National Center for Theoretical Sciences

NCTS/Math
Technical Report
2017-005

On Arithmetic of the Superspecial Locus

CHIA-FU YU

ON ARITHMETIC OF THE SUPERSPECIAL LOCUS

CHIA-FU YU

ABSTRACT. We develop a method for describing the Galois action on the superspecial locus of the Siegel moduli space in characteristic p. Using this description, we give a modern treatment for the results of Ibukiyama and Katsura [Compos. Math., 1994] concerning the $\mathbb{F}_p$-rational points and the trace of a Hecke operator of Atkin-Lehner type. This also leads to analogues with level-N structure. The trace of the Hecke operator can be reduced into one term (instead of finitely many terms a priori) by the simple trace formula when N is large.

1. INTRODUCTION

Throughout this paper p denotes a rational prime number. An abelian variety A over a field of characteristic p is said to be *superspecial* if it is isomorphic to a product of supersingular elliptic curves over an algebraic closure of the ground field. It is known that every supersingular elliptic curve E over any algebraically closed field k has a model defined over $\mathbb{F}_{p^2}$ (see Deuring [2]); this means that there exists an elliptic curve E' over $\mathbb{F}_{p^2}$ and there exists an isomorphism $E \simeq E' \otimes_{\mathbb{F}_{p^2}} k$ over k; the elliptic curve E' is called a model of (the isomorphism class of) E over $\mathbb{F}_{p^2}$. For any $g > 1$, there is only one isomorphism class of g-dimensional superspecial abelian varieties over k (due to Deligne, Shioda and Ogus, also see [21, Section 1.6, p. 13]). Particularly every superspecial abelian variety of dimension greater than one over k has a model defined over $\mathbb{F}_p$. In [12] Ibukiyama and Katsura studied the fields of definition of superspecial *polarized* abelian varieties. They showed that every superspecial principally polarized abelian variety over $\overline{\mathbb{F}}_p$ has a model defined over $\mathbb{F}_{p^2}$. They also expressed the number of those which have a model defined over $\mathbb{F}_p$ in terms of the class number and the type number of the quaternion unitary algebraic group in question; see Theorems 1.2 and 1.3 for more details.

Let $\mathcal{A}_g$ denote the moduli space over $\mathbb{F}_p$ of g-dimensional principally polarized abelian varieties. Let $\Lambda_g \subset \mathcal{A}_g(\overline{\mathbb{F}}_p)$ be the subset consisting of superspecial points, called the superspecial locus of $\mathcal{A}_g \otimes \overline{\mathbb{F}}_p$. This is a finite and closed subset that is stable under the action of Galois group $\mathcal{G} := \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ (Corollary 3.2). The unique $\mathbb{F}_p$-model of Λ_g, called the superspecial locus of $\mathcal{A}_g$, is denoted by $\mathbf{\Lambda}_g$; one has $\Lambda_g = \mathbf{\Lambda}_g(\overline{\mathbb{F}}_p)$.

The goal of this paper is to develop a method for describing the Galois action on Λ_g. One can regard this as a reciprocity law, which in some broad sense describes the Galois action on a class space of adelic points in terms of Hecke translations. For

---

Date: March 23, 2017.

2000 *Mathematics Subject Classification.* 14K10, 11E41, 11G18.

Key words and phrases. Superspecial abelian variety; explicit reciprocity law; class number; trace formula.

CM fields, the Shimura-Taniyama reciprocity law describes explicitly the action of the Galois group $\mathrm{Gal}(\overline{K'}/K')$ on the spaces of abelian varieties of CM type (K,Φ), where K' is the reflex field of the CM pair (K,Φ). This is known as the main theorem of complex multiplication [31]. For the field of rational numbers, the action of the Galois group $\mathcal{G}_{\mathbb{Q}}=\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the group of torsion points of the multiplicative group $\mathbb{G}_{\mathrm{m}}$ over $\mathbb{Q}$ gives rise to the cyclotomic character $\omega:\mathcal{G}_{\mathbb{Q}}\to\hat{\mathbb{Z}}^{\times}$, which factors through the isomorphism $\omega:\mathcal{G}_{\mathbb{Q}}^{\mathrm{ab}}\simeq\hat{\mathbb{Z}}^{\times}$. By the isomorphism $\mathbb{R}_{>0}\mathbb{Q}^{\times}\backslash\mathbb{A}_{\mathbb{Q}}^{\times}\simeq\hat{\mathbb{Z}}^{\times}$ and composing with the inverse map ω^{-1} of ω, we get a map $\mathrm{rec}_{\mathbb{Q}}:\mathbb{Q}^{\times}\backslash\mathbb{A}_{\mathbb{Q}}^{\times}\to\mathcal{G}_{\mathbb{Q}}^{\mathrm{ab}}$, which is the Artin reciprocity map. The Artin reciprocity map classifies all abelian extensions of $\mathbb{Q}$ and gives the explicit description of its maximal abelian extension, known as the Kronecker-Weber theorem (cf. [20, Part II]).

Let (A_0,λ_0) be a superspecial principally polarized abelian variety over $\mathbb{F}_p$, considered as the base point in Λ_g via the base change $(A_0,\lambda_0)\otimes\overline{\mathbb{F}}_p=:(\overline{A}_0,\overline{\lambda}_0)$. To (A_0,λ_0) we associate two group schemes $G_1\subset G$ over $\mathrm{Spec}\,\mathbb{Z}$ as follows. For any commutative ring R, the groups of their R-valued points are defined as

$$\begin{aligned} G(R)&:=\{x\in(\mathrm{End}(\overline{A}_0)\otimes R)^{\times}\mid x'x\in R^{\times}\},\\ G_1(R)&:=\{x\in(\mathrm{End}(\overline{A}_0)\otimes R)^{\times}\mid x'x=1\}, \end{aligned}\tag{1.1}$$

where the map $x\mapsto x'$ is the Rosati involution induced by the polarization λ_0. For convenience, we often also write G_1 and G for their generic fibers $G_{1,\mathbb{Q}}$ and $G_{\mathbb{Q}}$, respectively. As a well-known fact (cf. [13], [4], [35, Theorem 10.5], or [39, Theorem 2.2]), there is a natural parametrization of Λ_g by the following double coset spaces

$$\mathbf{d}:G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\hat{\mathbb{Z}})=G_1(\mathbb{Q})\backslash G_1(\mathbb{A}_f)/G_1(\hat{\mathbb{Z}})\simeq\Lambda_g\tag{1.2}$$

for which the base point (A_0,λ_0) corresponds to the identity class [1], where $\hat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$ and $\mathbb{A}_f=\hat{\mathbb{Z}}\otimes\mathbb{Q}$ is the finite adele ring of $\mathbb{Q}$. As the abelian variety A_0 is defined over $\mathbb{F}_p$, the Galois group $\mathcal{G}$ acts naturally acts on the adelic group $G(\mathbb{A}_f)$. We denote the (arithmetic) Frobenius automorphism in $\mathcal{G}$ by σ_p; one has $\sigma_p(x)=x^p$ for $x\in\overline{\mathbb{F}}_p$.

