\underline{n})_{/\mathbb{F}}\}.$$

Let M be a positive integer prime to p (resp. $M = \infty$). Let $\Lambda(M)$ be a set of closed points of $(Y(M)^0_{/\mathbb{F}})^m$ (resp. $(Y^{(p)}(\infty)^0_{/\mathbb{F}})^m$) which maps surjectively onto $\Xi(1;\underline{n})_{/\mathbb{F}}$ via the natural morphism: $(Y(M)^0_{/\mathbb{F}})^m \to (Y(1)_{/\mathbb{F}})^m$ (resp. $(Y^{(p)}(\infty)^0_{/\mathbb{F}})^m \to (Y(1)_{/\mathbb{F}})^m$). Then $\Lambda(M)$ is a Zariski dense subset of $(Y(M)^0_{/\mathbb{F}})^m$ (resp. $(Y^{(p)}(\infty)^0_{/\mathbb{F}})^m$).

Note that the set $\Xi(1;\underline{n})_{/\mathbb{F}}$ of course depends on δ_i but not on the choice of α_i $(1 \leq i \leq m)$.

Remark (2.3.5) (1) The conclusion of the theorem above for one M and one choice of $\Lambda(M)$ implies the whole theorem: This follows from (A.1.4) in the appendix. One example is the case where $M = \infty$ and $\Lambda(\infty)$ is obtained by choosing exactly one point in the inverse image of each point of $\Xi(1;\underline{n})_{/\mathbb{F}}$. This is the case considered by Hida (under a suitable choice of points). Another

extreme case is $\Lambda(1) = \Xi(1;\underline{n})_{/\mathbb{F}}$: Theorem (2.3.4) is equivalent to the Zariski density of $\Xi(1;\underline{n})_{/\mathbb{F}}$ in $(Y(1)_{/\mathbb{F}})^m$.

(2) It follows from this that the validity of (2.3.4) is independent of the choice of an irreducible component $Y^{(p)}(\infty)^0_{/\mathbb{F}}$.

(3) The map which sends $\mathrm{cl}(\mathfrak{a})$ to $x(\mathfrak{a})_{/\mathbb{F}}$ induces an injection $\coprod_j R_{n_j} \to Y(1)_{/\mathbb{F}}$. This is well-known for similar maps defined over $\mathbb{C}$ or $\mathcal{K}$. The characteristic p result follows from this because (p splits in K, and hence) the elliptic curve $E(\mathfrak{a})_{/\mathcal{W}}$ giving $x(\mathfrak{a})_{/\mathcal{W}}$ (see 2.4. below) is the canonical lifting of $E(\mathfrak{a})_{/\mathbb{F}}$ giving $x(\mathfrak{a})_{/\mathbb{F}}$. Especially, the set $\xi(1;\underline{n})_{/\mathbb{F}}$ is infinite, and (2.3.4) obviously holds when $m = 1$.

In Section 4, we will describe a proof of (2.3.4), via an argument using certain ("admissible") CM points on a subcover of $Y^{(p)}(\infty)^0_{/\mathbb{F}}/Y(1)_{/\mathbb{F}}$.

2.4. Admissible CM points. If $\mathfrak{a}$ is a lattice in K, we have canonical isomorphisms for the complex torus $\mathbb{C}/\mathfrak{a}$:

$$\text{(2.4.1)} \qquad \begin{cases} \mathbb{C}/\mathfrak{a}[M] = \frac{1}{M}\mathfrak{a}/\mathfrak{a} \cong \mathfrak{a}/M\mathfrak{a} \text{ for positive integers } M, \\ \widehat{T}^{(\mathcal{P})}(\mathbb{C}/\mathfrak{a}) \cong \widehat{\mathfrak{a}}^{(\mathcal{P})} := \mathfrak{a} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{(\mathcal{P})}. \end{cases}$$

Here, we are using the notation as in (1.2.2) and (1.2.4) (and the remark after it). We will identify the groups in each isomorphism in the following. Thus providing $\mathbb{C}/\mathfrak{a}$ with a $\Gamma(M)$-structure (resp. a $\Gamma^{(\mathcal{P})}(\infty)$-structure) is just to give an isomorphism $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z} \xrightarrow{\sim} \mathfrak{a}/M\mathfrak{a}$ (resp. $\widehat{\mathbb{Z}}^{(\mathcal{P})} \times \widehat{\mathbb{Z}}^{(\mathcal{P})} \xrightarrow{\sim} \widehat{\mathfrak{a}}^{(\mathcal{P})}$).

In the following, we consider $\Gamma^{(\mathcal{P})}(\infty)$-structures with $\mathcal{P} = \{p, \ell\}$. We put

$$\text{(2.4.2)} \qquad \begin{cases} K^{(p,\ell)}_{\mathbb{A},\mathrm{f}} := K \otimes_{\mathbb{Q}} \mathbb{A}^{(p,\ell)}_{\mathrm{f}}, \\ \widehat{\mathfrak{o}}^{(p,\ell)}_n = \mathfrak{o}_n \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}^{(p,\ell)} = \widehat{\mathfrak{o}}^{(p,\ell)}. \end{cases}$$

Thus $K^{(p,\ell)\times}_{\mathbb{A},\mathrm{f}}$ is the restricted direct product of $K_q^\times$ with respect to $\mathfrak{o}_q^\times$ for $q \neq p, \ell$; and we will often identify it with the subgroup of $K^\times_{\mathbb{A},\mathrm{f}}$ consisting of elements whose p- and ℓ-components are one. We also take and fix a $\mathbb{Z}$-basis $\underline{w} = \{w_1, w_2\}$ of $\mathfrak{o}$ on which the following constructions depend.

For $\gamma \in K^\times_{\mathbb{A},\mathrm{f}}$, let us denote by

$$\gamma^{(p,\ell)} = \gamma'$$

its projection to $K^{(p,\ell)\times}_{\mathbb{A},\mathrm{f}}$. Now for any $n \geq 0$, $\underline{w}$ gives a $\widehat{\mathbb{Z}}^{(p,\ell)}$-basis of $\widehat{\mathfrak{o}}^{(p,\ell)}_n$. So we can define

$$\text{(2.4.3)}\ \alpha_{\infty,\mathbb{C}}(\mathfrak{o}_n;1) : \widehat{\mathbb{Z}}^{(p,\ell)} \times \widehat{\mathbb{Z}}^{(p,\ell)} \xrightarrow{\sim} \widehat{\mathfrak{o}}^{(p,\ell)}_n = \widehat{T}^{(p,\ell)}(\mathbb{C}/\mathfrak{o}_n) \text{ by } (s,t) \mapsto sw_1 + tw_2.$$

When $\mathfrak{a}$ is a proper $\mathfrak{o}_n$-ideal, take $\gamma \in K^\times_{\mathbb{A},\mathrm{f}}$ such that $\mathfrak{a} = \gamma\mathfrak{o}_n$. We define

$$\text{(2.4.4)} \qquad \alpha_{\infty,\mathbb{C}}(\mathfrak{a};\gamma') : \widehat{\mathbb{Z}}^{(p,\ell)} \times \widehat{\mathbb{Z}}^{(p,\ell)} \xrightarrow{\sim} \widehat{\mathfrak{a}}^{(p,\ell)} = \widehat{T}^{(p,\ell)}(\mathbb{C}/\mathfrak{a})$$

by composing $\alpha_{\infty,\mathbb{C}}(\mathfrak{o}_n;1)$ and $\widehat{T}^{(p,\ell)}(\mathbb{C}/\mathfrak{o}_n) = \widehat{\mathfrak{o}}^{(p,\ell)}_n \underset{\sim}{\xrightarrow{\gamma'}} \widehat{\mathfrak{a}}^{(p,\ell)} = \widehat{T}^{(p,\ell)}(\mathbb{C}/\mathfrak{a})$.

Definition (2.4.5) Let the notation be as above. We denote by $x(\mathfrak{a};\gamma')_{/\mathbb{C}}$ the $\mathbb{C}$-valued point of $Y^{(p,\ell)}(\infty)_{/\mathbb{C}}$ determined by (the isomorphism class of) the pair $(\mathbb{C}/\mathfrak{a}, \alpha_{\infty,\mathbb{C}}(\mathfrak{a};\gamma'))$.

We next return to the situation of 1.4. It is known that there is an elliptic curve $E(\mathfrak{a})_{/\mathcal{K}}$ defined over $\mathcal{K}$ such that $E(\mathfrak{a})_{/\mathcal{K}}(\mathbb{C}) \cong \mathbb{C}/\mathfrak{a}$, having good reduction, i.e. it extends (uniquely) to an elliptic curve $E(\mathfrak{a})_{/\mathcal{W}}$ over $\mathcal{W}$; cf. Serre and Tate [ST, Theorems 8 and 9]. Since $\mathcal{W}$ is strictly local, all points of $E(\mathfrak{a})_{/\mathcal{K}}[M]$ are $\mathcal{K}$-rational, and they extend to sections of $E(\mathfrak{a})_{/\mathcal{W}}$ over $\mathcal{W}$, for all positive integers M prime to p. Especially, the model $E(\mathfrak{a})_{/\mathcal{K}}$ of $\mathbb{C}/\mathfrak{a}$ over $\mathcal{K}$ having this good reduction property is unique up to isomorphisms. Further, *any* $\Gamma(N)$-structure ($p \nmid N$) or $\Gamma^{(p,\ell)}(\infty)$-structure on $\mathbb{C}/\mathfrak{a}$ are defined over $\mathcal{K}$ (resp. over $\mathcal{W}$) for this model $E(\mathfrak{a})_{/\mathcal{K}}$ (resp. $E(\mathfrak{a})_{/\mathcal{W}}$). We can therefore make the following

Definition (2.4.6) Let the notation be as above. The point $x(\mathfrak{a};\gamma')_{/\mathbb{C}}$ is in fact a $\mathcal{K}$-rational point of $Y^{(p,\ell)}(\infty)_{/\mathcal{K}}$ which we denote by $x(\mathfrak{a};\gamma')_{/\mathcal{K}}$. It uniquely extends to a $\mathcal{W}$-valued point $x(\mathfrak{a};\gamma')_{/\mathcal{W}}$ of $Y^{(p,\ell)}(\infty)_{/\mathcal{W}}$. This then defines an $\mathbb{F}$-rational point $x(\mathfrak{a};\gamma')_{/\mathbb{F}}$ of the closed fibre $Y^{(p,\ell)}(\infty)_{/\mathbb{F}}$.

Points obtained in this manner will be called *admissible CM points* on $Y^{(p,\ell)}(\infty)_{/\mathcal{R}}$. We set

$$\xi^{\mathrm{adm}}(\infty;\underline{n})_{/\mathcal{R}} := \{x(\mathfrak{a};\gamma')_{/\mathcal{R}} \mid \mathfrak{a} = \gamma\mathfrak{o}_{n_j}, \mathrm{cl}(\mathfrak{a}) \in R_{n_j} \text{ for some } n_j \in \underline{n},\}$$

for $\mathcal{R} = \mathbb{C}$, $\mathcal{K}$, $\mathcal{W}$ or $\mathbb{F}$.

In the following, we list basic properties of admisible CM points. First we have:

Lemma (2.4.7) *For any $a \in K^\times$, we have*

$$x(a\mathfrak{a};(a\gamma)')_{/\mathcal{R}} = x(\mathfrak{a};\gamma')_{/\mathcal{R}},$$

for $\mathcal{R} = \mathbb{C}$, $\mathcal{K}$, $\mathcal{W}$ or $\mathbb{F}$.

Proof From the construction of our CM points, it is enough to prove the assertion for the $\mathbb{C}$-valued points; i.e. that

$$(\mathbb{C}/a\mathfrak{a}, \alpha_{\infty,\mathbb{C}}(a\mathfrak{a};(a\gamma)')) \cong (\mathbb{C}/\mathfrak{a}, \alpha_{\infty,\mathbb{C}}(\mathfrak{a};\gamma')).$$

Multiplication by a on $\mathbb{C}$ induces an isomorphism $\mathbb{C}/\mathfrak{a} \xrightarrow{\sim} \mathbb{C}/a\mathfrak{a}$, and it is easy to see that this isomorphism indeed carries $\alpha_{\infty,\mathbb{C}}(\mathfrak{a};\gamma')$ to $\alpha_{\infty,\mathbb{C}}(a\mathfrak{a};(a\gamma)')$. □

Next we consider a representation of $K^\times$ into $GL_2(\mathbb{Q})$:

Definition (2.4.8) We denote by

$$\rho : K^\times \to GL_2(\mathbb{Q})$$

the regular representation with respect to the basis $\underline{w}$. Thus the following diagram commutes for all $b \in K^\times$:

$$\begin{array}{ccc} \mathbb{Q}^2 & \xrightarrow{\sim} & K \\ {\scriptstyle \rho(b)}\downarrow & & \downarrow{\scriptstyle \times b} \\ \mathbb{Q}^2 & \xrightarrow{\sim} & K \end{array}$$

where the two horizontal arrows are given by $(s,t) \mapsto sw_1 + tw_2$.

We may consider this ρ as a homomorphism of algebraic groups over $\mathbb{Q}$ ($K^\times(R) = (K \otimes_{\mathbb{Q}} R)^\times$ for $\mathbb{Q}$-algebras R), and we have:

$$\text{(2.4.9)} \qquad \begin{cases} \det \circ \rho = N_{K/\mathbb{Q}}, \\ \rho(\mathfrak{o} \cap K^\times) \subseteq GL_2(\mathbb{Q}) \cap M_2(\mathbb{Z}), \\ \rho(\mathfrak{o}_q \cap K_q^\times) \subseteq GL_2(\mathbb{Q}_q) \cap M_2(\mathbb{Z}_q) \text{ for all primes } q, \\ \rho(\widehat{\mathfrak{o}}^{(p,\ell)\times}) \subseteq GL_2(\widehat{\mathbb{Z}}^{(p,\ell)}), \\ \rho(K_{\mathbb{A},\mathrm{f}}^{(p,\ell)\times}) \subseteq GL_2(\mathbb{A}_{\mathrm{f}}^{(p,\ell)}), \text{ and so on.} \end{cases}$$

Proposition (2.4.10) *Let δ' be an element of $K_{\mathbb{A},\mathrm{f}}^{(p,\ell)\times}$. Then the action of $\rho(\delta') \in GL_2(\mathbb{A}_{\mathrm{f}}^{(p,\ell)})$ on $Y^{(p,\ell)}(\infty)_{/\mathcal{R}}$ studied in* 1.3 *sends $x(\mathfrak{a};\gamma')_{/\mathcal{R}}$ to $x(\delta'\mathfrak{a};\delta'\gamma')_{/\mathcal{R}}$. Especially, the set of admissible CM points on $Y^{(p,\ell)}(\infty)_{/\mathcal{R}}$ is stable under the action of $\rho(K_{\mathbb{A},\mathrm{f}}^{(p,\ell)\times})$. Here, as before, $\mathcal{R} = \mathbb{C}$, $\mathcal{K}$, $\mathcal{W}$ or $\mathbb{F}$.*

Proof Again, it is enough to prove the assertion when $\mathcal{R} = \mathbb{C}$.

Set $g := \rho(\delta')$. Replacing δ' by $(1/N)\delta'$ with a suitable positive integer N, we may assume that $\delta'^{-1} \in K_{\mathbb{A},\mathrm{f}}^{(p,\ell)\times} \cap \widehat{\mathfrak{o}}^{(p,\ell)}$ so that $g^{-1} \in GL_2(\mathbb{A}_{\mathrm{f}}^{(p,\ell)}) \cap M_2(\widehat{\mathbb{Z}}^{(p,\ell)})$. The image of $(\mathbb{C}/\mathfrak{a}, \alpha_{\infty,\mathbb{C}}(\mathfrak{a};\gamma'))$ under the action of g was explicitly described in 1.3: The group(scheme) K_g defined in (1.3.5) in the present case is the (genuine) finite subgroup $\delta'\mathfrak{a}/\mathfrak{a}$ of $\mathbb{C}/\mathfrak{a}$, in view of the definition (2.4.8). The target elliptic curve denoted by E' is thus $\mathbb{C}/\delta'\mathfrak{a}$. The level structure denoted by $\alpha_\infty^{(p,\ell)\prime}$ in (1.3.6) is then $\alpha_{\infty,\mathbb{C}}(\delta'\mathfrak{a};\delta'\gamma')$, again by (2.4.8). This proves the first assertion, and the remaining one is clear from this. □

In the following corollary, we set $\mathfrak{o}_{n,(p,\ell)} := \mathfrak{o}_n \otimes_{\mathbb{Z}} \mathbb{Z}_{(p,\ell)}$ (cf. (1.2.3) for the symbol $\mathbb{Z}_{(p,\ell)}$), and use $i_p : K^\times \hookrightarrow K_p^\times \hookrightarrow K_{\mathbb{A},\mathrm{f}}^\times$ as well as previously defined $i_\ell : K^\times \hookrightarrow K_\ell^\times \hookrightarrow K_{\mathbb{A},\mathrm{f}}^\times$. Thus, via the natural decomposition $K_{\mathbb{A},\mathrm{f}}^\times = K_{\mathbb{A},\mathrm{f}}^{(p,\ell)\times} \times K_p^\times \times K_\ell^\times$, $c \in K^\times$ decomposes as $c = (c', i_p(c), i_\ell(c))$.