Theorem 1.1.

(1) *The action of $\mathcal{G}$ on $G(\mathbb{A}_f)$ is given by*

$$\sigma_p(x_\ell)_\ell=(\pi_0x_\ell\pi_0^{-1})_\ell,\quad (x_\ell)_\ell\in G(\mathbb{A}_f),\tag{1.3}$$

where $\pi_0\in G(\mathbb{Q})$ is the Frobenius endomorphism of A_0 over $\mathbb{F}_p$.

(2) *The natural map $\widetilde{\mathbf{d}}:G(\mathbb{A}_f)\to\Lambda_g$ induced by (1.2) is $\mathcal{G}$-equivariant.*

We now explain the main results of Ibukiyama and Katsura in [12]. We can select the base point (A_0,λ_0) over $\mathbb{F}_p$ such that the Frobenius endomorphism $\pi_0\in\mathrm{End}(A_0)$ satisfies $\pi_0^2=-p$. The existence of (A_0,λ_0) is known due to Deuring (cf. [12]); this also follows from the Honda-Tate theory [32]. Put $U:=G(\hat{\mathbb{Z}})$ and $U(\pi_0):=U\pi_0=\pi_0U$.

Theorem 1.2. ([12, Theorem 1])

(1) *Every member $(A,\lambda)\in\Lambda_g$ has a model defined over $\mathbb{F}_{p^2}$.*

(2) *A member $(A,\lambda)\in\Lambda_g$ admits a model defined over $\mathbb{F}_p$ if and only if*

$$G(\mathbb{Q})\cap xU(\pi_0)x^{-1}\neq\emptyset,\tag{1.4}$$

where $x \in G(\mathbb{A}_f)$ is any representative of the class $[x] \in G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U$ corresponding to (A, λ).

The second part of the work of Ibukiyama and Katsura concerns the trace of a Hecke operator of Atkin-Lehner type on the space of automorphic forms on the group G. Denote by $M_0(U)$ the vector space of all functions $f : G(\mathbb{A}_f) \to \mathbb{C}$ that satisfy $f(axu) = f(x)$ for all $a \in G(\mathbb{Q})$ and $u \in U$. Let $\mathcal{H}(G, U)$ denote the convolution algebra of bi-U-invariant functions h on $G(\mathbb{A}_f)$ with compact support, called the Hecke algebra. The Hecke algebra $\mathcal{H}(G, U)$ acts naturally on the space $M_0(U)$ by the following rule:

$$h * f(x) = \int_{G(\mathbb{A}_f)} h(y)f(xy)dy, \quad \text{for } h \in \mathcal{H}(G, U),\ f \in M_0(U), \tag{1.5}$$

where the Haar measure on $G(\mathbb{A}_f)$ is normalized with volume one on U. Explicitly, if we write the double coset UyU, where y is an element in $G(\mathbb{A}_f)$, into $\coprod_{i=1}^n y_i U$, and let $\mathbf{1}_{UyU}$ denote the characteristic function of UyU, then one has

$$\mathbf{1}_{UyU} * f(x) = \sum_{i=1}^{n} f(xy_i). \tag{1.6}$$

Let $R(\pi_0)$ be the operator induced from the characteristic function $\mathbf{1}_{U(\pi_0)}$. Let $\mathcal{T}(G)$ denote the set of $G(\mathbb{Q})$-conjugacy classes of maximal orders in the central simple algebra $\mathrm{End}^0(A_0 \otimes \overline{\mathbb{F}}_p) = \mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Q}$ which are $G(\mathbb{A}_f)$-conjugate to the maximal order $\mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p)$. We can write

$$\mathcal{T}(G) = G(\mathbb{Q})\backslash G(\mathbb{A}_f)/\mathfrak{N},$$

where $\mathfrak{N}$ is the open subgroup of $G(\mathbb{A}_f)$ that normalizes the ring $\mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \hat{\mathbb{Z}}$. The cardinality T of $\mathcal{T}(G)$ is called the type number of the group G, following Ibukiyama-Katsura [12]. In the case $g = 1$, the group G is equal to the multiplicative group of the quaternion $\mathbb{Q}$-algebra $B_{p,\infty}$ ramified exactly at $\{\infty, p\}$, and this agrees with the usual definition of the type number, namely the number of conjugacy classes of maximal orders in $B_{p,\infty}$.

Theorem 1.3. ([12, Theorem 2])

1. *The number of members (A, λ) in Λ_g that have a model defined over $\mathbb{F}_p$ is equal to* $\mathrm{tr}\, R(\pi_0)$.
2. *We have* $\mathrm{tr}\, R(\pi_0) = 2T - H$, *where H is the class number of G (for the level group U).*

Remark that the case $g = 1$ of Theorems 1.2 and 1.3 is due to Deuring, and the case $g > 1$ is proved in [12].

As the main application of Theorem 1.1, we give somehow simpler proofs of Theorems 1.2 and 1.3 (1). We also include an exposition of the proof of Theorem 1.3 (2) but in the language of adeles. As a byproduct, we obtain the following result, which is implicit in the proof of [12, Theorem 2]. By Theorem 1.1, the action of the Galois group $\mathcal{G}$ on Λ_g factors through the quotient group $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. Let $\mathbf{\Lambda}_g^0$ be the set of closed points of the finite $\mathbb{F}_p$-scheme $\mathbf{\Lambda}_g$; this is the set of Galois orbits of Λ_g, and can be also identified with the set of connected components of $\mathbf{\Lambda}_g$.