Corollary (2.4.11) *Let the terminology be as above, and take $c \in \mathfrak{o}_{(p,\ell)}^\times$. Then the action of $\rho(c') \in GL_2(\mathbb{A}_{\mathrm{f}}^{(p,\ell)})$ sends $x(\mathfrak{a};\gamma')_{/\mathcal{R}}$ to $x(i_\ell(c^{-1})\mathfrak{a};\gamma')_{/\mathcal{R}}$.*

If c belongs to $\mathfrak{o}_{n,(p,\ell)}^\times$ and $\mathfrak{a}$ is a proper $\mathfrak{o}_n$-ideal, $\rho(c')$ fixes $x(\mathfrak{a};\gamma')_{/\mathcal{R}}$.

If c belongs to $\mathfrak{o}_{n_0,(p,\ell)}^\times$, where n_0 is as in (2.3.1)*, then $\rho(c')$ leaves $\xi^{\mathrm{adm}}(\infty;\underline{n})_{/\mathcal{R}}$ stable.*

Proof By (2.4.10) and (2.4.7), we have

$$\rho(c')(x(\mathfrak{a};\gamma')_{/\mathcal{R}}) = x(c'\mathfrak{a};c'\gamma')_{/\mathcal{R}} = x(i_p(c)^{-1}i_\ell(c)^{-1}\mathfrak{a};\gamma')_{/\mathcal{R}}.$$

Since $c \in \mathfrak{o}^\times_{(p,\ell)}$, $i_p(c)$ belongs to $\mathfrak{o}_p^\times (= \mathfrak{o}^\times_{m,p}$ for all $m \geq 0)$, and hence we have $i_p(c)^{-1}\mathfrak{a} = \mathfrak{a}$, which proves the first assertion. The second (resp. the third) assertion follows from this since $i_\ell(c)^{-1}\mathfrak{a} = \mathfrak{a}$ (resp. $\mathrm{cl}(i_\ell(c)^{-1}\mathfrak{a}) \in R_{n_j}$ when $\mathrm{cl}(\mathfrak{a}) \in R_{n_j}$; cf. (2.3.2)) in the case under consideration. □

We next consider the determinant of the level structures considered above:

Proposition (2.4.12) *Let*

$$\det(\alpha_{\infty,\mathbb{C}}(\mathfrak{o};1)) =: \zeta_{\infty,0} = (\zeta_{N,0})_{p,\ell\nmid N} \in \boldsymbol{\mu}_\infty^{(p,\ell)\mathrm{prim}}(\overline{\mathbb{Q}})$$

be the determinant of $\alpha_{\infty,\mathbb{C}}(\mathfrak{o};1)$ *defined by* (1.2.7)*. Then we have:*

(1) $\det(\alpha_{\infty,\mathbb{C}}(\mathfrak{o}_n;1)) = \zeta_{\infty,0}^{1/\ell^n} := (\zeta_{N,0}^{1/\ell^n})_{p,\ell\nmid N} \in \boldsymbol{\mu}_\infty^{(p,\ell)\mathrm{prim}}(\overline{\mathbb{Q}})$ *for all* $n \geq 0$.

(2) *If* $\mathfrak{a} = \gamma'\mathfrak{o}_n$ *with* $\gamma' \in K^{(p,\ell)\times}_{\mathbb{A},\mathrm{f}}$*, we have:*

$$\det(\alpha_{\infty,\mathbb{C}}(\mathfrak{a};\gamma')) = \det(\alpha_{\infty,\mathbb{C}}(\mathfrak{o}_n;1))^{N_{K/\mathbb{Q}}(\gamma')_0},$$

where $N_{K/\mathbb{Q}}(\gamma')_0 \in \widehat{\mathbb{Z}}^{(p,\ell)\times}$ *is the projection of* $N_{K/\mathbb{Q}}(\gamma') \in \mathbb{A}_{\mathrm{f}}^{(p,\ell)\times}$ *to* $\widehat{\mathbb{Z}}^{(p,\ell)\times}$ *by the decomposition* (1.3.9)*.*

Proof There is a natural (quotient) homomorphism: $\pi : \mathbb{C}/\mathfrak{o}_n \to \mathbb{C}/\mathfrak{o}$ whose degree is ℓ^n. For a positive integer N prime to ℓ, and the $\Gamma(N)$-structure $\alpha_N : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \ni (s,t) \mapsto (sw_1 + tw_2)/N \in \mathbb{C}/\mathfrak{o}_n[N]$, the composite $\pi \circ \alpha_N$ also sends (s,t) to $(sw_1 + tw_2)/N \in \mathbb{C}/\mathfrak{o}[N]$. On the other hand, it is easy to see that $\det(\pi \circ \alpha_N) = \det(\alpha_N)^{\ell^n}$, from which the fist assertion follows.

The second assertion follows from (1.3.10), (2.4.10) and the first relation in (2.4.9). □

One can actually show that $\zeta_{N,0} = e^{2\pi i/N}$ for all N if $\mathrm{Im}(w_2/w_1) > 0$; but we will not need this fact. We also note that the action of $\rho(c')$ $(c \in \mathfrak{o}^\times_{(p,\ell)})$ leaves every irreducible component of $Y^{(p,\ell)}(\infty)_{/\mathcal{R}}$ stable by (1.3.10), because $N_{K/\mathbb{Q}}(c') \in \mathbb{Q}_+^{(p,\ell)\times}$.

Finally, we take the irreducible component $Y^{(p,\ell)}(\infty)^0_{/\mathcal{R}}$ containing $x(\mathfrak{o}_{n_0};1)_{/\mathcal{R}}$. Thus $Y^{(p,\ell)}(\infty)^0_{/\mathcal{R}} = Y^{(p,\ell)}(\infty)^{(\zeta_{\infty,0}^{1/\ell^{n_0}})}_{/\mathcal{R}}$ in the notation of (1.4.4).

Proposition (2.4.13) *Set* $\xi^{\mathrm{adm}}(\infty;\underline{n})^0_{/\mathcal{R}} := \xi^{\mathrm{adm}}(\infty;\underline{n})_{/\mathcal{R}} \cap Y^{(p,\ell)}(\infty)^0_{/\mathcal{R}}(\mathcal{R})$*. If all* $n_j \in \underline{n}$ $(j \geq 0)$ *have the same parity, the natural morphism* $Y^{(p,\ell)}(\infty)^0_{/\mathcal{R}}(\mathcal{R}) \to Y(1)_{/\mathcal{R}}(\mathcal{R})$ *maps* $\xi^{\mathrm{adm}}(\infty;\underline{n})^0_{/\mathcal{R}}$ *surjectively onto* $\xi(1;\underline{n})_{/\mathcal{R}}$*.*

Proof It is enough to show that, for each $\mathrm{cl}(\mathfrak{a}) \in R_{n_j}$ $(j \geq 0)$, we can choose $\mathfrak{a}^\circ = \gamma' \mathfrak{o}_{n_j}$ satisfying $\mathrm{cl}(\mathfrak{a}^\circ) = \mathrm{cl}(\mathfrak{a})$ and $\det(\alpha_{\infty,\mathbb{C}}(\mathfrak{a}^\circ;\gamma')) = \det(\alpha_{\infty,\mathbb{C}}(\mathfrak{o}_{n_0};1))$.

First recall that there is an $\varepsilon \in \mathfrak{o}_{n_0,\ell}^\times$ such that $\mathrm{cl}(\mathfrak{a}) = \mathrm{cl}(\varepsilon \mathfrak{o}_{n_j})$ by (2.1.9). We can take $d \in K^\times$ in such a way that $i_\ell(d)\varepsilon \in \mathfrak{o}_{n_j,\ell}^\times$ and $i_p(d) \in \mathfrak{o}_p^\times$. Set $\gamma_1 := d\epsilon$. Then $\mathfrak{a}_1 := \gamma_1 \mathfrak{o}_{n_j} = \gamma_1{}' \mathfrak{o}_{n_j}$, and γ_1' satisfies $N_{K/\mathbb{Q}}(\gamma_1') = N_{K/\mathbb{Q}}(d') \in \mathbb{Q}_+^{(p,\ell)\times}$ in the decomposition (1.3.9). This shows that $\mathrm{cl}(\mathfrak{a}_1) = \mathrm{cl}(\mathfrak{a})$, and $\det(\alpha_{\infty,\mathbb{C}}(\mathfrak{a}_1,\gamma_1')) = \det(\alpha_{\infty,\mathbb{C}}(\mathfrak{o}_{n_j};1))$ by (2.4.12), (2).

Now set $\gamma := \ell^{(n_j-n_0)/2}\gamma_1$, and $\mathfrak{a}^\circ := \gamma' \mathfrak{o}_{n_j}$. The element $\ell' \in K_{\mathbb{A},\mathrm{f}}^{(p,\ell)\times}$ belongs to $\widehat{\mathbb{Z}}^{(p,\ell)\times} \subset \widehat{\mathfrak{o}}_{n_j}^{(p,\ell)\times}$, and hence $\mathfrak{a}^\circ = \mathfrak{a}_1$. Also since $N_{K/\mathbb{Q}}(\gamma')_0 = \ell'^{(n_j-n_0)} \in \widehat{\mathbb{Z}}^{(p,\ell)\times}$, we have $\det(\alpha_{\infty,\mathbb{C}}(\mathfrak{a}^\circ;\gamma')) = \det(\alpha_{\infty,\mathbb{C}}(\mathfrak{o}_{n_0};1))$ by (2.4.12), as desired. □

§3. Finiteness of irreducible components in projective limits.

3.1. Preliminaries on Galois representations. Throughout this section, we fix a prime number p. In 3.1-3.4, we use the following notation:

(3.1.1)
$$\begin{cases} P\text{: a power of } p, \\ k_0 : \text{a finite field with } P \text{ elements}, \\ k\text{: an algebraic closure of } k_0, \\ L_0\text{: a finitely generated extension field of } k_0 \text{ in which } k_0 \text{ is algebraically closed}, \\ L := L_0 \cdot k, \\ \overline{L} := (\text{a separable closure of } L) = (\text{a separable closure of } L_0), \\ G_L := \mathrm{Gal}(\overline{L}/L), \\ G_{L_0} := \mathrm{Gal}(\overline{L}/L_0). \end{cases}$$

We have a canonical isomorphism: $G_{L_0}/G_L \cong \mathrm{Gal}(k/k_0) = \langle F_P \rangle_{\mathrm{top}}$, the latter group being the procyclic group topologically generated by the P-th power Frobenius automorpism F_P, which is isomorphic to $\widehat{\mathbb{Z}}$.

Let E be an elliptic curve over L_0. For each prime number $l \neq p$, we have the usual l-adic representation

$$\rho_l : G_{L_0} \to GL(T_l(E)) \cong GL_2(\mathbb{Z}_l) \tag{3.1.2}$$

whose restriction to G_L has the image in $SL(T_l(E)) \cong SL_2(\mathbb{Z}_l)$. We denote by $\langle P \rangle_{\mathrm{top},l}$ the subgroup of $\mathbb{Z}_l^\times$ topologically generated by P and set

$$GL^{\langle P \rangle}(T_l(E)) := \{g \in GL(T_l(E)) \mid \det g \in \langle P \rangle_{\mathrm{top},l}\}. \tag{3.1.3}$$

In the following, we often write T_l for $T_l(E)$ when the reference to E is obvious. We have the commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_L & \longrightarrow & G_{L_0} & \longrightarrow & \langle F_P\rangle_{\mathrm{top}} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \rho_l} & & \downarrow{\scriptstyle \rho_l} & & \downarrow{\scriptstyle F_P\mapsto P} & & \\ 1 & \longrightarrow & SL(T_l) & \longrightarrow & GL^{\langle P\rangle}(T_l) & \xrightarrow[\det]{} & \langle P\rangle_{\mathrm{top},l} & \longrightarrow & 1. \end{array} \tag{3.1.4}$$

We then consider these representations simultaneously: Let

$$\widehat{T}^{(p)}(E) = \prod_{l\neq p} T_l(E)$$

be the module already defined in (1.2.4) (considered as the "physical" Tate module), which will also be abbreviated as $\widehat{T}^{(p)}$, and consider the representation

$$\rho_\infty := \prod_{l\neq p} \rho_l : G_{L_0} \to GL(\widehat{T}^{(p)}) \cong GL_2(\widehat{\mathbb{Z}}^{(p)}) \tag{3.1.5}$$

which sends G_L to $SL(\widehat{T}^{(p)}) \cong SL_2(\widehat{\mathbb{Z}}^{(p)})$.

If we denote by $\langle P\rangle_{\mathrm{top}}$ the subgroup of $\widehat{\mathbb{Z}}^{(p)\times}$ topologically generated by P, we have the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_L & \longrightarrow & G_{L_0} & \longrightarrow & \langle F_P\rangle_{\mathrm{top}} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \rho_\infty} & & \downarrow{\scriptstyle \rho_\infty} & & \downarrow{\scriptstyle F_P\mapsto P} & & \\ 1 & \longrightarrow & SL(\widehat{T}^{(p)}) & \longrightarrow & GL^{\langle P\rangle}(\widehat{T}^{(p)}) & \xrightarrow[\det]{} & \langle P\rangle_{\mathrm{top}} & \longrightarrow & 1 \end{array} \tag{3.1.6}$$

where this time we have set

$$GL^{\langle P\rangle}(\widehat{T}^{(p)}) := \{g \in GL(\widehat{T}^{(p)}) \mid \det g \in \langle P\rangle_{\mathrm{top}}\}. \tag{3.1.7}$$

Next, we consider similar representations for a family of elliptic curves: We assume that we are given m elliptic curves $E_1, \cdots, E_m$ over L_0 ($m \geq 1$), and consider

$$\begin{cases} \rho_{l,i} : G_{L_0} \to GL^{\langle P\rangle}(T_{l,i}) \text{ with } T_{l,i} = T_l(E_i), \\ \rho_{\infty,i} : G_{L_0} \to GL^{\langle P\rangle}(\widehat{T}_i^{(p)}) \text{ with } \widehat{T}_i^{(p)} = \widehat{T}^{(p)}(E_i), \end{cases} \tag{3.1.8}$$

as in (3.1.2) ($l \neq p$) and (3.1.5) for $1 \leq i \leq m$. Put

(3.1.9)

$$\begin{cases} A_{l^\infty} := \{(g_1, \cdots, g_m) \in \prod_{i=1}^m GL(T_{l,i}) \mid \det g_1 = \cdots = \det g_m \in \langle P\rangle_{\mathrm{top},l}\}, \\ A_\infty := \{(g_1, \cdots, g_m) \in \prod_{i=1}^m GL(\widehat{T}_i^{(p)}) \mid \det g_1 = \cdots = \det g_m \in \langle P\rangle_{\mathrm{top}}\}. \end{cases}$$

We can then define representations

(3.1.10)

$$\begin{cases} \psi_{l^\infty} = \prod_{i=1}^m \rho_{l,i} : G_{L_0} \to A_{l^\infty} \text{ which satisfies } \psi_{l^\infty}(G_L) \subseteq \prod_{i=1}^m SL(T_{l,i}), \\ \psi_\infty = \prod_{i=1}^m \rho_{\infty,i} : G_{L_0} \to A_\infty \text{ which satisfies } \psi_\infty(G_L) \subseteq \prod_{i=1}^m SL(\widehat{T}_i^{(p)}). \end{cases}$$

Lemma (3.1.11) *Let the notation be as above.*

(1) $\psi_{l^\infty}(G_{L_0})$ *is open in* A_{l^∞} *if* $\psi_{l^\infty}(G_L)$ *is open in* $\prod_{i=1}^m SL(T_{l,i})$.

(2) $\psi_\infty(G_{L_0})$ *is open in* A_∞ *if and only if* $\psi_\infty(G_L)$ *is open in* $\prod_{i=1}^m SL(\widehat{T}_i^{(p)})$.

Proof In the second case, we have the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_L & \longrightarrow & G_{L_0} & \longrightarrow & \langle F_P\rangle_{\mathrm{top}} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \psi_\infty} & & \downarrow{\scriptstyle \psi_\infty} & & \downarrow{\scriptstyle F_P\mapsto P} & & \\ 1 & \longrightarrow & \prod_{i=1}^m SL(\widehat{T}_i^{(p)}) & \longrightarrow & A_\infty & \xrightarrow[\det]{} & \langle P\rangle_{\mathrm{top}} & \longrightarrow & 1 \end{array}$$

where the lower right "det" sends $(g_1, \cdots, g_m) \in A_\infty$ to the common value $\det g_i$. Since the right vertical map is surjective, the cokernel of the middle vertical map is finite if the cokernel of the left vertical map is finite, which proves the "if" part, and the same proof works for the part (1).

In the present second case, we moreover have that the right vertical map is an isomorphism, and hence the "only if" part follows. □

3.2. Function field analogue of a theorem of Serre. In [Se3], Serre proved his celebrated open image theorem for elliptic curves without complex multiplication over number fields. Based on this, he extended such a result to a product of two elliptic curves [Se3, Théorème 6]. The purpose of subsections 3.2-3.3 is to show the function field analogue of this latter result. We thus work under the situation considered in 3.1; and *in* 3.2 *and* 3.3*, we further assume that* $\dim_{k_0} L_0 = 1$*, i.e.* L_0 *is an algebraic function field of one variable over* k_0. Our result is based on the following theorem of Igusa:

Theorem (3.2.1) (cf. [I, Section 5, Theorem 3]) *Let the notation and the assumption be as above, and let* E *be an elliptic curve over* L_0 *whose* j*-invariant is transcendental over* k_0*. Then* $\rho_\infty(G_L)$ *is an open subgroup of* $SL(\widehat{T}^{(p)}(E))$*, and* $\rho_\infty(G_{L_0})$ *is an open subgroup of* $GL^{\langle P\rangle}(\widehat{T}^{(p)}(E))$.

Igusa in fact proved that, if $L_0 = \mathbb{F}_p(j)$ is a rational function field over the prime field, and E is an elliptic curve over L_0 of the absolute invariant j, then $\rho_\infty(G_L) = SL(\widehat{T}^{(p)}(E))$ and $\rho_\infty(G_{L_0}) = GL^{\langle P\rangle}(\widehat{T}^{(p)}(E))$. The extension of $\mathbb{F}_p(j)$ corresponding to ρ_∞ is the quadratic extension of the subfield corresponding to $\{\pm 1\} \subset SL(\widehat{T}^{(p)}(E))$, which is nothing other than the function field of an irreducible component of $Y^{(p)}(\infty)_{/\mathbb{F}}$.

It is therefore natural to expect the following result for the case $m = 2$:

Theorem (3.2.2) *Let the notation and the assumption be as above, and let* E_1 *and* E_2 *be elliptic curves over* L_0 *satisfying the following conditions:*

i) *The* j*-invariants of* E_1 *and* E_2 *are transcendental over* k_0.

ii) E_1 *and* E_2 *are not isogenous over any extension field of* L_0.

Then $\psi_\infty(G_L)$ *is an open subgroup of* $SL(\widehat{T}_1^{(p)}) \times SL(\widehat{T}_2^{(p)})$*; and hence* $\psi_\infty(G_{L_0})$ *is an open subgroup of* A_∞ *also.*

Here are some remarks about the assumption ii) (cf. the remarks after the corollaries of [Se3, Théorème 6]). First we note the following (presumably well-known)

Lemma (3.2.3) *In general, let H_0 be a group and H its normal subgroup. Suppose we are given two representations*

$$\rho_i : H_0 \to GL(V_i),\ i = 1, 2,$$

over n-dimensional vector spaces over a field F of characteristic zero. Assume:

1) *the restrictions $\rho_1 \mid_H$ and $\rho_2 \mid_H$ to H are equivalent,*

2) *$\rho_i \mid_H$ as representations on $V_i \otimes_F \overline{F}$ are irreducible ($i = 1, 2$), $\overline{F}$ being an algebraic closure of F.*

3) $\det \rho_1 = \det \rho_2$.

Then there is a homomorphism $\varepsilon : H_0/H \to \boldsymbol{\mu}_n(F) :=$ (the group of n-roots of unity in $F^\times$) such that ρ_1 and ρ_2 are equivalent on the subgroup $\mathrm{Ker}(\varepsilon)$ of H_0.

Proof By the assumption 1), there is an isomorphism $t : V_1 \xrightarrow{\sim} V_2$ of vector spaces over F such that $t \circ \rho_1(\tau) = \rho_2(\tau) \circ t$ for all $\tau \in H$. Take and fix an element $\sigma \in H_0$. We have an isomorphism

$$u_\sigma := \rho_2(\sigma) \circ t \circ \rho_1(\sigma)^{-1} : V_1 \xrightarrow{\sim} V_2.$$

For any $\tau \in H$, we obtain from the relation $t \circ \rho_1(\sigma^{-1}\tau\sigma) = \rho_2(\sigma^{-1}\tau\sigma) \circ t$ that $u_\sigma \circ \rho_1(\tau) = \rho_2(\tau) \circ u_\sigma$ and hence u_σ is an isomorphism of H-modules. Therefore by the assumption 2), we have: $u_\sigma \circ t^{-1} =$ (multiplication by a scalar $c_\sigma \in F^\times$). We easily see that $\sigma \mapsto c_\sigma$ gives a homomorphism $H_0 \to F^\times$, which we call ε. Since $c_\sigma = \rho_2(\sigma) \circ (t \circ \rho_1(\sigma) \circ t^{-1})^{-1}$, we see from 3) that $c_\sigma^n = 1$. Since $u_\tau = t$ when $\tau \in H$, we see that $c_\tau = 1$ and ε factors as:

$$\varepsilon : H_0 \to H_0/H \to \boldsymbol{\mu}_n(F) \subset F^\times.$$

Finally, for any $\sigma \in \mathrm{Ker}(\varepsilon)$, we have $u_\sigma = t$; i.e. $t \circ \rho_1(\sigma) = \rho_2(\sigma) \circ t$. $\square$

We now return to the situation of (3.2.2).

Proposition (3.2.4) *Let E_1 and E_2 be elliptic curves over L_0 satisfying the condition* i) *in* (3.2.2)*, and let l be a prime number different from p. Then the following four conditions are equivalent.*

1) *E_1 and E_2 are isogenous over some extension field of L_0,*

2) *E_1 and E_2 are isogenous over some finite separable extension field of L_0,*

3) *There is a finite separable extension L_0' of L_0 such that the representations $\rho_{l,1}$ on $T_{l,1} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and $\rho_{l,2}$ on $T_{l,2} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ of $\mathrm{Gal}(\overline{L}/L_0')$ are equivalent,*

4) *There is a finite separable extension L' of L such that the representations $\rho_{l,1}$ on $T_{l,1} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and $\rho_{l,2}$ on $T_{l,2} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ of $\mathrm{Gal}(\overline{L}/L')$ are equivalent.*

Proof The equivalence of 1) and 2) are well-known, and the implications 2) $\Rightarrow$ 3) $\Rightarrow$ 4) are clear.

4) $\Rightarrow$ 3): Let L' be as in 4). There is a finite separable extension L'_0 of L_0 such that $L'_0 \cdot k = L'$. Then apply the previous lemma to $H_0 = \mathrm{Gal}(\overline{L}/L'_0)$ and $H = \mathrm{Gal}(\overline{L}/L')$.

The remaining (hardest) implication 3) $\Rightarrow$ 2) is a consequence of a theorem of Zarhin who proved a conjecture of Tate for abelian varieties over function fields in positive characteristic; cf. [Z]. $\square$

3.3. Proof of (3.2.2). In this subsection, we prove Theorem (3.2.2) following Serre. The method is the same as in his paper. In the following, we write E for E_1, ρ_l for the representation (3.1.2) for E on $T_l(E) = T_l$, etc.; and we write E' for E_2, and express the corresponding objects for E' by putting a prime symbol: ρ'_l, T'_l, etc. We will always assume i) and ii) in (3.2.2).

Lemma (3.3.1) (cf. [Se3, Lemme 7]) *For any prime number $l \neq p$, the image of the l-adic representation*

$$\rho_l \times \rho'_l : G_L \to SL(T_l) \times SL(T'_l)$$

is open.

Proof $(\rho_l \times \rho'_l)(G_L)$ is an l-adic Lie subgroup of $SL(T_l) \times SL(T'_l)$. Let

$$\mathfrak{g}_l := \mathrm{Lie}((\rho_l \times \rho'_l)(G_L)) \subseteq \mathfrak{h}_l := \mathfrak{sl}(V_l) \oplus \mathfrak{sl}(V'_l) \cong \mathfrak{sl}_2(\mathbb{Q}_l) \oplus \mathfrak{sl}_2(\mathbb{Q}_l)$$

be their Lie algebras, where $V_l := T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and $V'_l := T'_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. We want to show that $\mathfrak{g}_l = \mathfrak{h}_l$.

By (3.2.1), the two projections from $\mathfrak{g}_l$ to $\mathfrak{sl}(V_l)$ and $\mathfrak{sl}(V'_l)$ are surjective. Since $\mathfrak{sl}_2(\mathbb{Q}_l)$ is simple, if $\mathfrak{g}_l \neq \mathfrak{h}_l$, we must have that $\mathfrak{g}_l$ is a graph of a Lie algebra isomorphism $\alpha : \mathfrak{sl}(V_l) \xrightarrow{\sim} \mathfrak{sl}(V'_l)$. Then as in [Se3], there is a $\mathbb{Q}_l$-linear isomorphism $f : V_l \xrightarrow{\sim} V'_l$ such that $\alpha(u) = f \circ u \circ f^{-1}$ for all $u \in \mathfrak{sl}(V_l)$. It follows that there is an open subgroup U of $(\rho_l \times \rho'_l)(G_L)$ such that f is a U-module isomorphism. Thus if L' is the subfield of $\overline{L}$ corresponding to U, ρ_l and ρ'_l are isomorphic on $\mathrm{Gal}(\overline{L}/L')$, which contradicts our assumption ii) in (3.2.2), by (3.2.4). $\square$

Our next purpose is to show Lemma (3.3.3) below. To do this, for a prime number l different from p, we define

$$\begin{cases} E_l := E[l](\overline{L}), \\ \varphi_l : G_{L_0} \to GL^{\langle P \rangle}(E_l) := \{g \in GL(E_l) \mid \det g \in \langle P \rangle \subseteq (\mathbb{Z}/l\mathbb{Z})^\times\}, \end{cases}$$

and also E'_l, φ'_l for E' similarly; and consider

$$\psi_l : G_{L_0} \to A_l := \{(g, g') \in GL(E_l) \times GL(E'_l) \mid \det(g) = \det(g') \in \langle P \rangle\},$$

through the natural action of the Galois group. By the assumption (3.2.2), i), φ_l and φ'_l are surjective for almost all l, by (3.2.1).

Lemma (3.3.2) (cf. [Se3, Lemme 8]) *Let $l(\neq p)$ be a prime number ≥ 5 such that:*

$$\varphi_l \text{ and } \varphi_l' \text{ are surjective, but } \psi_l \text{ is not surjective.}$$

Then there is a continuous homomorphism $\varepsilon_l : G_{L_0} \to \{\pm 1\}$ and an isomorphism $f : E_l \to E_l'$ satisfying:

$$f \circ \varphi_l(s) = \varepsilon_l(s) \circ \varphi_l'(s) \circ f \text{ for all } s \in G_{L_0}.$$

Further, ε_l is unramified at every prime of L_0/k_0 at which E and E' have good reduction.

Proof Put $B := GL^{\langle P \rangle}(E_l)$, $B' := GL^{\langle P \rangle}(E_l')$, $A := A_l$ and $H := \psi_l(G_{L_0})$ so that $H \subseteq A \subseteq B \times B'$, and the projections from H to B and B' are surjective. Identifying B with the subgroup $B \times \{1\}$ of $B \times B'$, we set $N := B \cap H$. Thus N is a normal subgroup of B contained in $SL(E_l)$. As is well-known, $PSL(E_l) := SL(E_l)/\{\pm 1\}$ is a noncommutative simple group when $l \geq 5$, and no proper subgroup of $SL(E_l)$ maps surjectively onto $PSL(E_l)$ (cf. [Se2, IV-23, Lemmas 1 and 2]). Therefore N must be one of $SL(E_l)$, $\{\pm 1\}$ or $\{1\}$. The same holds for $N' := B' \cap H$. Now by "Goursat's lemma" (cf. Ribet [R, Lemma (3.2)]), the image of H in $B/N \times B'/N'$ is the graph of an isomorphism $\alpha : B/N \xrightarrow{\sim} B'/N'$. If $N = SL(E_l)$, then $H \supseteq SL(E_l) \times \{1\}$ and hence $H \supseteq SL(E_l) \times SL(E_l')$ which implies that $H = A$, contradicting our assumption. We therefore have $N \subseteq \{\pm 1\}$ and $N' \subseteq \{\pm 1\}$, and N and N' have the same order since so are B/N and B'/N'.

On the other hand, it is clear that $C := GL^{\langle P \rangle}(E_l) \cap \mathbb{F}_l^\times$ ($\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}$, identified with the scalar multiplication endomorphisms) is the center of $GL^{\langle P \rangle}(E_l)$, and it is easy to see that $C/\{\pm 1\}$ is the center of $GL^{\langle P \rangle}(E_l)/\{\pm\}$; and the same holds for $C' := GL^{\langle P \rangle}(E_l') \cap \mathbb{F}_l^\times$. Therefor α induces an isomorphism $C/\{\pm 1\} \xrightarrow{\sim} C'/\{\pm 1\}$, and whence an isomorphism $\widetilde{\alpha} : B/C \xrightarrow{\sim} B'/C'$. The image of B/C in $PGL(E_l) := GL(E_l)/\mathbb{F}_l^\times$ is either $PSL(E_l)$ or $PGL(E_l)$ because the index of $PSL(E_l)$ in $PGL(E_l)$ is two; and the image of B'/C' in $PGL(E_l')$ is either $PSL(E_l')$ or $PGL(E_l')$ accordingly. But it is known that any automorphism of $PGL_2(\mathbb{F}_l)$ is inner, and any automorphism of $PSL_2(\mathbb{F}_l)$ is obtained by the restriction of such an automorphism on $PGL_2(\mathbb{F}_l)$ (cf. [R, Proposition (3.7)]). We conclude that there is an isomorphism $f : E_l \xrightarrow{\sim} E_l'$ such that $\widetilde{\alpha}(u) = f \circ u \circ f^{-1}$ for all $u \in B/C$. Take $h = (u, u') \in H$. It follows from the above that $u' = \varepsilon(h) f \circ u \circ f^{-1}$ with $\varepsilon(h) \in \mathbb{F}_l^\times$. Taking the determinants, we see that $\varepsilon(h)^2 = 1$. Thus ε gives a map $H \to \{\pm 1\}$, which is easily seen to be a homomorphism. If we denote by ε_l the composite of $G_{L_0} \xrightarrow{\psi_l} H \xrightarrow{\varepsilon} \{\pm 1\}$, we have $\varphi_l'(s) = \varepsilon_l(s) f \circ \varphi_l(s) \circ f^{-1}$ for all $s \in G_{L_0}$, which proves the first assertion.

Finally, φ_l and φ_l' are unramified at every prime of L_0/k_0 at which E and E' have good reduction; and hence so is ε_l. $\square$

We use this lemma to prove:

Lemma (3.3.3) (cf. [Se3, Lemme 9]) *We have $\psi_l(G_{L_0}) = A_l$ for almost all prime numbers l.*

Proof Assume otherwise. Then there is an infinite set $\mathcal{L}$ of prime numbers $l \geq 5$ ($l \neq p$), such that both φ_l and φ'_l are surjective but ψ_l is not. For such an l, the previous lemma provides us with a character $\varepsilon_l : G_{L_0} \to \{\pm 1\}$ satisfying the unramifiedness condition stated there. It follows that the set of such characters is finite; and hence replacing $\mathcal{L}$ by its infinite subset, we may assume that ε_l is common to all $l \in \mathcal{L}$, which we denote by ε. Thus if we denote by F_0 the extension of L_0 corresponding to $\mathrm{Ker}(\varepsilon)$ ($[F_0 : L_0] \leq 2$), E_l and E'_l are isomorphic as modules over $G_{F_0} := \mathrm{Gal}(\overline{L}/F_0)$ for all $l \in \mathcal{L}$.