Theorem 1.4 (Theorem 5.9). *The composition $\Lambda_g \simeq G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U \overset{\mathrm{pr}}{\to} \mathcal{T}(G)$, where* pr *is the natural projection, induces a bijection between the set of* $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$*-orbits of Λ_g and the set $\mathcal{T}(G)$ of G-types. In other words, there is a natural bijection between the set $\mathbf{\Lambda}_g^0$ of closed points of $\mathbf{\Lambda}_g$ and the set $\mathcal{T}(G)$.*

In some sense we have the following equality in the "arithmetic side"

$$\mathrm{tr}\, R(\pi_0) = 2T - H \tag{1.7}$$

and its mirror in the geometric side

$$|\mathbf{\Lambda}_g(\mathbb{F}_p)| = 2|\mathbf{\Lambda}_g^0| - |\Lambda_g| \tag{1.8}$$

where $\mathbf{\Lambda}_g(\mathbb{F}_p) \subset \Lambda_g$ is the subset of $\mathbb{F}_p$-rational points. Moreover, this is the term-by-term equality; see Theorems 1.3 and 1.4.

The explicit computation of the class number H is extremely difficult; see [9] for the case $g = 2$. However, if we add a prime-to-p level structure to the superspecial locus and form a cover $\Lambda_{g,1,N}$ of Λ_g, then one can compute the cardinality $|\Lambda_{g,1,N}|$ rather easily using the mass formula:

(1.9)
$$|\Lambda_{g,1,N}| = |\,\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})| \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{k=1}^{g} \zeta(1-2k) \right\} \cdot \prod_{k=1}^{g} \left\{ (p^k + (-1)^k \right\},$$

where $\zeta(s)$ is the Riemann zeta function. See Ekedahl [4, p.159] and Hashimoto-Ibukiyama [9, Proposition 9], also cf. [38, Section 3]. This leads us to examine whether the analogous statements for (1.7) and (1.8) can be extended to the objects with prime-to-p level structures, and whether all the terms can be computed explicitly. This is the content of the second part of this paper.

We first describe the Galois action on the superspecial locus with a (usual) prime-to-p level structure. Let N be a prime-to-p positive integer. Let $\mathcal{A}_{g,1,N}$ denote the moduli space over $\mathbb{F}_p$ of g-dimensional principally polarized abelian varieties with a (full) symplectic level-N structure; see Section 6.4 for details. Let $\widetilde{\mathcal{A}}_g^{(p)} := (\mathcal{A}_{g,1,N})_{p\nmid N}$ be the tower of Siegel modular varieties with prime-to-p level structures. Let $\widetilde{\Lambda}_g \subset \widetilde{\mathcal{A}}_g^{(p)} \otimes \overline{\mathbb{F}}_p$ be the superspecial locus, which is the tower of superspecial loci $\Lambda_{g,1,N} \subset \mathcal{A}_{g,1,N} \otimes \overline{\mathbb{F}}_p$ for all prime-to-p positive integers N; $\widetilde{\Lambda}_g$ is a profinite set together with a $\mathcal{G}$-action. Let $T^{(p)}(A_0) := \prod_{\ell \neq p} T_\ell(A_0)$ be the prime-to-p Tate module of A_0; it is equipped with an action of $\mathcal{G}$ so that we have a Galois representation

$$\rho : \mathcal{G} \to G(\hat{\mathbb{Z}}^{(p)}) \subset G(\mathbb{A}_f^p),$$

where $\hat{\mathbb{Z}}^{(p)} := \prod_{\ell \neq p} \mathbb{Z}_\ell$ and $\mathbb{A}_f^p := \hat{\mathbb{Z}}^{(p)} \otimes \mathbb{Q}$ is the prime-to-p finite adele ring of $\mathbb{Q}$. We fix a point $(A_0, \lambda_0, \widetilde{\alpha}_0) \in \widetilde{\Lambda}_g$ over (A_0, λ_0), where $\widetilde{\alpha}_0 : (\hat{\mathbb{Z}}^{(p)})^{2g} \simeq T^{(p)}(A_0)$ is a trivialization which preserves the pairings up to an element in $(\hat{\mathbb{Z}}^{(p)})^\times$. The trivialization $\widetilde{\alpha}_0$ induces an isomorphism

$$i_0 : G(\mathbb{A}_f^p) \simeq \mathrm{GSp}_{2g}(\mathbb{A}_f^p),$$

and a Galois representation

$$\rho_0 = i_0 \circ \rho : \mathcal{G} \to \mathrm{GSp}_{2g}(\mathbb{A}_f^p).$$

Let $\mathcal{G}$ act on $\mathrm{GSp}_{2g}(\mathbb{A}_f^p)$ by the action ρ_0:

$$\sigma \cdot x = \rho_0(\sigma)x, \quad \forall\, \sigma \in \mathcal{G},\ x \in \mathrm{GSp}_{2g}(\mathbb{A}_f^p). \tag{1.10}$$

Proposition 1.5. *There is an isomorphism (depending on the choice of $\widetilde{\alpha}_0$)*

$$\mathbf{b}_0^p : \widetilde{\Lambda}_g \simeq i_0(G(\mathbb{Z}_{(p)}))\backslash \mathrm{GSp}_{2g}(\mathbb{A}_f^p)$$

which is compatible with the right $\mathrm{GSp}_{2g}(\mathbb{A}_f^p)$*-action and the (left)* $\mathcal{G}$*-action.*

The action of the Galois group $\mathcal{G}$ on the finite subset $\Lambda_{g,1,N}$ somehow contains a twist which comes from the trivialization between $A_0[N]$ and $(\mathbb{Z}/N\mathbb{Z})^{2g}$. This forces the subset $\mathbf{\Lambda}_{g,1,N}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points to be *empty* when N is large. As a result, the analogous result for $\Lambda_{g,1,N}$ as in (1.8) (the geometric side) is false. However, the formulation of (1.7) (the arithmetic side) extends well without any modification. To correct the identity (1.8) for higher level, we introduce a new level-N structure for members in Λ_g which relies on the base point (A_0, λ_0). This yields a cover $\Lambda^*_{g,N}$ of Λ_g for which the Galois action becomes well-behaved. As a result, Theorems 1.2, 1.3 and 1.4 can be generalized without any difficulty from the present approach; see Theorem 6.6. Note that the sets $\Lambda^*_{g,N}$ and $\Lambda_{g,1,N}$ are isomorphic as Hecke sets but they have different Galois actions.