It follows that for any prime v of F_0 at which E and E' have good reduction, the traces of the Frobenius endomorphisms $t_v(E)$ on E and $t_v(E')$ on E' are congruent modulo l for all $l \in \mathcal{L}$. Therefore we have $t_v(E) = t_v(E')$. Since two representations of G_{F_0}, ρ_l on V_l and ρ'_l on V'_l are simple, Čebotarev density theorem (cf. Weil [W, Chapter XIII, § 12, Theorem 12]) implies that these two representations are equivalent for any $l \neq p$. This again contradicts our assumption (3.2.2), ii). □

Recall that we have the representation ψ_∞ defined by (3.1.10), which in the present case gives us $\psi_\infty : G_{L_0} \to A_\infty \subseteq GL(\widehat{T}^{(p)}) \times GL(\widehat{T}^{(p)\prime})$, and it induces $G_L \to SL(\widehat{T}^{(p)}) \times SL(\widehat{T}^{(p)\prime})$. Set

$$\begin{cases} \widetilde{G}_L := \psi_\infty(G_L), \\ H_l := (SL(T_l) \times SL(T'_l)) \cap \widetilde{G}_L, \end{cases}$$

for each prime number $l \neq p$, where we consider $SL(T_l) \times SL(T'_l)$ as the direct factor of $SL(\widehat{T}^{(p)}) \times SL(\widehat{T}^{(p)\prime})$. Note that H_l is a normal subgroup of $\psi_\infty(G_{L_0})$, and that we have an exact sequence:

$$1 \to H_l \to \widetilde{G}_L \to \prod_{l' \neq l,p} (SL(T_{l'}) \times SL(T'_{l'})).$$

Lemma (3.3.4) (cf.[Se2, ChapterIV, 3.4, Lemma5]) *Two projections $H_l \to SL(T_l)$ and $H_l \to SL(T'_l)$ are surjections for almost all prime numbers l.*

Proof We recall that, via the projections, $\widetilde{G}_L$ maps surjectively onto $SL(T_l)$ and $SL(T'_l)$ for almost all l, by (3.2.1). We only consider such $l > 5$ in the following.

In general, for a profinite group Y, denote by $\mathrm{Occ}(Y)$ the set of isomorphism classes of finite noncommutative simple groups that "occur" in Y; i.e. those isomorphic to Y_1/Y_2 for suitable closed subgroups Y_1 and Y_2 of Y with Y_2 normal in Y_1. See [Se2, Chapter IV, 3.4] for basic properties of this assignment. Especially, from the above exact sequence, we have:

$$\mathrm{Occ}(\widetilde{G}_L/H_l) \subseteq \cup_{l' \neq l,p} \mathrm{Occ}(SL(T_{l'}) \times SL(T'_{l'})).$$

Consider the composite of homomorphisms:

$$H_l \hookrightarrow \widetilde{G}_L \twoheadrightarrow SL(T_l) \twoheadrightarrow PSL(E_l).$$

The image of H_l is a normal subgroup of the simple group $PSL(E_l)$. If this is trivial, then we have that (the isomorphism class of) $PSL(E_l) \cong PSL_2(\mathbb{F}_l) \in \mathrm{Occ}(\widetilde{G}_L/H_l)$. It follows from the above relation that this belongs to $\mathrm{Occ}(SL_2(\mathbb{Z}_{l'}))$ for some prime $l' \neq l$, p, which is impossible. We conclude that H_l maps surjectively onto $PSL(E_l)$, which implies that $H_l \to SL(T_l)$ is also surjective by loc. cit. Lemmas 2 and 3; and similarly for $H_l \to SL(T_l')$. $\square$

Corollary (3.3.5) (cf. [Se3, Lemme 11]) *The group H_l coincides with the direct factor $SL(T_l) \times SL(T_l')$ of $SL(\widehat{T}^{(p)}) \times SL(\widehat{T}^{(p)\prime})$ for almost all l.*

Proof It is enough to show that $H_l \subseteq SL(T_l) \times SL(T_l')$ maps surjectively onto $SL(E_l) \times SL(E_l')$ for almost all l by [Se3 , Lemme 10]. For this, we may assume that $l > 5$.

Let $\overline{H}_l$ be the image of H_l in $SL(E_l) \times SL(E_l')$. We know that $\overline{H}_l$ is a normal subgroup of $\psi_l(G_{L_0})$ and that $\psi_l(G_{L_0}) = A_l$ for almost all l by (3.3.3). We conclude from this and (3.3.4) that $\overline{H}_l$ is a normal subgroup of $SL(E_l) \times SL(E_l')$ which projects to two direct factors surjectively, for almost all l. That such a subgroup must coincide with $SL(E_l) \times SL(E_l')$ follows from the argument as in the proof of (3.3.2): Set $N := \overline{H}_l \cap SL(E_l)$ and $N' := \overline{H}_l \cap SL(E_l')$. "Goursat's lemma" implies that $\overline{H}_l$ gives the graph of an isomorphism: $SL(E_l)/N \xrightarrow{\sim} SL(E_l')/N'$. If $N = SL(E_l)$ or $N' = SL(E_l')$, we are done. Otherwise, N and N' are both trivial, or both equal to $\{\pm 1\}$, in which cases we easily get contradiction from the normality of $\overline{H}_l$. $\square$

We can now proceed to prove Theorem (3.2.2). By (3.3.5), there is a finite set S of prime numbers ($S \not\ni p$) such that $\psi_\infty(G_L) = \widetilde{G}_L$ contains the direct factor $\widetilde{G}_S' := \prod_{l \notin S, l \neq p}(SL(T_l) \times SL(T_l'))$ of $SL(\widehat{T}^{(p)}) \times SL(\widehat{T}^{(p)\prime})$. Therefore, if we denote by $\widetilde{G}_S$ the projection of $\widetilde{G}_L$ to $\prod_{l \in S}(SL(T_l) \times SL(T_l'))$, we have a direct product decomposition $\widetilde{G}_L = \widetilde{G}_S \times \widetilde{G}_S'$.

Lemma (3.3.6) (cf. [Se2, Chapter IV, 3.4, Lemma 4]) *$\widetilde{G}_S$ is an open subgroup of $\prod_{l \in S}(SL(T_l) \times SL(T_l'))$.*

Proof $SL(T_l) \times SL(T_l')$ contains an open pro-l subgroup N_l (product of congruence subgroups). It is thus enough to show that $\widetilde{G}_S \cap \prod_{l \in S} N_l =: \widetilde{G}_S^\circ$ is open in $\prod_{l \in S} N_l$. But then $\widetilde{G}_S^\circ$ is a pronilpotent group and hence it is a product of l-Sylow subgroups $\widetilde{G}_{S,l}^\circ$ contained in N_l. Lemma (3.3.1) assures us that $\widetilde{G}_{S,l}^\circ$ is open in N_l, which completes the proof. $\square$

This completes the proof of Theorem (3.2.2).

Question: Is it possible to give a simpler proof of (3.2.2) using the geometry of modular curves?

3.4. Generalization via a lemma of Ribet. Ribet [R, Theorem (3.5)] generalized Serre's theorem for products of more than two elliptic curves over

number fields. It was a consequence of a group theoretical lemma. We recall its special case in the form convenient for our purpose:

Lemma (3.4.1) (cf. [R, Lemma (3.4)]) *Suppose that we are given profinite groups $\mathcal{S}_i$ $(1 \leq i \leq t\ ;\ t \geq 2)$ such that $\mathcal{S}_i \cong \prod_{l \in P_i} SL_2(\mathbb{Z}_l)$ with a set P_i of prime numbers for each i, and let $\mathcal{S} = \mathcal{S}_1 \times \cdots \times \mathcal{S}_t$ be their product. Let $\mathcal{G}$ be a closed subgroup of $\mathcal{S}$ which projects to an open subgroup of $\mathcal{S}_i \times \mathcal{S}_j$ for each pair (i,j) $(i \neq j)$. Then $\mathcal{G}$ is an open subgroup of $\mathcal{S}$.*

We now return to the general situation considered in 3.1: We let the fields $L/L_0/k_0$ etc. be as in (3.1.1) for which we no longer assume that $\dim_{k_0} L_0 = 1$, and let $E_1, \cdots, E_m$ be elliptic curves over L_0. We can then consider Galois representation ψ_∞ defined in (3.1.10).

Theorem (3.4.2) *The notation being as above, assume that:*

i) *The j-invariants of E_i are transcendental over k_0 for $1 \leq i \leq m$.*

ii) *E_i and E_j are not isogenous over any extension field of L_0 for $1 \leq i, j \leq m$ $(i \neq j)$.*

Then $\psi_\infty(G_{L_0})$ is an open subgroup of A_∞, and $\psi_\infty(G_L)$ is an open subgroup of $\prod_{i=1}^m SL(\widehat{T}^{(p)}(E_i))$.

Proof First note that it suffices to prove the second assertion by (3.1.11). When $m = 1$ the claim follows easily from (3.2.1), and hence we assume that $m \geq 2$. Then for any pair (i,j) as above, the representation ψ_∞ of G_L followed by the projection

$$\psi_\infty^{(i,j)} : G_L \to SL(\widehat{T}^{(p)}(E_i)) \times SL(\widehat{T}^{(p)}(E_j))$$

is of course the representation attached to two elliptic curves E_i and E_j over L_0. Therefore by Ribet's lemma (3.4.1), to prove (3.4.2), it enough to prove it for $m = 2$. Namely we need to prove (3.2.2) without assuming that $\dim_{k_0} L_0 = 1$.

So we consider E_1 and E_2 over general L_0 satisfying i) and ii). Fix a positive integer $N_0 \geq 3$ prime to p and a primitive N_0-th root of unity $\zeta_{N_0} \in k$. Replacing L_0 by a finite separable extension if necessary, we may assume from the beginning that $E_1[N_0]$ and $E_2[N_0]$ are constant over L_0 (and hence ζ_{N_0} belongs to k_0). We fix a $\Gamma(N_0)$-structure of determinant ζ_{N_0} on each E_i in the following. These data define morphisms $\eta_i : \mathrm{Spec}(L_0) \to Y(N_0)^{(\zeta_N)}_{/k_0} =: Y$ to the moduli scheme Y classifying elliptic curves with a $\Gamma(N_0)$-structure of determinant ζ_{N_0} over k_0-schemes, so that E_i is the pullback by η_i of the universal elliptic curve on Y. Let $\eta : \mathrm{Spec}(L_0) \to Y \times_{k_0} Y$ be the morphism corresponding to η_1 and η_2.

Y is an affine scheme, and we denote by A its coordinate ring. Therefore η defines a ring homomorphism $L_0 \leftarrow A \otimes_{k_0} A$. Let $\mathfrak{p}$ be its kernel. By our assumption i), $\mathfrak{p}$ is a non-maximal prime ideal. If the height of $\mathfrak{p}$ is one, the quotient field F_0 of $(A \otimes_{k_0} A)/\mathfrak{p}$ is a function field over k_0 of one variable, and E_i are obtained from elliptic curves $E_{i,0}$ over F_0 satisfying i) and ii) by

base extension to L_0. Since L_0 is a finitely generated extension of F_0, Theorem (3.2.2) for $E_{i,0}$ over F_0 implies Theorem (3.4.2) for E_i over L_0. In the remaining case where $\mathfrak{p} = (0)$, it is clear that (3.4.2) holds for two elliptic curves over the quotient field of $A \otimes_{k_0} A$ obtained from the universal curve on Y via two projections $Y \times_{k_0} Y \rightrightarrows Y$, and hence (3.4.2) is also true in this case. This completes the proof of (3.4.2). $\square$

3.5. Torsors defined by elliptic curves. For a positive integer N, a $\mathbb{Z}[1/N]$-scheme S, and an elliptic curve E over S, we consider the S-scheme

$$I_N(E/S) := \mathrm{Isom}_{S\text{-gp}}(\underline{\mathbb{Z}/N\mathbb{Z}} \times \underline{\mathbb{Z}/N\mathbb{Z}}, E[N]) \tag{3.5.1}$$

which represents the functor $(\mathrm{Schemes}/S)\ni T \mapsto$ (the set of $\Gamma(N)$-structures on $E_T := E \times_S T$) (cf. (1.1.1)). It is therefore the S-scheme denoted $[\Gamma(N)]_{E/S}$ (with $\mathcal{P} = [\Gamma(N)]$) in [KM, (4.2), (4.6)], and is a $GL_2(\mathbb{Z}/N\mathbb{Z})$-torsor over S with respect to the right action (1.1.4). (Cf. [SGA 1, V, Section 2] for basic facts about torsors under a finite group $\mathcal{G}$, where the terminology "principal coverings of Galois group $\mathcal{G}$" is used.) Clearly, its formation commutes with base changes:

$$I_N(E/S) \times_S T \cong I_N(E_T/T) \text{ for any } S\text{-scheme } T, \tag{3.5.2}$$

and when M is a positive divisor of N, there is a natural S-morphism

$$I_N(E/S) \to I_M(E/S), \tag{3.5.3}$$

defined by the correspondence $\alpha_N \mapsto \alpha_M$ (1.1.8).

There is a natural S-morphism $I_N(E/S) \to \boldsymbol{\mu}_{N/S}^{\mathrm{prim}} = \boldsymbol{\mu}_N^{\mathrm{prim}} \times_{\mathbb{Z}} S$ given by $\alpha_N \mapsto \det(\alpha_N)$ (cf. (1.1.2) and (1.1.3) for notation). Assume that S is a $\mathbb{Z}[1/N, \mu_N]$-scheme, μ_N being the group of N-th roots of unity in $\overline{\mathbb{Q}}$. Also take and fix $\zeta_N \in \boldsymbol{\mu}_N^{\mathrm{prim}}(\overline{\mathbb{Q}})$. This determines a section $S \to \boldsymbol{\mu}_{N/S}^{\mathrm{prim}}$ corresponding to the ring homomorphism $\mathbb{Z}[X]/(\Phi_N(X)) \to \Gamma(S, \mathcal{O}_S)$ given by $X \mapsto \zeta_N$. Then via the base change by this morphism, we obtain

$$I_N(E/S)^{(\zeta_N)} := I_N(E/S) \times_{\boldsymbol{\mu}_{N/S}^{\mathrm{prim}}} S. \tag{3.5.4}$$

This S-scheme classifies $\Gamma(N)$-structures of determinant ζ_N on E_T for S-schemes T. It is an $SL_2(\mathbb{Z}/N\mathbb{Z})$-torsor over S by (1.1.5).

We keep the assumption that S is a $\mathbb{Z}[1/N, \mu_N]$-scheme. Assume that we are given a positive divisor N_0 of N, and let $\zeta_{N_0} = \zeta_N^{N/N_0}$. Then (3.5.3) induces an S-morphism $I_N(E/S)^{(\zeta_N)} \to I_{N_0}(E/S)^{(\zeta_{N_0})}$, "($\alpha_N$ of determinant ζ_N) $\mapsto$ (α_{N_0} of determinant ζ_{N_0})"; cf. (1.1.9). We further assume that we are given $\alpha_{N_0} \in I_{N_0}(E/S)^{(\zeta_{N_0})}(S)$, a section of $I_{N_0}(E/S)^{(\zeta_{N_0})}$ over S. We then form the fibre product:

$$I_N(E/S)^{(\zeta_N)}\,|_{\alpha_{N_0}} := I_N(E/S)^{(\zeta_N)} \times_{I_{N_0}(E/S)^{(\zeta_{N_0})}} S, \tag{3.5.5}$$

the inverse image of α_{N_0}. Thus if we set

$$SL_2(\mathbb{Z}/N\mathbb{Z}; N_0) := \{g \in SL_2(\mathbb{Z}/N\mathbb{Z}) \mid g \equiv 1 \pmod{N_0}\}, \tag{3.5.6}$$

$I_N(E/S)^{(\zeta_N)}\,|_{\alpha_{N_0}}$ is an $SL_2(\mathbb{Z}/N\mathbb{Z}; N_0)$-torsor over S, because $I_N(E/S)^{(\zeta_N)}$ is an $SL_2(\mathbb{Z}/N\mathbb{Z}; N_0)$-torsor over $I_{N_0}(E/S)^{(\zeta_{N_0})}$. Using these terminologies, we have the following rather tautological

Lemma (3.5.7) *Assume that $N_0 \geq 3$, and let $(\mathcal{E}, \alpha_{N_0}^{\mathrm{univ}})$ be the universal elliptic curve with $\Gamma(N_0)$-structure over $Y(N_0)_{/R}^{(\zeta_{N_0})}$, where $R = \mathbb{Z}[1/N, \mu_N]$ for simplicity. Then we have a canonical isomorphism over R:*

$$I_N(\mathcal{E}/Y(N_0)_{/R}^{(\zeta_{N_0})})^{(\zeta_N)}\,|_{\alpha_{N_0}^{\mathrm{univ}}} \cong Y(N)_{/R}^{(\zeta_N)}.$$

If M is anther positive divisor of N divisible by N_0 and $\zeta_M = \zeta_N^{N/M}$, the above defined isomorphisms for N and M are compatible with natural morphisms

$$\begin{cases} Y(N)_{/R}^{(\zeta_N)} \to Y(M)_{/R}^{(\zeta_M)}, \\ I_N(\mathcal{E}/Y(N_0)_{/R}^{(\zeta_{N_0})})^{(\zeta_N)}\,|_{\alpha_{N_0}^{\mathrm{univ}}} \to I_M(\mathcal{E}/Y(N_0)_{/R}^{(\zeta_{N_0})})^{(\zeta_M)}\,|_{\alpha_{N_0}^{\mathrm{univ}}}\ . \end{cases}$$

Proof For any R-scheme T, we have a canonical identification of

$$I_N(\mathcal{E}/Y(N_0)_{/R}^{(\zeta_{N_0})})^{(\zeta_N)}\,|_{\alpha_{N_0}^{\mathrm{univ}}}(T)$$

$$= I_N(\mathcal{E}/Y(N_0)_{/R}^{(\zeta_{N_0})})^{(\zeta_N)}(T) \times_{I_{N_0}(\mathcal{E}/Y(N_0)_{/R}^{(\zeta_{N_0})})^{(\zeta_{N_0})}(T)} Y(N_0)_{/R}^{(\zeta_{N_0})}(T)$$

with the set of T-isomorphism classes of the pairs (E_T, α_N) consisting of an elliptic curve and a $\Gamma(N)$-structure of determinant ζ_N over T, because the pair consisting of E_T and a $\Gamma(N_0)$-structure has no non-trivial automorphism. This proves the first assertion, and the second one is also clear. □

We next want to study the set of irreducible components of the torsors considered above, when S is the spectrum of a field. In the rest of this section, we assume that $S = \mathrm{Spec}(F)$ with a field F. We let $\overline{F}$ be a separable closure of F, and G_F the Galois group of $\overline{F}$ over F.