We use the simple trace formula to compute the trace of the Hecke operator $R(\pi_0)$. Our final result says that when N is sufficiently large, $\mathrm{tr}\, R(\pi_0)$ is reduced to the product of the mass of the centralizer G_{π_0} of π_0 and a standard orbital integral; see Theorem 8.9 for details. We remark that one can calculate the mass of G_{π_0} explicitly using the methods of G. Prasad [25] or of Shimura [30], and that the orbital integral is of purely local nature. Note that we had an explicit formula for the class number $H_N = |\Lambda_{g,1,N}|$ (1.9) due to Ekedahl and others; knowing one of $\mathrm{tr}\, R(\pi_0)$ and the type number would know the other.

The method of the present paper works for more general Shimura varieties. One can apply it to describe the Galois action on the *minimal basic locus* (also called the superspecial locus in [33]) in the reduction mod p of a PEL-type Shimura variety. See [18] and [27] for precise definitions of these moduli spaces and basic abelian varieties. We call a basic polarized abelian variety (A, λ, ι) with an O_B-action (for an order O_B in a semi-simple $\mathbb{Q}$-algebra B) *minimal* if $\mathrm{End}_{O_B}(A) \otimes_{\mathbb{Z}_p}$ is a maximal order. These are natural generalizations of superspecial abelian varieties. The existence of basic points is known due to many people in many cases (see [32], [36], [5], [22], [37], [33]). The existence of minimal basic points can be deduced using the method in [40, Theorem 1.3]. The parametrization of the minimal basic locus by double coset spaces (similar to (1.2)) is also available; see [39, Theorems 2.2 and 4.6]. For describing the Galois action, our study indicates that a good base point in the minimal basic locus plays a crucial role in the general theory.

There has been a theory of modular forms mod p initiated by Serre [29] and more generally on algebraic modular forms developed by Gross [8] where the superspecial locus plays an important role. Under the framework of Gross' theory, Ghitza [7] proved the Jacquet-Langlands correspondence (JLC) modulo p between modular forms on GSp_{2g} and algebraic modular forms on its compact inner form "twisted at p and ∞". He obtained this by restricting modular forms mod p to the Siegel superspecial locus, and used the meaning of modular forms as global sections of an automorphic bundle. The result of Ghitza has been generalized by Reduzzi [28] to the Shimura varieties attached to unitary groups $GU(r, s)$ associated to imaginary quadratic fields where the prime p is inert. The description of $\mathbb{F}_p$-structure of the superspecial locus of this paper should provide finer information to the theory of algebraic modular forms. For example, the Frobenius map is closely related to an Atkin-Lehner involution. One can also consider the refined JLC modulo p with respect to the decomposition of automorphic forms by the Galois action.

The paper is organized as follows. Section 2 collects elementary properties of schemes transformed by Galois groups and recalls Weil's descent theorem for varieties. In Section 3 we study the field of definition for the superspecial locus as well as NP and EO strata. Proof of Theorem 1.1 is given in Section 4. In Section 5 we show that results of Ibukiyama-Katsura mentioned above follow from Theorem 1.1. In Section 6, we treat the situation with a prime-to-p level structure and generalize Theorems 1.2, 1.3 and 1.4 to higher level structures. Similar results for the *non-principal genus* case are also included. We abstract the properties of computing $\operatorname{tr} R(\pi_0)$ and work on the trace formula in a slightly more general content. As a result, we reduce the calculation of trace of $R(\pi)$ to certain more manageable terms when the level group is small.

2. Preliminaries

In this section we include elementary properties about schemes transformed by Galois groups and Galois descent. This is for the reader's convenience.

2.1. Let $f : X \to S$ be a morphism of schemes, and let $\tau : T \to S$ be a base morphism. Write $X_T := X \times_S T$ for the fiber product, and hence we have the cartesian diagram

$$\begin{array}{ccc} X_T & \xrightarrow{\tau_X} & X \\ \Big\downarrow{\scriptstyle f_T} & & \Big\downarrow{\scriptstyle f} \\ T & \xrightarrow{\tau} & S. \end{array} \tag{2.1}$$

Let T' be a T-scheme, which also regarded as an S-scheme via τ. If $t' \in X_T(T')$, then $\tau_X \circ t \in X_S(T')$. By the functorial property of the fiber product, we get a canonical isomorphism

$$\tau_X : X_T(T') \xrightarrow{\sim} X_S(T'). \tag{2.2}$$

2.2. Let $f : X \to S$ and $\tau : T \to S$ be as above. Regarding X as a contravariant functor, one has a map $X(S) \xrightarrow{\tau^*} X(T)$. Composing with the canonical isomorphism (2.2), we get a map,

$$\tau^* : X(S) \longrightarrow X_T(T). \tag{2.3}$$

Suppose that $S = \operatorname{Spec} A$ is affine. For any $\sigma \in \operatorname{Aut}(A)$, the group of ring automorphisms of A, we have the cartesian diagram

$$\begin{array}{ccc} {}^{\sigma}X & \xrightarrow{(\sigma^*)_X} & X \\ \Big\downarrow{\scriptstyle {}^{\sigma}f} & & \Big\downarrow{\scriptstyle f} \\ S & \xrightarrow{\sigma^*} & S. \end{array} \tag{2.4}$$

where $\sigma^* : S \to S$ denotes the induced isomorphism and ${}^{\sigma}X := X \times_{S,\sigma^*} S$. Note that as schemes, there is a natural morphism from ${}^{\sigma}X$ to X only. The naive Galois action on the *solutions* of X gives a mapping, through (2.3),

$$\sigma_* : X(A) \longrightarrow {}^{\sigma}X(A). \tag{2.5}$$

However, this map does not arise from a morphism of schemes in general.

For any two elements $\sigma_1, \sigma_2 \in \mathrm{Aut}(A)$, one easily sees the relations:

$$\sigma_2^* \circ \sigma_1^* = (\sigma_1\sigma_2)^*, \quad {}^{\sigma_1}({}^{\sigma_2}X) = {}^{\sigma_1\sigma_2}X, \quad \text{and} \quad (\sigma_2^*)_X \circ (\sigma_1^*)_{({}^{\sigma_2}X)} = (\sigma_1\sigma_2)^*_X, \tag{2.6}$$

and

$$\sigma_{1*}\sigma_{2*} = (\sigma_1\sigma_2)_* : X(A) \xrightarrow{\sigma_{2*}} {}^{\sigma_2}X(A) \xrightarrow{\sigma_{1*}} {}^{\sigma_1\sigma_2}X(A). \tag{2.7}$$

We remark that these relations (2.6) and (2.7) still hold if we replace the automorphism group $\mathrm{Aut}(A)$ by the monoid $\mathrm{End}(A)$ of ring endomorphisms of A.

2.3. Let $f_X : X \to S$ and $f_Y : Y \to S$ be two schemes over S. Let $\tau : T \to S$ be a morphism of schemes. If $f : X \to Y$ is a morphism of schemes over S, then we denote by $f^\tau : X_T \to Y_T$ the induced morphism of schemes over T. So we have the following cartesian diagram

$$\begin{array}{ccc} X_T & \xrightarrow{\tau_X} & X \\ \downarrow{\scriptstyle f^\tau} & & \downarrow{\scriptstyle f} \\ Y_T & \xrightarrow{\tau_Y} & Y. \end{array} \tag{2.8}$$

If $\tau' : T' \to T$ be a T-scheme, then we have the relations

$$(f^\tau)^{\tau'} = f^{\tau\tau'}, \quad \tau_X \circ \tau'_{X_T} = (\tau\tau')_X, \quad \text{and} \quad \tau_Y \circ \tau'_{Y_T} = (\tau\tau')_Y. \tag{2.9}$$

Following from functorial properties, we have the following commutative diagram (cf. (2.3)) of sets

$$\begin{array}{ccc} X(S) & \xrightarrow{\tau^*} & X_T(T) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f^\tau} \\ Y(S) & \xrightarrow{\tau^*} & Y_T(T). \end{array} \tag{2.10}$$

In general this is not induced from morphisms of schemes (under $T = S$). However, in some special situation we do have such an analogue; see (3.2).

Suppose that $S = \operatorname{Spec} A$ and $T = \operatorname{Spec} B$ are affine. Let $\mathrm{Aut}_A(B)$ be the group of A-automorphisms of B. For each element $\sigma \in \mathrm{Aut}_A(B)$ and $f \in \mathrm{Hom}_B(X \otimes_A B, Y \otimes_A B)$, the action of σ on f is defined to be $\sigma(f) := {}^\sigma f$ (see (2.4)) in the cartesian diagram:

$$\begin{array}{ccc} X_T & \xrightarrow{\sigma_X^*} & X_T \\ \downarrow{\scriptstyle \sigma(f)} & & \downarrow{\scriptstyle f} \\ Y_T & \xrightarrow{\sigma_Y^*} & Y_T. \end{array} \tag{2.11}$$

Then $\sigma_1(\sigma_2(f)) = (\sigma_1\sigma_2)(f)$, for $\sigma_1, \sigma_2 \in \mathrm{Aut}_A(B)$. That is, the group $\mathrm{Aut}_A(B)$ acts on the set $\mathrm{Hom}_B(X \otimes_A B, Y \otimes_A B)$ from the left.

2.4. Galois descent. We recall Weil's descent theorem for varieties. By a variety over a field k we mean a scheme of finite type of k that is geometrically irreducible. Let k/k_0 be a field extension; we say a variety V over k is defined over k_0 if there exists a variety V_0 over k_0 and there exists an isomorphism $f : V_0 \otimes_{k_0} k \simeq V$ of varieties over k. In this case, the pair (V_0, f) is called a model of V over k_0. Let k be a finite separable extension of a field k_0, and let V be a variety over k. Let $\bar{k}_0$ be the algebraic closure of k_0, and let $\mathfrak{I} := \mathrm{Hom}_{k_0}(k, \bar{k}_0)$ be the set of field embeddings of k into $\bar{k}_0$ over k_0. The Galois group $\mathcal{G}_{k_0} := \mathrm{Gal}(\bar{k}_0/k_0)$ acts naturally on the finite set $\mathfrak{I}$ from the left: For $\sigma \in \mathfrak{I}$ and $\omega \in \mathcal{G}_{k_0}$, set $\omega\sigma = \omega \circ \sigma$. For each element $\sigma \in \mathfrak{I}$, we write ${}^{\sigma}V$ for the variety $V \otimes_{k,\sigma} \bar{k}_0$ over $\bar{k}_0$. Suppose that there is a variety V_0 over k_0 and there is an isomorphism $f : V_0 \otimes_{k_0} k \simeq V$ of varieties over k. For each $\sigma \in \mathfrak{I}$, we have an isomorphism ${}^{\sigma}f : \overline{V}_0 := V_0 \otimes_{k_0} \bar{k}_0 \to {}^{\sigma}V$ over $\bar{k}_0$. Then, for $\sigma, \tau \in \mathfrak{I}$, we have an isomorphism

$$f_{\tau,\sigma} := {}^{\tau}f \circ ({}^{\sigma}f)^{-1} : {}^{\sigma}V \xrightarrow{\sim} {}^{\tau}V$$

of varieties over $\bar{k}_0$. It is easy to check that the morphisms $f_{\tau,\sigma}$ satisfy the following conditions:

(i) $f_{\tau,\rho} = f_{\tau,\sigma} \circ f_{\sigma,\rho}$ for all $\tau, \sigma, \rho \in \mathfrak{I}$,

(ii) $f_{\omega\tau,\omega\sigma} = \omega(f_{\tau,\sigma})$ for all $\tau, \sigma \in \mathfrak{I}$ and $\omega \in \mathcal{G}_{k_0}$.

Conversely, Weil showed that these necessary conditions are also sufficient for V over k to have a model (V_0, f) over k_0, provided that V is quasi-projective over k.