For the moment, Let $X = \mathrm{Spec}(A)$ be a $\mathcal{G}$-torsor over S, $\mathcal{G}$ being a finite group. Thus A is a finite étale F-algebra:

$$A = \oplus_{i=1}^n A_i \text{ with finite separable field extensions } A_i \text{ of } F.$$

We have $X = \coprod_{i=1}^n C_i$ with $C_i := \mathrm{Spec}(A_i)$, and $\{C_1, \cdots, C_n\}$ is the set of irreducible components of X, which we denote by $\mathrm{Irr}(X)$. Set

$$\mathcal{G}_i := \{g \in \mathcal{G} \mid C_i^g = C_i\}.$$

This group acts on C_i (resp. A_i) from the right (resp. left). Since $\mathcal{G}$ acts simply transitively on $X(\overline{F})$, it also acts transitively on the set $\mathrm{Irr}(X)$.

Lemma (3.5.8) *Let the notation be as above. We have a bijection*

$$\mathcal{G}_i\backslash\mathcal{G} \xrightarrow{\sim} \mathrm{Irr}(X) \text{ by the correspondence } \mathcal{G} \ni g : C_i \to C_i^g \text{ for each } i.$$

A_i is a Galois extension of F, and we have

$$\mathcal{G}_i \xrightarrow{\sim} \mathrm{Aut}(C_i/S) \cong \mathrm{Gal}(A_i/F).$$

Proof It follows from the remark above that the first map is bijective. It also follows that the homomorphism $\mathcal{G}_i \to \mathrm{Aut}(C_i/S)$ is injective for each i; and since the action of $\mathcal{G}_i$ on $C_i(\overline{F})$ is transitive, the order of $\mathcal{G}_i$ satisfies $^{\#}\mathcal{G}_i \geq {}^{\#}C_i(\overline{F}) = [A_i : F]$, which completes the proof. □

The Galois group G_F acts on $X(\overline{F}) = \coprod_{i=1}^n C_i(\overline{F})$ from the left, and preserves each $C_i(\overline{F})$.

Lemma (3.5.9) *Fix a point $Q \in X(\overline{F})$, belonging to $C_i(\overline{F})$. For each $\sigma \in G_F$, there is a unique $g(\sigma) \in \mathcal{G}$ such that $\sigma Q = Q^{g(\sigma)}$. We obtain a map $G_F \to \mathcal{G}_i$ by $\sigma \mapsto g(\sigma)$, and this is a surjective homomorphism.*

Proof Since the Galois action preserves $C_i(\overline{F})$, $g(\sigma)$ belongs to $\mathcal{G}_i$, and it is easy to see that the above map is a homomorphism of G_F to $\mathcal{G}_i$. Since the action of G_F on $C_i(\overline{F}) = \mathrm{Hom}_F(A_i, \overline{F})$ is transitive, the number of the elements of the image is ${}^{\#}C_i(\overline{F}) = {}^{\#}\mathcal{G}_i$ by the previous lemma. □

Summing up, we obtain the following

Proposition (3.5.10) *Fix $Q \in X(\overline{F})$ and let $C_Q \in \mathrm{Irr}(X)$ be the irreducible component containing Q. We have a homomorphism $G_F \to \mathcal{G}$ by the correspondence: $\sigma \mapsto g(\sigma)$ defined by $\sigma Q = Q^{g(\sigma)}$. Let $\mathcal{H}_Q$ be the image of this homomorphism. Then we have a bijection*

$$\mathcal{H}_Q\backslash\mathcal{G} \xrightarrow{\sim} \mathrm{Irr}(X) \text{ by } g \mapsto C_Q^g.$$

□

We now turn our attention to the torsors attached to elliptic curves over $S = \mathrm{Spec}(F)$. Take an elliptic curve E over S and a positive integer N prime to the characteristic of F. In this case, an element Q of $I_N(E/S)(\overline{F})$ is nothing but a $\Gamma(N)$-structure on $E_{/\overline{F}} = E \otimes_F \overline{F}$. Take and fix one such $Q = \alpha_N$. Via the canonical isomorphism $E[N] \otimes_F \overline{F} \cong E[N](\overline{F}) \times \mathrm{Spec}(\overline{F})$, giving α_N is equivalent to giving a group isomorphism $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} E[N](\overline{F})$, which we call α'_N. From such an α'_N, we obtain the Galois representation

$$\rho_{N,Q} : G_F \to GL_2(\mathbb{Z}/N\mathbb{Z})$$

in the usual manner by the commutativity of

$$\begin{array}{ccc} \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} & \xrightarrow[\sim]{\alpha'_N} & E[N](\overline{F}) \\ {\scriptstyle \rho_{N,Q}(\sigma)}\downarrow & & \downarrow{\scriptstyle \text{action of } \sigma} \\ \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} & \xrightarrow[\alpha'_N]{\sim} & E[N](\overline{F}) \end{array} \tag{3.5.11}$$

for $\sigma \in G_F$.

Proposition (3.5.12) *Let the notation be as above, and fix a point $Q = \alpha_N \in I_N(E/S)(\overline{F})$. Let C_Q be the irreducible component of $I_N(E/S)$ containing Q. Then we have a bijection*

$$\rho_{N,Q}(G_F)\backslash GL_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \mathrm{Irr}(I_N(E/S)) \ \text{ by } g \mapsto C_Q^g.$$

Proof For $\sigma \in G_F$, $\sigma Q = \sigma\alpha_N$ is obtained from α_N by base change by the action of σ on $\mathrm{Spec}(\overline{F})$:

$$\begin{array}{ccccc} \underline{\mathbb{Z}/N\mathbb{Z}} \times \underline{\mathbb{Z}/N\mathbb{Z}} & \xrightarrow{\sigma\alpha_N} & E[N] \otimes_F \overline{F} & \xrightarrow{\sim} & E[N](\overline{F}) \times \mathrm{Spec}(\overline{F}) \\ {\scriptstyle \mathrm{id}\times}\downarrow{\scriptstyle \mathrm{Spec}(\sigma)} & & {\scriptstyle \mathrm{id}\otimes}\downarrow{\scriptstyle \mathrm{Spec}(\sigma)} & & {\scriptstyle \sigma^{-1}\times}\downarrow{\scriptstyle \mathrm{Spec}(\sigma)} \\ \underline{\mathbb{Z}/N\mathbb{Z}} \times \underline{\mathbb{Z}/N\mathbb{Z}} & \xrightarrow{\alpha_N} & E[N] \otimes_F \overline{F} & \xrightarrow{\sim} & E[N](\overline{F}) \times \mathrm{Spec}(\overline{F}) \end{array}$$

for the schemes obtained by base extension from F to $\overline{F}$. The commutativity of this diagram means that $(\sigma\alpha_N)' = \alpha'_N \circ \rho_{N,Q}(\sigma)$ and hence $\sigma\alpha_N = \alpha_N \circ \rho_{N,Q}(\sigma)$; i.e. the element denoted above by $g(\sigma) \in GL_2(\mathbb{Z}/N\mathbb{Z})$ is $\rho_{N,Q}(\sigma)$. Our claim follows from the previous proposition. $\square$

Clearly the same argument can be used to describe the sets $\mathrm{Irr}(I_N(E/S)^{(\zeta_N)})$ and $\mathrm{Irr}(I_N(E/S)^{(\zeta_N)}\ |_{\alpha_{N_0}})$. We include the result for the latter set in the following

Variant (3.5.13) Assume that F contains a primitive N-th root of unity ζ_N. Let N_0 be a positive divisor of N and set $\zeta_{N_0} = \zeta_N^{N/N_0}$. Let $E_1, \cdots, E_m$ be elliptic curves over F, given with a $\Gamma(N_0)$-structure $\alpha_{N_0,i}$ of determinant ζ_{N_0} on each E_i over F. Then the S-scheme

$$X := I_N(E_1/S)^{(\zeta_N)}\ |_{\alpha_{N_0,1}} \times_S \cdots \times_S I_N(E_m/S)^{(\zeta_N)}\ |_{\alpha_{N_0,m}}$$

is a torsor under $\mathcal{G} := SL_2(\mathbb{Z}/N\mathbb{Z}; N_0)^m$, the product of m copies of $SL_2(\mathbb{Z}/N\mathbb{Z}; N_0)$. Take and fix a point $Q = (\alpha_{N,1}, \cdots, \alpha_{N,m}) \in X(\overline{F})$. Then we obtain representations $\rho_{N,i} : G_F \to GL_2(\mathbb{Z}/N\mathbb{Z})$ as in (3.5.11) which factor through $SL_2(\mathbb{Z}/N\mathbb{Z}; N_0) \hookrightarrow GL_2(\mathbb{Z}/N\mathbb{Z})$ for $1 \le i \le m$, giving rise to

$$\rho_{N,Q} := \rho_{N,1} \times \cdots \times \rho_{N,m} : G_F \to SL_2(\mathbb{Z}/N\mathbb{Z}; N_0)^m.$$

Let C_Q be the irreducible component of X containing Q. Then we have the following bijection:

$$\rho_{N,Q}(G_F)\backslash SL_2(\mathbb{Z}/N\mathbb{Z};N_0)^m \xrightarrow{\sim} \mathrm{Irr}(X) \quad \text{by } g \mapsto C_Q^g.$$

3.6. A result on the finiteness of irreducible components. In this subsection, we consider modular curves over fields of characteristic $p>0$. We for the moment work over an algebraic closure $\mathbb{F}$ of the prime field $\mathbb{F}_p$. Throughout we fix a compatible system of primitive N-th roots of unity $\zeta_\infty = (\zeta_N) \in \boldsymbol{\mu}_\infty^{(p)\mathrm{prim}}(\mathbb{F}) = \varprojlim_{p\nmid N} \boldsymbol{\mu}_N^{\mathrm{prim}}(\mathbb{F})$ and consider irreducible modular curves

$$\text{(3.6.1)} \qquad \begin{cases} Y(N)^0_{/\mathbb{F}} := Y(N)^{(\zeta_N)}_{/\mathbb{F}}, \\ Y^{(p)}(\infty)^0_{/\mathbb{F}} := Y^{(p)}(\infty)^{(\zeta_\infty)}_{/\mathbb{F}} = \varprojlim_{p\nmid N} Y(N)^0_{/\mathbb{F}} \end{cases}$$

(cf. 1.4).

We also fix $N_0 \geq 3$ prime to p. $Y^{(p)}(\infty)^0_{/\mathbb{F}}$ is a Galois covering of $Y(1)_{/\mathbb{F}}$ with group $SL_2(\widehat{\mathbb{Z}}^{(p)})/\{\pm 1\}$; and is an étale Galois covering of $Y(N_0)^0_{/\mathbb{F}}$ with group

$$\text{(3.6.2)} \quad SL_2(\widehat{\mathbb{Z}}^{(p)};N_0) := \varprojlim_{p\nmid N, N_0 | N} SL_2(\mathbb{Z}/N\mathbb{Z};N_0) = \mathrm{Ker}(SL_2(\widehat{\mathbb{Z}}^{(p)}) \to SL_2(\mathbb{Z}/N_0\mathbb{Z})).$$

For a positive integer m, as in 2.3, we set

$$\text{(3.6.3)} \quad \begin{cases} ((Y(N)^0_{/\mathbb{F}})^m := \text{the } m\text{-fold fibre product of } Y(N)^0_{/\mathbb{F}} \text{ over } \mathbb{F}, \\ ((Y^{(p)}(\infty)^0_{/\mathbb{F}})^m := \text{the } m\text{-fold fibre product of } Y^{(p)}(\infty)^0_{/\mathbb{F}} \text{ over } \mathbb{F}, \\ f_N^m : (Y^{(p)}(\infty)^0_{/\mathbb{F}})^m \to (Y(N)^0_{/\mathbb{F}})^m : \text{the natural morphism.} \end{cases}$$

The following is the main result of this section:

Theorem (3.6.4) *Let Z be an irreducible closed subvariety of $(Y(N_0)^0_{/\mathbb{F}})^m$ defined over $\mathbb{F}$. Assume the following two conditions:*

i) *Let $\overline{p}_i$ be the composite of the closed immersion $Z \hookrightarrow (Y(N_0)^0_{/\mathbb{F}})^m$ and the projection $p_i : (Y(N_0)^0_{/\mathbb{F}})^m \to Y(N_0)^0_{/\mathbb{F}}$ to the i-th direct factor. Then $\overline{p}_i$ is dominant for each $1 \leq i \leq m$;*

ii) *Let $E_{Z,i}$ be the pull-back to Z of the universal elliptic curve on $Y(N_0)^0_{/\mathbb{F}}$ by $\overline{p}_i$. Then for each pair $(i,j) \subseteq \{1,\cdots,m\}$ $(i \neq j)$, the generic fibres of $E_{Z,i}$ and $E_{Z,j}$ are not isogenous over any extension field.*

Then the inverse image of Z to $(Y^{(p)}(\infty)^0_{/\mathbb{F}})^m$:

$$(f_{N_0}^m)^{-1}(Z) = Z \times_{(Y(N_0)^0_{/\mathbb{F}})^m} (Y^{(p)}(\infty)^0_{/\mathbb{F}})^m$$

has only a finite number of irreducible components.

Proof For the moment fix a positive multiple N of N_0 prime to p, and let $(Y(N)^0_{/\mathbb{F}})_i$ be the base change to $(Y(N_0)^0_{/\mathbb{F}})^m$ of $Y(N)^0_{/\mathbb{F}} \to Y(N_0)^0_{/\mathbb{F}}$ by p_i. Then $(Y(N)^0_{/\mathbb{F}})^m$ is $(Y(N_0)^0_{/\mathbb{F}})^m$-isomorphic to the fibre product of these $(Y(N)^0_{/\mathbb{F}})_i$ $(1 \le i \le m)$ over $(Y(N_0)^0_{/\mathbb{F}})^m$. Denoting by $(\mathcal{E}_i, p_i^*\alpha_{N_0}^{\mathrm{univ}})$ the base extension by p_i of the universal pair $(\mathcal{E}, \alpha_{N_0}^{\mathrm{univ}})$ on $Y(N_0)^0_{/\mathbb{F}}$, we see from (3.5.7) and (3.5.2) that:

$$(Y(N)^0_{/\mathbb{F}})_i \cong I_N(\mathcal{E}_i/(Y(N_0)^0_{/\mathbb{F}})^m)^0 \mid_{p_i^*\alpha_{N_0}^{\mathrm{univ}}}$$

as $SL_2(\mathbb{Z}/N\mathbb{Z}; N_0)$-torsors over $(Y(N_0)^0_{/\mathbb{F}})^m$, where we wrote $I_N(-)^0$ for $I_N(-)^{(\zeta_N)}$.