Theorem 2.1. (Weil [34, Theorem 3]) *Notations as above. Assume that V is quasi-projective over k, and that for each pair of elements $\tau, \sigma \in \mathfrak{I}$, there exists an isomorphism $f_{\tau,\sigma} : {}^{\sigma}V \xrightarrow{\sim} {}^{\tau}V$ such that the conditions* (i) *and* (ii) *are satisfied. Then there exists a model (V_0, f) of V over k_0, unique up to an isomorphism over k_0, such that $f_{\tau,\sigma} = {}^{\tau}f \circ ({}^{\sigma}f)^{-1}$, for all $\tau, \sigma \in \mathfrak{I}$.*

Moreover, if V is quasi-projective (resp. affine), then the variety V_0 is quasi-projective (resp. affine).

If the extension k/k_0 is Galois, letting $a_\sigma := f_{\sigma,1} : V \to {}^{\sigma}V$, then the conditions (i) and (ii) are equivalent to the 1-cocycle condition $a_{\tau\sigma} = \tau(a_\sigma) \circ a_\tau$ for all $\tau, \sigma \in \mathrm{Gal}(k/k_0)$:

$$\begin{tikzcd} V \arrow[r, "a_\tau"'] \arrow[rr, bend left, "a_{\tau\sigma}"] & {}^{\tau}V \arrow[r, "\tau(a_\sigma)"'] & {}^{\tau\sigma}V. \end{tikzcd}$$

3. Abelian varieties in characteristic p

3.1. Let S be an $\mathbb{F}_p$-scheme, and let $f_X : X \to S$ be an S-scheme. Denote by $F_S : S \to S$ (resp. $F_X : X \to X$) the Frobenius morphism on S (resp. on X), which is obtained by raising to the p-th power on its functions. Denote by

$$X^{(p)} := X \times_{S,F_S} S$$

the base change of X with respect to the morphism F_S. Let $F_{X/S}$ be the relative Frobenius morphism of X over S, which is defined by the following diagram:

$$\begin{tikzcd} X \arrow[dr, "F_{X/S}"] \arrow[drr, bend left, "F_X"] \arrow[ddr, bend right, "f"'] & & \\ & X^{(p)} \arrow[r] \arrow[d, "f_X^{(p)}"] & X \arrow[d, "f_X"] \\ & S \arrow[r, "F_S"] & S. \end{tikzcd} \tag{3.1}$$

Let $f_Y : Y \to S$ be an S-scheme, and let $f : X \to Y$ be a morphism of schemes over S. We write $f^{(p)}$ for the morphism $X^{(p)} \to Y^{(p)}$ induced by the base change morphism $F_S : S \to S$. Hence, we have the following cartesian diagram and commutative diagram

$$\begin{tikzcd} X^{(p)} \arrow[r] \arrow[d, "f^{(p)}"] & X \arrow[d, "f"] & X \arrow[r, "F_{X/S}"] \arrow[d, "f"] & X^{(p)} \arrow[d, "f^{(p)}"] \\ Y^{(p)} \arrow[r] & Y, & Y \arrow[r, "F_{Y/S}"] & Y^{(p)}. \end{tikzcd} \tag{3.2}$$

Note that the second diagram is not necessarily cartesian. If we write $Frob_p$ for the Frobenius map $\mathcal{O}_S \to \mathcal{O}_S$ raising to the p-th power, then we also write $Frob_p(f)$ for $f^{(p)}$.

3.2. Let A be an abelian variety over a perfect field k of characteristic p. Let $M^*(A)$ be the classical contravariant Dieudonné module of A. Let $W(k)$ be the ring of Witt vectors over k, and let σ_p be the Frobenius map on $W(k)$. If K is a perfect field containing the field k, then we have

$$M^*(A \otimes_k K) = W(K) \otimes_{W(k)} M^*(A). \tag{3.3}$$

In particular, we have

$$M^*(A^{(p)}) = W(k) \otimes_{W(k),\,\sigma_p} M^*(A) \tag{3.4}$$

By definition, the Frobenius map F on $M^*(A)$ is given by the composition of the ($W(k)$-linear) pull-back map

$$F^*_{X/k} : M^*(A^{(p)}) \to M^*(A)$$

and the σ_p-linear map

$$1 \otimes \mathrm{id} : M^*(A) \to W(k) \otimes_{W(k),\,\sigma_p} M^*(A) = M^*(A^{(p)}).$$

Proposition 3.1. *Let X be a p-divisible group over an algebraically closed field k of characteristic p, and let σ be an automorphism of the field k.*

(1) *The p-divisible groups X and ${}^{\sigma}X$ have the same Newton polygon.*
(2) *The p-divisible groups X and ${}^{\sigma}X$ have the same Ekedahl-Oort type. That is, there exists an isomorphism $X[p] \simeq {}^{\sigma}X[p]$ of finite group schemes over k, where $X[p]$ denotes the finite subgroup scheme of p-torsion of X.*
(3) *If X is superspecial, then so ${}^{\sigma}X$ is.*

PROOF. (1) Let X_0 be a p-divisible group over $\mathbb{F}_p$ which has the same Newton polygon as X does. Choose an isogeny $\varphi : X_0 \to X$ over k. Then we have the commutative diagram

$$\begin{tikzcd} X \arrow[dr, "f"'] & X_0 = {}^\sigma X_0 \arrow[l, "\varphi"'] \arrow[r, "{}^\sigma\varphi"] \arrow[d, "f_0 = {}^\sigma f_0"] & {}^\sigma X \arrow[dl, bend left, "{}^\sigma f"] \\ & \operatorname{Spec} k & \end{tikzcd}.$$

This shows that there is an isogeny between the p-divisible groups X and ${}^\sigma X$.

(2) According to the classification of the truncated BT groups of level 1 (see [24]), there is a p-divisible group X_0 over $\mathbb{F}_p$ such that an isomorphism $X[p] \simeq X_0[p]$ over k exists. Applying the automorphism σ on this isomorphism, we get an isomorphism ${}^\sigma X[p] \simeq {}^\sigma X_0[p] = X_0[p]$ over k. This proves (2).

(3) Since X is superspecial, we have $FM^*(X) = VM^*(X)$. This yields that $FM^*({}^\sigma X) = VM^*({}^\sigma X)$. Therefore, the p-divisible group ${}^\sigma X$ is superspecial. ∎

Recall that Λ_g is the superspecial locus of $\mathcal{A}_g \otimes \overline{\mathbb{F}}_p$. The following result follows from Proposition 3.1 (3).