Letting $(E_{Z,i}, \alpha_{N_0,Z,i})$ be the pull-back of $(\mathcal{E}, \alpha_{N_0}^{\mathrm{univ}})$ by $\overline{p}_i$, it follows from this that

$$Z \times_{(Y(N_0)^0_{/\mathbb{F}})^m} (Y(N)^0_{/\mathbb{F}})^m \cong I_N(E_{Z,1}/Z)^0 \mid_{\alpha_{N_0,Z,1}} \times_Z \cdots \times_Z I_N(E_{Z,m}/Z)^0 \mid_{\alpha_{N_0,Z,m}}$$

as $SL_2(\mathbb{Z}/N\mathbb{Z}; N_0)^m$-torsors over Z. These are étale coverings of Z, and so, the irreducible components of these schemes correspond bijectively with those of the generic fibre over Z. So letting L be the function field of Z, and $(E_i, \alpha_{N_0,i}) := (E_{Z,i}, \alpha_{N_0,Z,i}) \times_Z \mathrm{Spec}(L)$ the generic fibre of $(E_{Z,i}, \alpha_{N_0,Z,i})/Z$ $(1 \le i \le m)$, we obtain a canonical bijection:

$$\mathrm{Irr}(Z \times_{(Y(N_0)^0_{/\mathbb{F}})^m} (Y(N)^0_{/\mathbb{F}})^m) \cong \mathrm{Irr}(\mathcal{I}_N)$$

where

$$\mathcal{I}_N := I_N(E_1/S)^0 \mid_{\alpha_{N_0,1}} \times_S \cdots \times_S I_N(E_m/S)^0 \mid_{\alpha_{N_0,m}} \quad \text{with } S = \mathrm{Spec}(L).$$

It therefore follows that we have bijections

$$\mathrm{Irr}((f_{N_0}^m)^{-1}(Z)) \cong \varprojlim_{p\nmid N, N_0 \mid N} \mathrm{Irr}(Z \times_{(Y(N_0)^0_{/\mathbb{F}})^m} (Y(N)^0_{/\mathbb{F}})^m) \cong \varprojlim_{p\nmid N, N_0 \mid N} \mathrm{Irr}(\mathcal{I}_N)$$

(cf. Appendix (A.2.1)). Take and fix $Q_\infty = (Q_N)_{p\nmid N, N_0 \mid N} \in (\varprojlim_{p\nmid N, N_0 \mid N} \mathcal{I}_N)(\overline{L}) = (\varprojlim_{p\nmid N, N_0 \mid N} (\mathcal{I}_N(\overline{L}))$ with each $Q_N \in \mathcal{I}_N(\overline{L})$. This provides with us, via (3.5.13), a Galois representation

$$\rho_{\infty, Q_\infty} := \varprojlim_{p\nmid N, N_0 \mid N} \rho_{N, Q_N} : G_L \to SL_2(\widehat{\mathbb{Z}}^{(p)}; N_0)^m,$$

and a bijection

$$\varprojlim_{p\nmid N, N_0 \mid N} \mathrm{Irr}(\mathcal{I}_N) \cong \rho_{\infty, Q_\infty}(G_L) \backslash SL_2(\widehat{\mathbb{Z}}^{(p)}; N_0)^m.$$

Here, ρ_{∞, Q_∞} is exactly the Galois representation denoted by ψ_∞ in (3.1.10) attached to elliptic curves $E_1, \cdots, E_m$ over L, transformed in the above form by the isomorphism ("coordinate system") : $(\widehat{\mathbb{Z}}^{(p)} \times \widehat{\mathbb{Z}}^{(p)})^m \xrightarrow{\sim} \widehat{T}^{(p)}(E_1) \times \cdots \times \widehat{T}^{(p)}(E_m)$ given by Q_∞. Finally, we remark that, although we started with a

closed subvariety Z of $(Y(N_0)^0_{/\mathbb{F}})^m$ defined over $\mathbb{F}$, it comes by base extension to $\mathbb{F}$ from a closed subvariety $Z_0 \hookrightarrow (Y(N_0)^0_{/k_0})^m$ defined over some finite extension k_0 of the prime field $\mathbb{F}_p$. We conclude by Theorem (3.4.2) that the set $\mathrm{Irr}((f^m_{N_0})^{-1}(Z))$ is finite. $\square$

The essential point of the proof of (3.6.4) was the open image result (3.4.2). We give below another application of this result. For this, in general, let E be an ordinary elliptic curve over a finite field with p^n elements, and F_E the p^n-th power Frobenius endomorphism of E. Let $f_E(X) = X^2 - \mathrm{trace}(F_E)X + p^n \in \mathbb{Z}[X]$ be the characteristic polynomial of F_E. By the ordinariness assumption, this polynomial has the unique unit root in $\mathbb{Q}_p$, which we call $\alpha(E)$. Thus we have $\mathrm{trace}(F_E) = \alpha(E) + p^n\alpha(E)^{-1}$. If E' is another ordinary elliptic curve over the same field, then obviously $\alpha(E) = \pm\alpha(E')$ implies $\mathrm{trace}(F_E) = \pm\mathrm{trace}(F_{E'})$.

Now let $Z \subset (Y(N_0)^0_{/\mathbb{F}})^m$ be as in (3.6.4). As we observed above, it is obtained by base extension to $\mathbb{F}$ from a closed subvariety $Z_0 \subset (Y(N_0)^0_{/k_0})^m$ defined over a finite subfield k_0 of $\mathbb{F}$. Accordingly, we have elliptic curves $E_{Z_0,i}$ over Z_0 $(1 \leq i \leq m)$ defined as (3.6.4) ii) (which were implicitly used in the proof of (3.6.4)).

Proposition (3.6.5) *Let the notation and the assumption be as above. For a closed point x of Z_0, we let $E_{Z_0,i/x}$ be the fibre of $E_{Z_0,i}$ at x.*

Then there are infinitely many closed points x of Z_0 satisfying the following conditions:

1) *$E_{Z_0,i/x}$ are ordinary $(1 \leq i \leq m)$.*

2) *If $i \neq j$, we have $\alpha(E_{Z_0,i/x}) \neq \pm\alpha(E_{Z_0,j/x})$ for the unit roots of the Frobenius endomorphism.*

Moreover, when a proper Zariski closed subset C of Z_0 is given, we can take these points x from $Z_0 - C$.

Proof Let L_0 be the function field of Z_0, and $E_{L_0,i}$ the generic fibre of $E_{Z_0,i}/Z_0$. Setting $T_{l,i} := T_l(E_{L_0,i})$ for prime numbers $l \neq p$, we obtain representations of Galois groups

$$\begin{array}{ccc} G_L & \longrightarrow & \prod_{i=1}^m SL(T_{l,i}/l^M T_{l,i}) \\ {\scriptstyle \mathrm{incl.}}\downarrow & & \downarrow{\scriptstyle \mathrm{incl.}} \\ G_{L_0} & \longrightarrow & \prod_{i=1}^m GL(T_{l,i}/l^M T_{l,i}) \end{array}$$

for any positive integer M. Theorem (3.4.2) guarantees that the upper horizontal arrows are surjective for any M for all but a finite number of l $(l \nmid N_0)$. Fix such l and $M \gg 0$, and let L_2 (resp. L_1) be the extension of L_0 corresponding to the kernel of the lower horizontal arrow (resp. the maximal constant field subextension of L_2/L_0). Thus $\mathrm{Gal}(L_2/L_1)$ is canonically isomorphic to $\prod_{i=1}^m SL(T_{l,i}/l^M T_{l,i})$. We then obtain étale Galois coverings $X_0 \to Y_0 \to Z_0$ whose generic points give the field extensions $L_2/L_1/L_0$; X_0/Y_0 being obtained from an étale covering of a product of modular curves by base change. Via the

canonical isomorphism $\mathrm{Gal}(X_0/Y_0) \cong \prod_{i=1}^m SL(T_{l,i}/l^M T_{l,i}) \cong SL_2(\mathbb{Z}/l^M\mathbb{Z})^m$, we may identify

$$R := \{(g_1, \cdots, g_m) \in SL_2(\mathbb{Z}/l^M\mathbb{Z})^m \mid \pm\mathrm{trace}(g_1), \cdots, \pm\mathrm{trace}(g_m) \text{ are all different}\}$$

with a subset of $\mathrm{Gal}(X_0/Y_0)$. Let us take M so large that this set is non-empty. Then Čebotarev density theorem, as formulated in Serre [Se1, Theorem 7], applies to assure that the set of closed points of Y_0 whose Frobenius conjugacy class belongs to R is of positive density.

If a proper Zariski closed subset $C \subset Z_0$ is given, the set of such closed points of Y_0 not in the inverse image of C still have positive density. Especially we may exclude points corresponding to supersingular elliptic curves to obtain the same result. If y is such a closed point of Y_0, the elliptic curves $E_{Z_0,i/y}$, the fibres at y of $E_{Z_0,i} \times_{Z_0} Y_0$, satisfy the properties 1) and 2), by the preceding remark. The image of these points to Z_0 satisfy the same properties. □

§4. Zariski density of CM points.

4.1. "Independence" of elliptic curves. In this final section, we will prove the main theorem (2.3.4).

We thus return to the situation considered in 2.3: We fix an imaginary quadratic field K in which p splits, and a prime number $\ell \neq p$. We take a sequence $\underline{n} = \{0 \leq n_0 < n_1 < \cdots\}$ of integers, $\delta_1, \cdots, \delta_m \in \mathrm{Ker}(\mathrm{Cl}_\infty \to \mathrm{Cl}_{n_0})$ which give distinct classes in $\mathrm{Cl}_\infty/\mathrm{Cl}^{\mathrm{alg}}$, and define a set of closed points $\Xi(1;\underline{n})_{/\mathbb{F}}$ of $(Y(1)_{/\mathbb{F}})^m$; cf. (2.3.1)-(2.3.4).

In what follows, when we are given a subset T of a scheme X, we will always consider the Zariski closure of T in X as a reduced closed subscheme of X. When the reference to X is obvious, we denote this scheme $\overline{T}$.

Proposition (4.1.1) *Let the notation be as above. Let N_0 be an integer ≥ 3, and $\Lambda(N_0)$ a set of closed points of $(Y(N_0)^0_{/\mathbb{F}})^m$ mapping surjectively onto $\Xi(1;\underline{n})_{/\mathbb{F}}$. Take an irreducible component Z of the Zariski closure of $\Lambda(N_0)$ in $(Y(N_0)^0_{/\mathbb{F}})^m$. If $\dim Z > 0$, Z satisfies the conditions* i) *and* ii) *in* (3.6.4).

Proof $Z \cap \Lambda(N_0)$ is an infinite set. So the image of the composite $Z \hookrightarrow (Y(N_0)^0_{/\mathbb{F}})^m \xrightarrow{p_i} Y(N_0)^0_{/\mathbb{F}}$ contains infinitely many distinct points as seen from the definition of $\Xi(1;\underline{n})_{/\mathbb{F}}$. The condition (3.6.4), i) is therefore satisfied.

To show the second condition, we fix indices i and j $(1 \leq i, j \leq m, i \neq j)$. Let L be the field of rational functions of Z, and consider the situation similar to the proof of (3.4.2):

$$\mathrm{Spec}(L) \to Z \hookrightarrow (Y(N_0)^0_{/\mathbb{F}})^m \xrightarrow{(p_i,p_j)} Y(N_0)^0_{/\mathbb{F}} \times_{\mathbb{F}} Y(N_0)^0_{/\mathbb{F}}.$$

These schemes are all affine. Set $Y(N_0)^0_{/\mathbb{F}} = \mathrm{Spec}(A)$ and $Z = \mathrm{Spec}(B)$ so that we have ring homomorphisms:

$$L \hookleftarrow B \leftarrow A \otimes_{\mathbb{F}} A.$$

The kernel $\mathfrak{p}$ of the right homomorphism is a non-maximal prime ideal. Let $\mathcal{E}'_i$ and $\mathcal{E}'_j$ be the elliptic curves over $C := \mathrm{Spec}((A \otimes_{\mathbb{F}} A)/\mathfrak{p})$ obtained by pulling back the universal elliptic curve via $C \to Y(N_0)^0_{/\mathbb{F}} \times_{\mathbb{F}} Y(N_0)^0_{/\mathbb{F}}$ followed by two projections to $Y(N_0)^0_{/\mathbb{F}}$. We want to show that the generic fibres of $\mathcal{E}'_i$ and $\mathcal{E}'_j$ over any finite extension of the quotient field $\mathcal{L}$ of $(A \otimes_{\mathbb{F}} A)/\mathfrak{p}$ are non-isogenous.

If $\mathfrak{p} = (0)$, this is obvious. We henceforth assume that $\mathfrak{p}$ is of height one, and hence C is an irreducible reduced curve over $\mathbb{F}$. Let $\mathcal{L}'$ be a finite extension of $\mathcal{L}$, and C' the normalization of C in $\mathcal{L}'$. Set $\mathcal{E}''_i := \mathcal{E}'_i \times_C C'$ and $\mathcal{E}''_j = \mathcal{E}'_j \times_C C'$. Assume that there were an isogeny over $\mathcal{L}'$ between the generic fibres of these curves. It then extends uniquely to an isogeny $\lambda : \mathcal{E}''_i :\to \mathcal{E}''_j$ over C' by the Néron property. Since $Z \cap \Lambda(N_0)$ is infinite, the image of Z to $C \hookrightarrow Y(N_0)^0_{/\mathbb{F}} \times_{\mathbb{F}} Y(N_0)^0_{/\mathbb{F}}$ contains closed points lying above the points of the form $x_r := (x(\alpha_i \mathfrak{a}_r), x(\alpha_j \mathfrak{a}_r)) \in Y(1)_{/\mathbb{F}} \times_{\mathbb{F}} Y(1)_{/\mathbb{F}}$ for infinitely many values $r \in \underline{n}$, where $\mathrm{cl}(\mathfrak{a}_r) \in R_r$ (cf. (2.3.2)) and α_i, α_j are as in (2.3.4). Let $E(\mathfrak{a})_{/\mathcal{K}}$ be the elliptic curve over $\mathcal{K}$ whose complex points are isomorphic to $\mathbb{C}/\mathfrak{a}$ as described in 2.4, and let $E(\mathfrak{a})_{/\mathcal{W}}$ (resp. $E(\mathfrak{a})_{/\mathbb{F}}$) be its extension to $\mathcal{W}$ (resp. the reduction to $\mathbb{F}$). Then taking the fibre at an inverse image in C' of each x_r, we obtain from λ an isogeny $\lambda_{x_r} : E(\alpha_i \mathfrak{a}_r)_{/\mathbb{F}} \to E(\alpha_j \mathfrak{a}_r)_{/\mathbb{F}}$. This then lifts to an isogeny $\widetilde{\lambda}_{x_r} : E(\alpha_i \mathfrak{a}_r)_{/\mathcal{W}} \to E(\alpha_j \mathfrak{a}_r)_{/\mathcal{W}}$ over $\mathcal{W}$ because $E(\alpha_i \mathfrak{a}_r)_{/\mathcal{W}}$ (resp. $E(\alpha_j \mathfrak{a}_r)_{/\mathcal{W}}$) is the canonical lifting of $E(\alpha_i \mathfrak{a}_r)_{/\mathbb{F}}$ (resp. $E(\alpha_j \mathfrak{a}_r)_{/\mathbb{F}}$); cf Messing [M, Chapter V, Corollary (3.4)]. This in turn gives us an isogeny of complex tori $\mathbb{C}/\alpha_i \mathfrak{a}_r \to \mathbb{C}/\alpha_j \mathfrak{a}_r$ of the same degree as λ for each r. We may assume that $\mathfrak{a}_r$ is of the form $\mathfrak{a}_r = c_r \mathfrak{o}_r$ with $c_r \in \mathfrak{o}_\ell^\times$, and also that $\alpha_i, \alpha_j \in \mathfrak{o}_\ell^\times$ by (2.1.9). We have obtained isogenies

$$\mathbb{C}/(c_r \alpha_i)\mathfrak{o}_r \to \mathbb{C}/(c_r \alpha_i)(\alpha_i^{-1}\alpha_j)\mathfrak{o}_r$$

of degree independent of r for infinitely many values $r \in \underline{n}$. But our assumption implies that $(\mathrm{cl}(\alpha_i^{-1}\alpha_j \mathfrak{o}_n)_{n \geq 0}) \in \mathrm{Cl}_\infty$ does not belong to $\mathrm{Cl}^{\mathrm{alg}}$. We have seen in (2.2.6) that this condition rules out the possibility of the existence of such an infinite family of isogenies. $\square$

Therefore $Z \subseteq (Y(N_0)^0_{/\mathbb{F}})^m$ obtained in the above manner, and its model Z_0 over a finite subfield of $\mathbb{F}$, satisfy the conclusions of (3.6.4) and (3.6.5), respectively.