Corollary 3.2. *The action of the Galois group* $\mathcal{G} := \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ *on the set* $\mathcal{A}_g(\overline{\mathbb{F}}_p)$ *leaves the superspecial locus* Λ_g *invariant.*

3.3. For any abelian variety A over a field of characteristic p, we write $A(\ell) := A[\ell^\infty]$ for the associated ℓ-divisible group, and $T_\ell(A)$ for the Tate module module of A in the case $\ell \neq p$. Let σ_p be the Frobenius automorphism in $\mathcal{G}$.

Lemma 3.3. *Let* A_0 *be an abelian variety over* $\mathbb{F}_p$. *Let* π_0 *be the Frobenius endomorphism of* A_0 *over* $\mathbb{F}_p$.

(1) *For any endomorphism* $f \in \mathrm{End}_{\overline{\mathbb{F}}_p}(A_0 \otimes \overline{\mathbb{F}}_p)$ *of* $A_0 \otimes \overline{\mathbb{F}}_p$, *we have the commutative diagram of abelian varieties over* $\overline{\mathbb{F}}_p$

$$\begin{array}{ccc} A_0 \otimes \overline{\mathbb{F}}_p & \xrightarrow{f} & A_0 \otimes \overline{\mathbb{F}}_p \\ \downarrow \pi_0 & & \downarrow \pi_0 \\ A_0 \otimes \overline{\mathbb{F}}_p & \xrightarrow{\sigma_p(f)} & A_0 \otimes \overline{\mathbb{F}}_p. \end{array} \tag{3.5}$$

(2) *For any prime* ℓ *and any endomorphism* f *of the* ℓ*-divisible group* $A_0(\ell) \otimes \overline{\mathbb{F}}_p$, *we have the commutative diagram of* ℓ*-divisible groups over* $\overline{\mathbb{F}}_p$

$$\begin{array}{ccc} A_0(\ell) \otimes \overline{\mathbb{F}}_p & \xrightarrow{f} & A_0(\ell) \otimes \overline{\mathbb{F}}_p \\ \downarrow \pi_0 & & \downarrow \pi_0 \\ A_0(\ell) \otimes \overline{\mathbb{F}}_p & \xrightarrow{\sigma_p(f)} & A_0(\ell) \otimes \overline{\mathbb{F}}_p. \end{array} \tag{3.6}$$

(3) *For any prime $\ell \neq p$, any endomorphism f of the Tate module $T_\ell(A_0)$ and any element $\sigma \in \mathcal{G}$, we have the commutative diagram of Tate modules*

$$\begin{array}{ccc} T_\ell(A_0) & \xrightarrow{f} & T_\ell(A_0) \\ \big\downarrow \sigma & & \big\downarrow \sigma \\ T_\ell(A_0) & \xrightarrow{\sigma(f)} & T_\ell(A_0). \end{array} \tag{3.7}$$

Proof. The statements (1) and (2) follow immediately from the second commutative diagram in (3.2). The statement (3) follows immediately from the commutative diagram (2.10) by letting $S = T = \operatorname{Spec} \overline{\mathbb{F}}_p$ and $\tau = \sigma^*$ and taking the projective limit. ∎

3.4. An example. We show that there is a p-divisible group X over an algebraically closed field k such that X is not isomorphic to ${}^\sigma X$ for some automorphism σ of k. Let E_0 be a supersingular p-divisible group of rank 2 over $\mathbb{F}_{p^2}$ such that the relative Frobenius morphism (from $E_0 \to E_0^{(p^2)} = E_0$) is equal to the morphism $[-p]$. Let $X_0 := E_0^2$. The functor

$$\mathcal{P} : (\mathbb{F}_{p^2}\text{−schemes}) \to (\text{sets}), \quad \mathcal{P}(T) := \operatorname{Hom}_T(\alpha_p \times T, X_0 \times T)$$

is representable by the projective line $\mathbf{P}^1$ over $\mathbb{F}_{p^2}$. Since any morphism $\varphi \in \operatorname{Hom}_T(\alpha_p \times T, X_0 \times T)$ factors through the morphism $(\alpha_p \times \alpha_p) \times T \to X_0 \times T$, the group $\operatorname{End}_{\mathbb{F}_{p^2}}(\alpha_p^2)^\times = \mathrm{GL}_2(\mathbb{F}_{p^2})$ acts naturally on the projective line from the left. For any point $\varphi = [a : b] \in \mathbf{P}^1(k)$, we write $X_{[a:b]}$ for the quotient p-divisible group $X_0/\varphi(\varphi)$.

Lemma 3.4. *Two p-divisible groups $X_{[a:b]}$ and $X_{[a':b']}$ are isomorphic over k if and only if there exists an element $h \in \mathrm{GL}_2(\mathbb{F}_{p^2})$ such that $h[a : b] = [a' : b']$.*

We leave this as an exercise to the reader. Take $k = \overline{\mathbb{F}_p(t)}$. Let $b \in k$ be any linear fractional transformation such that $[1 : b] \notin \mathrm{GL}_2(\mathbb{F}_{p^2})[1 : t]$. Let $\sigma \in \operatorname{Aut}(k)$ be an automorphism which sends t to b. Then the p-divisible group ${}^\sigma X_{[1:t]} = X_{[1:b]}$ is not isomorphic to $X_{[1:t]}$ over k.

3.5. Relationship between p-divisible groups X and ${}^\sigma X$. Let c, d be two positive integers. Let p-$\mathbf{div}(d, c)(k)$ be the set of isomorphism classes of p-divisible groups X of dimension d and of co-dimension c over a field k of characteristic p. By a *p-adic invariant* ψ we mean the association to the equivalence class for an equivalent relation $\sim$ on p-$\mathbf{div}(d, c)(k)$ that is defined using the morphisms F^m, V^n and $[p^r]$, for some integers m, n, r. For any two p-divisible groups $X_1, X_2 \in p$-$\mathbf{div}(d, c)(k)$, we write $\psi(X_1) = \psi(X_2)$ if $X_1 \sim X_2$. Examples of equivalence relations (over an algebraically closed field) are:

(i) Define $X_1 \sim X_2$ if X_1 is isogenous to X_2. In this case, the p-adic invariant ψ associates to X its Newton polygon $NP(X)$.
(ii) Define $X_1 \sim X_2$ if there exists an isomorphism $X_1[p] \simeq X_2[p]$. In this case, the p-adic invariant ψ associates to X its EO type $ES(X)$; see Oort [24] for detail descriptions of EO types.
(iii) Define $X_1 \sim X_2$ if there exists an isomorphism $X_1 \simeq X_2$. In this case, the p-adic invariant ψ associates to X the isomorphism class of itself.