4.2. Tate-linearity. In this section, we prove (2.3.4). To do this, aside from the notation already used in 4.1, we need to recall the constructions in 2.4: We first recall that we defined the set of admissible CM points $\xi^{\mathrm{adm}}(\infty; \underline{n})_{/\mathbb{F}}$ in $Y^{(p,\ell)}(\infty)_{/\mathbb{F}}$ in (2.4.6), which will be considered as a set consisting of closed points of $Y^{(p,\ell)}(\infty)_{/\mathbb{F}}$. We take the irreducible component $Y^{(p,\ell)}(\infty)^0_{/\mathbb{F}}$ of $Y^{(p,\ell)}(\infty)_{/\mathbb{F}}$ containing the point $x(\mathfrak{o}_{n_0}; 1)_{/\mathbb{F}}$ and set $\xi^{\mathrm{adm}}(\infty; \underline{n})^0_{/\mathbb{F}} = \xi^{\mathrm{adm}}(\infty; \underline{n})_{/\mathbb{F}} \cap Y^{(p,\ell)}(\infty)^0_{/\mathbb{F}}$ as in (2.4.13). We hereafter always assume that *all elements in the infinite set* $\underline{n}$ *have the same parity*, as it is enough to prove (2.3.4) under this condition. This assures that $\xi^{\mathrm{adm}}(\infty; \underline{n})^0_{/\mathbb{F}}$ maps surjectively onto $\xi(1; \underline{n})_{/\mathbb{F}}$ by (2.4.13).

Definition (4.2.1) We take and fix $\delta_1, \cdots, \delta_m \in \mathrm{Ker}(\mathrm{Cl}_\infty \to \mathrm{Cl}_{n_0})$ giving distinct elements in $\mathrm{Cl}_\infty/\mathrm{Cl}^{\mathrm{alg}}$, and choose $\alpha_i \in K^\times_{\mathbb{A},\mathrm{f}}$ as in (2.3.4) so that $\delta_i = (\mathrm{cl}(\alpha_i \mathfrak{o}_n))_{n\geq 0}$. We let $\Xi^{\mathrm{adm}}(\infty; \underline{n})^0$ be the set of closed points of $(Y^{(p,\ell)}(\infty)^0_{/\mathbb{F}})^m$ defined by

$$\{(x(\alpha_1\mathfrak{a}; (\alpha_1\gamma_1)')_{/\mathbb{F}}, \cdots, x(\alpha_m\mathfrak{a}; (\alpha_m\gamma_m)')_{/\mathbb{F}}) \mid x(\mathfrak{a}; \gamma_i')_{/\mathbb{F}} \in \xi^{\mathrm{adm}}(\infty; \underline{n})^0_{/\mathbb{F}} \ (1 \leq i \leq m)\}.$$

For $M \geq 1$ prime to p and ℓ, we define $\Xi^{\mathrm{adm}}(M; \underline{n})^0$ as the image of $\Xi^{\mathrm{adm}}(\infty; \underline{n})^0$ by the morphism $(Y^{(p,\ell)}(\infty)^0_{/\mathbb{F}})^m \to (Y(M)^0_{/\mathbb{F}})^m$.

The sets $\Xi^{\mathrm{adm}}(\infty; \underline{n})^0$ and $\Xi^{\mathrm{adm}}(M; \underline{n})^0$ therefore depend on δ_i $(1 \leq i \leq m)$, but in view of (2.1.8) and (2.4.7), do not depend on the choice of α_i $(1 \leq i \leq m)$.

We fix an integer $N_0 \geq 3$ prime to p and ℓ. Our goal will be to show that $\Xi^{\mathrm{adm}}(N_0; \underline{n})^0$ is Zariski dense in $(Y(N_0)^0_{/\mathbb{F}})^m$. Remember that this statement is equivalent to Theorem (2.3.4); cf. (2.3.5), (1). The theorem is obvious for $m = 1$. *We hereafter assume that $m > 1$, and assume that* (2.3.4) *is true up to $(m-1)$-fold self-products of $Y(N_0)^0_{/\mathbb{F}}$, but false for the m-fold self-product, until we arrive at a contradiction at the end of this section.*

Let us take any partial direct product factor $(Y(N_0)^0_{/\mathbb{F}})^{m-1}$ of $(Y(N_0)^0_{/\mathbb{F}})^m$, and let pr be the projection to this factor. Then $pr(\Xi^{\mathrm{adm}}(N_0; \underline{n})^0)$ is a set defined exactly in the same manner as $\Xi^{\mathrm{adm}}(N_0; \underline{n})^0$ for $(Y(N_0)^0_{/\mathbb{F}})^{m-1}$. By the above assumption, this is a Zariski dense subset of $(Y(N_0)^0_{/\mathbb{F}})^{m-1}$. Therefore, pr induces a dominant morphism of the Zariski closure $\overline{\Xi^{\mathrm{adm}}(N_0; \underline{n})^0}$ to $(Y(N_0)^0_{/\mathbb{F}})^{m-1}$. Since we are assuming that (2.3.4) does not hold for $(Y(N_0)^0_{/\mathbb{F}})^m$, it follows that there is an irreducible component of dimension $m-1$ in $\overline{\Xi^{\mathrm{adm}}(N_0; \underline{n})^0}$. Take and fix such an irreducible component, and call it Z.

In general, for a scheme X and its closed subscheme W, denote by $X^{/W}$ the formal completion of X along W. Let x be a closed point of $(Y(N_0)^0_{/\mathbb{F}})^m$ which is ordinary in the sense that it corresponds to an m-tuple of ordinary elliptic curves. Then it is known from the theory of Serre and Tate that $(Y(N_0)^0_{/\mathbb{F}})^{m/x}$ canonically has a structure of a formal torus over $\mathbb{F}$. If V is a closed subvariety of $(Y(N_0)^0_{/\mathbb{F}})^m$ and $x \in V$ is as above, V is said to be *Tate-linear at x* if $V^{/x}$ is a formal subtorus of the Serre-Tate formal torus $(Y(N_0)^0_{/\mathbb{F}})^{m/x}$. This notion was introduced and studied in detail by Chai [C1] in connection with the Hecke orbit problem. Its importance in the arithmetic, for example the study of the special values of Hecke L-functions, was found by Hida.

Proposition (4.2.2) *Let the notation be as above. Z is Tate-linear at every ordinary normal closed point of Z.*

Although we stated the result for Z lying in the product of modular curves of finite level, it is indispensable to go up to infinite level, as observed by Hida. We will describe a proof of this proposition in several steps below.

First, we note that it is enough to prove the Tate-linearity for one (ordinary normal) point of Z, for then a result of Chai assures us that the whole statement

is valid. Chai in fact proved a stronger result in [C1, Proposition 5.3]; the result of the above form follows from [C1, Proposition 5.2], either by the same reasoning as loc. cit. or from the fact that $(Y(N_0)^0_{/\mathbb{F}})^m$ is closely immersed in a Siegel modular variety.

We now consider the infinite covering

$$g^m_{N_0} : (Y^{(p,\ell)}(\infty)^0_{/\mathbb{F}})^m = \varprojlim_{p,\ell\nmid M} (Y(M)^0_{/\mathbb{F}})^m \to (Y(N_0)^0_{/\mathbb{F}})^m.$$

Since the projective limit is taken with respect to finite surjective morphisms, this is a closed morphism (cf. Appendix (A.1.2)), and hence $g^m_{N_0}$ induces a surjective morphism: $\overline{\Xi^{\mathrm{adm}}(\infty;\underline{n})^0} \twoheadrightarrow \overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0}$. Thus there is an irreducible component $\widetilde{Z}$ of $\overline{\Xi^{\mathrm{adm}}(\infty;\underline{n})^0}$ such that $g^m_{N_0}(\widetilde{Z}) = Z$, and since $\widetilde{Z}$ is integral over Z, $\dim \widetilde{Z} = m-1$.

Lemma (4.2.3) *We have*

$$\widetilde{Z} = \overline{\Xi^{\mathrm{adm}}(\infty;\underline{n})^0 \cap \widetilde{Z}},$$

and this is an irreducible component of $(g^m_{N_0})^{-1}(\overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0})$.

Proof Write $\overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0} = \cup_{i=0}^{m-1} I_i$ with I_i the union of all irreducible components of dimension i of $\overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0}$, and hence $(g^m_{N_0})^{-1}(\overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0}) = \cup_{i=0}^{m-1}\mathcal{I}_i$ with $\mathcal{I}_i = (g^m_{N_0})^{-1}(I_i)$. We have:

$$\overline{\Xi^{\mathrm{adm}}(\infty;\underline{n})^0} = \cup_{i=0}^{m-1} \overline{\Xi^{\mathrm{adm}}(\infty;\underline{n})^0 \cap \mathcal{I}_i}.$$

Since $\widetilde{Z}$ is its irreducible component, $\widetilde{Z}$ must be contained in one of the members in the right hand side; and since $\widetilde{Z}$ maps to Z, we have $\widetilde{Z} \subseteq \overline{\Xi^{\mathrm{adm}}(\infty;\underline{n})^0 \cap \mathcal{I}_{m-1}}$. Now by (4.1.1) and (3.6.4), $\mathcal{I}_{m-1}$ is a union of *finite number of* irreducible components: $\mathcal{I}_{m-1} = \cup_{j=1}^s D_j$ with irreducible components D_j. We therefore have

$$\widetilde{Z} \subseteq \cup_{j=1}^s \overline{\Xi^{\mathrm{adm}}(\infty;\underline{n})^0 \cap D_j}.$$

Again the irreducibility of $\widetilde{Z}$ implies that there is an index j such that

$$\widetilde{Z} \subseteq \overline{\Xi^{\mathrm{adm}}(\infty;\underline{n})^0 \cap D_j} \subseteq D_j.$$

Since $\dim D_j < m$, we conclude that $\widetilde{Z} = D_j$. $\square$

Let Z° be the intersection of Z with the smooth locus of $\overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0}$. This is a non-empty open subscheme of Z, and for any closed point z of Z°, Z is the only irreducible component of $\overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0}$ containing z. By the lemma above, $g^m_{N_0}(\Xi^{\mathrm{adm}}(\infty;\underline{n})^0 \cap \widetilde{Z})$ is dense in Z, and hence we can take a closed point $z' \in \Xi^{\mathrm{adm}}(\infty;\underline{n})^0 \cap \widetilde{Z}$ such that $z := g^m_{N_0}(z') \in Z^\circ$. Since $(g^m_{N_0})^{-1}(\overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0})$ is a pro-étale covering of $\overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0}$, $\widetilde{Z}$ is the only irreducible component of

$(g_{N_0}^m)^{-1}(\overline{\Xi^{\mathrm{adm}}(N_0;\underline{n})^0})$ containing z'. Fix such choice of z' and z. The morphism $\widetilde{Z} \to Z$ is pro-étale at z', and we have the commutative diagram with two vertical isomorphisms:

$$\begin{array}{ccc} \widetilde{Z}^{/z'} & \xrightarrow{\text{incl.}} & (Y^{(p,\ell)}(\infty)^0_{/\mathbb{F}})^{m/z'} \\ \wr\downarrow & & \downarrow\wr \\ Z^{/z} & \xrightarrow[\text{incl.}]{} & (Y(N_0)^0_{/\mathbb{F}})^{m/z}. \end{array} \tag{4.2.4}$$

Recall that we have an action of $K_{\mathbb{A},\mathrm{f}}^{(p,\ell)\times}$ on $Y^{(p,\ell)}(\infty)_{/\mathbb{F}}$ via the representation ρ (2.4.8). We then let $K_{\mathbb{A},\mathrm{f}}^{(p,\ell)\times}$ act on $(Y^{(p,\ell)}(\infty)_{/\mathbb{F}})^m$ diagonally. We see from (2.4.11) (cf. also a remark after (2.4.12)) that the action of $\mathfrak{o}^\times_{n_0,(p,\ell)}$, via $c \mapsto \rho(c')$, leaves $\overline{\Xi^{\mathrm{adm}}(\infty;\underline{n})^0}$ stable. Moreover, if $z' = (x(\alpha_1\mathfrak{a};(\alpha_1\gamma_1)')_{/\mathbb{F}}, \cdots, x(\alpha_m\mathfrak{a};(\alpha_m\gamma_m)')_{/\mathbb{F}})$ with $\mathfrak{a}$ a proper $\mathfrak{o}_n$-ideal, then $\mathfrak{o}^\times_{n,(p,\ell)}$ fixes z'. We conclude that $\mathfrak{o}^\times_{n,(p,\ell)}$ acts as automorphisms of $\widetilde{Z}$ fixing z', and hence induces automorphisms of $\widetilde{Z}^{/z'}$ and $(Y^{(p,\ell)}(\infty)^0_{/\mathbb{F}})^{m/z'} = (Y^{(p,\ell)}(\infty)_{/\mathbb{F}})^{m/z'}$.

To show that this induces a p-adically continuous action of $\mathfrak{o}_p^\times$ on the above formal schemes, we need some preliminaries. In general, let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$ ideal in K, and let $x = x(\mathfrak{a};\gamma')_{/\mathbb{F}}$ be an admissible CM point on $Y^{(p,\ell)}(\infty)_{/\mathbb{F}}$. It therefore consists of (the isomorphism class of) an elliptic curve $E(\mathfrak{a})_{/\mathbb{F}}$ together with a $\Gamma^{(p,\ell)}(\infty)$-structure. For an element $c \in K^\times \subseteq K_{\mathbb{A},\mathrm{f}}^\times$, express it as $c = (c', i_p(c), i_\ell(c))$ with $c' \in K_{\mathbb{A},\mathrm{f}}^{(p,\ell)\times}$, $i_p(c) \in K_p^\times$ and $i_\ell(c) \in K_\ell^\times$ as in 2.4. The action of $\mathfrak{o}_n$ on $E(\mathfrak{a})_{/\mathbb{F}}$ naturally extends to the action of $\mathfrak{o}_n \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathfrak{o}_p$ on the p-divisible group $E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]$; and hence we have the action of $\mathfrak{o}_p^\times$ on the deformation space $\mathrm{Def}(E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]/\mathbb{F})$; cf. Chai and Oort [CO, 2.14, Remark]. On the other hand, when $c \in \mathfrak{o}^\times_{n,(p,\ell)}$, $\rho(c')$ fixes x and hence induces an automorphism of $(Y^{(p,\ell)}(\infty)_{/\mathbb{F}})^{/x}$.

Lemma (4.2.5) (cf. [CO, page 508]) *Let the notation be as above, and let c be an element of $\mathfrak{o}^\times_{n,(p,\ell)}$. Then via the canonical isomorphisms:*

$$\mathrm{Def}(E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]/\mathbb{F}) \overset{\text{Serre}-\text{Tate}}{\cong} \mathrm{Def}(E(\mathfrak{a})_{/\mathbb{F}}/\mathbb{F}) \cong (Y^{(p,\ell)}(\infty)_{/\mathbb{F}})^{/x},$$

the action of $i_p(c)$ on the left hand side and the action of $\rho(c')^{-1}$ on the right hand side commute.

Proof See the proof of the "local stabilizer principle" given there. □

Let $E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]_{\text{ét}}$ (resp. $E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]_{\mathrm{mult}}$) be the maximal étale quotient (resp. the multiplicative part) of the p-divisible group $E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]$. We recall that there is a canonical isomorphism:

(4.2.6)
$$(Y^{(p,\ell)}(\infty)_{/\mathbb{F}})^{/x} \cong \underline{\mathrm{Hom}}_{\mathbb{Z}_p}(T_p(E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]_{\text{ét}}) \otimes_{\mathbb{Z}_p} X_*(E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]_{\mathrm{mult}})^\vee, \widehat{\mathbb{G}}_m)$$

where X_* (resp. $\vee$) means the cocharacter group (resp. the $\mathbb{Z}_p$-dual); cf. [CO, Theorem 2.19]. The action of $i_p(c)$ on the cocharacter group of this formal torus, i.e. $(T_p(E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]_{\text{ét}})^\vee \otimes_{\mathbb{Z}_p} X_*(E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]_{\text{mult}})$, is then given by the non-trivial character $c \mapsto c/c^*$, where $*$ denotes the nontrivial automorphism of $K/\mathbb{Q}$, if we embed K into $\mathbb{Q}_p$ via its action on $X_*(E(\mathfrak{a})_{/\mathbb{F}}[p^\infty]_{\text{mult}}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Proof of (4.2.2) We return to the situation after (4.2.3), and use the notation there. In view of the commutative diagram (4.2.4), it is enough to show that $\widetilde{Z}^{/z'}$ is a formal subtorus of the Serre-Tate formal torus $(Y^{(p,\ell)}(\infty)_{/\mathbb{F}})^{m/z'}$.

We can embed $\mathfrak{o}_p^\times$ into the product $\prod_{i=1}^m \mathrm{Aut}(E(\alpha_i\mathfrak{a})_{/\mathbb{F}}[p^\infty])$ diagonally, and hence we may let this group act on $(Y^{(p,\ell)}(\infty)_{/\mathbb{F}})^{m/z'}$ ($z' = (\cdots, x(\alpha_i\mathfrak{a}; (\alpha_i\gamma_i)')_{/\mathbb{F}}, \cdots)$ as in (4.2.1)). This action is continuous on the (discrete) set $Y^{(p,\ell)}(\infty)_{/\mathbb{F}})^{m/z'}(R)$ for each artinian local $\mathbb{F}$-algebra R.

On the other hand, we have seen that, via $c \mapsto \rho(c')$, $\mathfrak{o}_{n,(p,\ell)}^\times$ acts on $\widetilde{Z}^{/z'}$. We see from this and (4.2.5) that $\widetilde{Z}^{/z'}$ is stable under the action of $\mathfrak{o}_p^\times$. With this, together with the remark made above, we can apply Chai's rigidity theorem [C1, Theorem 6.6] to conclude that $\widetilde{Z}^{/z'}$ is a formal subtorus of $(Y^{(p,\ell)}(\infty)_{/\mathbb{F}})^{m/z'}$. □

We now prove (2.3.4). First recall that $Z \subset (Y(N_0)^0_{/\mathbb{F}})^m$ is obtained from $Z_0 \subset (Y(N_0)^0_{/k_0})^m$ defined over a finite subfield k_0 of $\mathbb{F}$ by base extension. Let $p_i : (Y(N_0)^0_{/k_0})^m \to Y(N_0)^0_{/k_0}$ be the projection to the i-th direct factor ($1 \le i \le m$):

$$Z_0 \hookrightarrow (Y(N_0)^0_{/k_0})^m \xrightarrow{p_i} Y(N_0)^0_{/k_0}. \tag{4.2.7}$$

Take an ordinary and smooth closed point x of Z_0, and let $x_i = p_i(x)$. We have the morphisms of formal schemes over k_0:

$$Z_0^{/x} \hookrightarrow (Y(N_0)^0_{/k_0})^{m/x} \cong (Y(N_0)^0_{/k_0})^{/x_1} \times_{k_0} \cdots \times_{k_0} (Y(N_0)^0_{/k_0})^{/x_m} \xrightarrow{p_i} (Y(N_0)^0_{/k_0})^{/x_i}.$$

Here, by (4.2.2), $Z_0^{/x}$ is a formal subtorus of the Serre-Tate formal torus $(Y(N_0)^0_{/k_0})^{m/x}$ defined over $k(x)$, the residue field at x. Therefore, if we denote by $\mathcal{E}_{/x_i}$ the fibre at x_i of the universal elliptic curve on $Y(N_0)^0_{/k_0}$, we obtain a non-trivial homomorphism of cocharacter groups

$$X_*(Z_0^{/x}) \to X_*((Y(N_0)^0_{/k_0})^{/x_i}) \cong \\ \underline{\mathrm{Hom}}_{\mathbb{Z}_p}(T_p(\mathcal{E}_{/x_i}[p^\infty]_{\text{ét}}) \otimes_{\mathbb{Z}_p} X_*(\mathcal{E}_{/x_i}[p^\infty]_{\text{mult}})^\vee, \widehat{\mathbb{G}}_m)$$

which commutes with the natural action of $\mathrm{Gal}(\mathbb{F}/k(x))$. If we denote by $\mathrm{Fr}_x \in \mathrm{Gal}(\mathbb{F}/k(x))$ the Frobenius automorphism, the eigenvalue of Fr_x acting on $T_p(\mathcal{E}_{/x_i}[p^\infty]_{\text{ét}})$ is the unit root $\alpha(E_{Z_0,i,/x})$ of the Frobenius endomorphism considered in (3.6.5); and hence $\alpha(E_{Z_0,i,/x})^{-2}$ appears as an eigenvalue of Fr_x acting on $X_*(Z_0^{/x}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ ($1 \le i \le m$). But we have seen in (3.6.5) that we can choose x in such a way that $\alpha(E_{Z_0,i,/x})^{-2}$ ($1 \le i \le m$) are all different. We conclude that $\dim X_*(Z_0^{/x}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = m$, which in turn implies that

$\dim \widehat{\mathcal{O}}_{Z_0,x} = \dim \mathcal{O}_{Z_0,x} = m$. This means that $\dim Z_0 = m$, contradicting our starting hypothesis that $\dim Z = m - 1$. This completes the proof of Theorem (2.3.4).

Appendix: Some properties of projective limits of schemes. In this appendix, we give elementary topological properties of projective limits of schemes. As for general treatment of projective limits of schemes, see [EGA IV, §8].

A.1. Zariski closures. Throughout, we work under the following situation: We let $(X_\alpha, f_{\alpha,\beta})$ be a projective system of schemes having a directed set I as the index set. Thus $f_{\alpha,\beta} : X_\beta \to X_\alpha$ for $\alpha, \beta \in I$ with $\alpha \leq \beta$. We assume:

$$(A.1.1) \qquad \begin{cases} f_{\alpha,\beta} \text{ is finite and surjective for each pair } \alpha \leq \beta \text{ in } I; \\ I \text{ has a minimum element } \alpha_0. \end{cases}$$

Thus all X_α are X_{α_0}-schemes, and the conditions in [EGA IV, (8.2.2)] are satisfied. Especially the projective limit

$$X := \varprojlim_{\alpha \in I} X_\alpha$$

in the category of schemes exists [EGA IV, (8.2.3)]; and as (underlying) topological spaces, X is also the projective limit of X_α [EGA IV, (8.2.9)]. Let

$$f_\alpha : X \to X_\alpha$$

be the natural morphism. This is surjective by [EGA IV, (8.3.8), (i)]; and it also follows from the argument of (A.1.2) below.

Lemma (A.1.2) *For each $\alpha \in I$, f_α is a closed morphism.*

Proof Let A be a non-empty closed subset of X, and set $A_\alpha := f_\alpha(A)$. We have $A = \varprojlim_{\alpha \in I} \overline{A_\alpha}$ (cf. Bourbaki [B, Chapitre 1, §4, n°4, Corollaire]). Fix $\alpha \in I$ and take a point $a \in \overline{A_\alpha}$. We see from (A.1.1) that $f_{\alpha,\beta}(\overline{A_\beta}) = \overline{A_\alpha}$ for all $\beta \geq \alpha$. Therefore $S_\beta := \{b \in \overline{A_\beta} \mid f_{\alpha,\beta}(b) = a\}$ is a non-empty finite subset of $\overline{A_\beta}$. Therefore $A \supseteq \varprojlim_{\beta \geq \alpha} S_\beta \neq \phi$. It follows that $f_\alpha(A) \ni a$, and we have $f_\alpha(A) = \overline{A_\alpha}$. □

We also note that if all $f_{\alpha,\beta}$ are flat, then f_α are also flat; and in this case, $f_{\alpha,\beta}$ and f_α are open morphisms as well.

Proposition (A.1.3) *Let A be a subset of X and set $A_\alpha = f_\alpha(A)$ for each $\alpha \in I$. Then A is Zariski dense in X if and only if A_α is Zariski dense in X_α for every $\alpha \in I$.*

Proof We have $f_\alpha(\overline{A}) \subseteq \overline{f_\alpha(A)} = \overline{A_\alpha}$ in general. If $\overline{A} = X$, then we have $\overline{A_\alpha} = f_\alpha(X) = X_\alpha$.

Conversely, assume that $\overline{A_\alpha} = X_\alpha$ for all $\alpha \in I$. Then we have $\overline{A} = \varprojlim_{\alpha \in I} \overline{A_\alpha} = \varprojlim_{\alpha \in I} X_\alpha = X$ by [B, loc. cit.]. □

Proposition (A.1.4) *Let the notation be as in* (A.1.3). *Assume that* $(X_\alpha, f_{\alpha,\beta})$ *is a projective system of schemes of finite type over a field, and moreover assume that all* X_α *are irreducible. Then* A *is Zariski dense in* X *if and only if* A_{α_0} *is Zariski dense in* X_{α_0}. *Also, a subset* B *of* X_β *is Zariski dense if and only if* $f_{\alpha_0,\beta}(B)$ *is Zariski dense in* X_{α_0}.

Proof We only give a proof for the first assertion, since the same argument settles the second.

The "only if" part is clear.

Assume that A_{α_0} is Zariski dense in X_{α_0}. For $\beta \in I$, $f_{\beta,\alpha_0} : X_\beta \to X_{\alpha_0}$ and also the induced $\overline{A_\beta} \to \overline{A_{\alpha_0}}$ are finite and surjective. It follows that $\dim(\overline{A_\beta}) = \dim(X_\beta)$. Irreducibility of X_β then implies that $\overline{A_\beta} = X_\beta$, and hence A is Zariski dense in X by (A.1.3). $\square$

Corollary (A.1.5) *Under the same situation as in* (A.1.4), A *is Zariski dense in* X *if and only if* $f_{\alpha_0}^{-1}(A_{\alpha_0})$ *is Zariski dense in* X.

A.2. Irreducible components. For a topological space T, let $\mathrm{Irr}(T)$ be the set of irreducible components of T.

Proposition (A.2.1) *Let* $(X_\alpha, f_{\alpha,\beta})$ *satisfy* (A.1.1) *and let* X *and* f_α *be defined as before. Assume in addition that* $f_{\alpha,\beta}$ *are flat for all* $\alpha \leq \beta$ *in* I. *Then we have a natural bijection:*

$$\mathrm{Irr}(X) \xrightarrow{\sim} \varprojlim_{\alpha \in I} \mathrm{Irr}(X_\alpha).$$

Proof In general, if $g : S \to T$ is a faithfully flat closed morphism of schemes, it induces a surjection $\mathrm{Irr}(S) \twoheadrightarrow \mathrm{Irr}(T)$. Indeed, if C is an irreducible component of S, $g(C)$ belongs to $\mathrm{Irr}(T)$ by the closedness of g and [EGA IV, (2.3.5), (ii)]. On the other hand, take an irreducible component of T, and let t be its generic point. Then there is an $s \in S$ such that $g(s) = t$; and hence $g(\overline{\{s\}}) = \overline{\{t\}}$. If $\overline{\{s\}}$ is not an irreducible component, there is an irreducible component containing $\overline{\{s\}}$. Let s' be its generic point. Then we must have $g(\overline{\{s'\}}) = \overline{\{t\}}$. This shows the surjectivity of the above map.

Now the morphisms $f_{\alpha,\beta}$ and f_α are faithfully flat and closed by (A.1.2). Thus each f_α induces a surjection $\mathrm{Irr}(X) \twoheadrightarrow \mathrm{Irr}(X_\alpha)$ from which we obtain $\widetilde{f} : \mathrm{Irr}(X) \to \varprojlim_{\alpha \in I} \mathrm{Irr}(X_\alpha)$. This map is injective: If $\overline{\{x\}}$ and $\overline{\{x'\}}$ are different elements of $\mathrm{Irr}(X)$, then clearly there is an index $\alpha \in I$ such that $f_\alpha(x) \neq f_\alpha(x')$ and hence $\overline{\{f_\alpha(x)\}}$ and $\overline{\{f_\alpha(x')\}}$ are different elements of $\mathrm{Irr}(X_\alpha)$. Finally let us show the surjectivity of $\widetilde{f}$: Let $(\overline{\{x_\alpha\}})_{\alpha \in I}$ be an element of $\varprojlim_{\alpha \in I} \mathrm{Irr}(X_\alpha)$. Since $f_{\alpha,\beta}$ maps $\overline{\{x_\beta\}}$ surjectively onto $\overline{\{x_\alpha\}}$ for each $\alpha \leq \beta$ in I, it must preserve generic points: $f_{\alpha,\beta}(x_\beta) = x_\alpha$. Therefore the element $x = (x_\alpha)_{\alpha \in I}$ belongs to $\varprojlim_{\alpha \in I} X_\alpha = X$, and we have $f_\alpha(\overline{\{x\}}) = \overline{\{x_\alpha\}}$ for each $\alpha \in I$. If $\overline{\{x\}}$ were not an element of $\mathrm{Irr}(X)$, we can take a generalization x' of x, as in the first step

of this proof, satisfying $\overline{\{x'\}} \in \mathrm{Irr}(X)$ and $f_\alpha(\overline{\{x'\}}) = \overline{\{x_\alpha\}}$ for all $\alpha \in I$. This completes the proof. $\square$

References

[B] N. Bourbaki, Éléments de mathématique, Topologie générale, Chapitres 1 et 2, Hermann, 1965.

[C1] C.-L. Chai, Families of ordinary abelian varieties: canonical coordinates, p-adic monodromy, Tate-linear subvarieties and Hecke otbits, preprint, 2003.

[C2] C.-L. Chai, A rigidity result for p-divisible formal groups, Asian J. Math., **12** (2008), 193-202.

[CO] C.-L. Chai and F. Oort, Moduli of abelian varieties and p-divisible groups, In: Arithmetic Geometry, Clay Mathematics Proceedings **8** (2009), 439-534.

[D1] P. Deligne, Variétés abéliennes ordinaires sur un corps fini, Invent. Math., **8** (1969), 238-243.

[D2] P. Deligne, Formes modulaires et représentation l-adiques, Sém. Bourbaki, exp. 355, In: Lecture Notes in Math., **179**, Springer, 1971, 139-172.

[DR] P. Deligne and M. Rapoport, Les shémas de modules de courbes elliptiques, In: Modular functions of one variable II, Lecture Notes in Math., **349**, Springer, 1973, 143-316.

[EGA IV] A. Grothendieck, Éléments de géométrie algébrique IV, rédigés avec la collaboration de J. Dieudonné, Publ. Math. IHES, **24** (Seconde Partie) (1965), **28** (Troisième Partie) (1966).

[SGA 1] A. Grothendieck, Revêtements étales et groupe fondamental (SGA 1), Séminaire de géométrie algébrique du Bois Marie 1960-1961, Documents Math. 3, Soc. Math. Fr., 2003.

[H1] H. Hida, Non-vanishing modulo p of Hecke L-values, In: Geometric Aspects of Dwork Theory, ed. by A. Adolphson, F. Baldssarri, P. Berthlot, N. Katz, F. Loeser, Walter de Gruyter, 2004, 735-784.

[H2] H. Hida, Non-vanishing modulo p of Hecke L-values and application, In: L-functions and Galois Representations, London Math. Soc. Lecture Note Ser., **320**, Cambridge Univ. Press, 2007, 207-269.

[H3] H. Hida, Elliptic curves and arithmetic invariants, Springer Monographs in Mathematics, 2013.

[H4] H. Hida, Non-vanishing of integrals of a mod p modular form, to appear in the review volume of the 2022 ICTS conference: "Elliptic curves and special values of L-functions", World Scientific.

[I] J. Igusa, Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves, Amer. J. Math., **81** (1959), 453-476.

[KM] N. Katz and B. Mazur, Arithmetic moduli of elliptic curves, Ann. of Math. Stud., **108**, Princeton Univ. Press, 1985.

[M] W. Messing, The crystals associated to Barsotti-Tate groups: with applications to abelian schemes, Lecture Notes in Math., **264**, Springer, 1972.

[O] M. Ohta, μ-type subgroups of $J_1(N)$ and application to cyclotomic fields, J. Math. Soc. Japan, **72** (2020), 333-412.

[R] K.A. Ribet, On ℓ-adic representations attached to modular forms, Invent. Math., **28** (1975), 245–275.

[Se1] J.-P. Serre, Zeta and L functions, In: Arithmetical Algebraic Geometry, Harper and Row, 1965, 82-92, (Œuvres II, No. 64).

[Se2] J.-P. Serre, Abelian l-adic representations and elliptic curves, Benjamin, 1968.

[Se3] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math., **15** (1972), 259-331, (Œuvres III, No. 94).

[ST] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. Math., **88** (1968), 492-517.

[Sh] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, **11**, Iwanami Shoten and Princeton Univ. Press, 1971.

[V] V. Vatsal, Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves, J. Inst. Math. Jussieu, **4** (2005), 281-316.

[W] A. Weil, Basic number theory, Grundl. Math. Wiss., **144**, Springer-Verlag (1967).

[Z] Ju. G. Zarhin, Endomorphisms of abelian varieties over fields of finite characteristic, Math. USSR Izvestija, **9** (1975), No. 2, 255-260.

Masami Ohta
Professor Emeritus
Tokai University
Hiratsuka, Kanagawa, 259-1292, Japan
E-mail: rm010354-5984@tbz.t-com.ne.jp