A p-adic invariant ψ is said to be *discrete* if the image

$$\Psi(k) := \{\psi(X); X \in p\text{-}\mathbf{div}(d,c)(k)\}$$

is finite for any algebraically closed field $k \supset \mathbb{F}_p$. The p-adic invariants in (i) and (ii) are discrete, while the p-adic invariant in (iii) is not.

Proposition 3.5. *Let ψ be a discrete p-adic invariant on the set p-$\mathbf{div}(d,c)(k)$, where k is an algebraically closed field of characteristic p. Then there is a p-power integer $q \in \mathbb{N}$ such that*

$$\psi(X) = \psi({}^{\sigma}X)$$

for all $X \in p$-$\mathbf{div}(d,c)(k)$ and $\sigma \in \mathrm{Gal}(k/\mathbb{F}_q)$.

PROOF. Since ψ is discrete, there is a p-power integer $q \in \mathbb{N}$ such that for any $X \in p$-$\mathbf{div}(d,c)(k)$, there is a p-divisible group X_0 over $\mathbb{F}_q$ such that

$$\psi(X) = \psi(X_0 \otimes_{\mathbb{F}_q} k). \tag{3.8}$$

(otherwise $\Psi(\overline{\mathbb{F}}_p)$ would be infinite). We apply any element $\sigma \in \mathrm{Gal}(k/\mathbb{F}_q)$ and get $\psi({}^{\sigma}X) = \psi(X_0 \otimes_{\mathbb{F}_q} k)$. Then the assertion follows. ∎

Due to the example in Section 3.4, Proposition 3.5 seems to be the best we can hope for about the relationship between the p-divisible groups X and ${}^{\sigma}X$.

4. Proof of Theorem 1.1

4.1. Let $\underline{A}_0 = (A_0, \lambda_0)$ be a g-dimensional superspecial principally polarized abelian variety over $\mathbb{F}_p$. Recall that to the polarized abelian variety $\underline{A}_0$ we associate two group schemes $G_1 \subset G$ over $\mathbb{Z}$ as (1.1). Let $\nu : G \to \mathbb{G}_{\mathrm{m}}$ be the multiplier character; we have $\ker \nu = G_1$. Recall that σ_p denotes the Frobenius automorphism in $\mathcal{G} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, and π_0 is the Frobenius endomorphism of A_0 over $\mathbb{F}_p$.

Lemma 4.1. *We have $\pi_0 \in G(\mathbb{Q})$.*

PROOF. Choose any prime $\ell \neq p$. The polarization λ_0 induces the Weil pairing $e_\ell : T_\ell(A_0) \times T_\ell(A_0) \to \mathbb{Z}_\ell(1)$, which is $\mathcal{G}$-equivariant. Then we have (cf. Lemma 3.3 (2) and (3)) $e_\ell(\pi x_0, \pi_0 y) = e_\ell(\sigma_p x, \sigma_p y) = p e_\ell(x,y)$ and $\pi_0' \pi_0 = p$ on $T_\ell(A_0)$. Since the ℓ-adic representation is faithful, $\pi_0 \in G(\mathbb{Q})$. ∎

Proposition 4.2. *The action of $\mathcal{G}$ on $G(\mathbb{A}_f)$ is given by*

$$\sigma_p(x_\ell)_\ell = (\pi_0 x_\ell \pi_0^{-1})_\ell, \quad (x_\ell)_\ell \in G(\mathbb{A}_f). \tag{4.1}$$

PROOF. It suffices to show that for any prime ℓ (including p), the action of $\mathcal{G}$ on $\mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Z}_\ell$ is given by

$$\sigma_p x_\ell = \pi_0 x_\ell \pi_0^{-1}, \quad x_\ell \in \mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Z}_\ell. \tag{4.2}$$

Since A_0 is supersingular, we have the natural isomorphism

$$\mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Z}_\ell \simeq \mathrm{End}(A(\ell) \otimes \overline{\mathbb{F}}_p).$$

The relation (4.2) then follows from Lemma 3.3 (2). ∎

4.2. We now describe the map

$$\mathbf{d_1} : G_1(\mathbb{Q})\backslash G_1(\mathbb{A}_f)/G_1(\hat{\mathbb{Z}}) \simeq \Lambda_g$$

and show that it is $\mathcal{G}$-equivariant. We introduce some notation.

Notation. Let k be any field. Let ℓ be a prime, not necessarily invertible in k. For any object $\underline{A} = (A, \lambda)$ in $\mathcal{A}_g$ over k, we write $\underline{A}(\ell) := (A, \lambda)[\ell^\infty]$ for the associated ℓ-divisible group with the induced quasi-polarization. For any two members $\underline{A}_1 = (A_1, \lambda_1)$ and $\underline{A}_2 = (A_2, \lambda_2)$ in $\mathcal{A}_g$ over k, denote by

- $\mathrm{Isog}_k(\underline{A}_1, \underline{A}_2)$ (resp. $\mathrm{Isom}_k(\underline{A}_1, \underline{A}_2)$) the set of quasi-isogenies (resp. isomorphisms) $\varphi : A_1 \to A_2$ over k such that $\varphi^*\lambda_2 = \lambda_1$, and
- $\mathrm{Isog}_k(\underline{A}_1(\ell), \underline{A}_2(\ell))$ (resp. $\mathrm{Isom}_k(\underline{A}_1(\ell), \underline{A}_2(\ell))$) the set of quasi-isogenies (resp. isomorphisms) $\varphi : A_1[\ell^\infty] \to A_2[\ell^\infty]$ such that $\varphi^*\lambda_2 = \lambda_1$.

Proposition 4.3. *Let $(\phi_\ell)_\ell \in G_1(\mathbb{A}_f)$ be an element. Then there exist*

- *a member $\underline{A} = (A, \lambda) \in \Lambda_g$ determined up to isomorphism,*
- *a quasi-isogeny $\phi \in \mathrm{Isog}_{\overline{\mathbb{F}}_p}(\underline{A}, \underline{A}_0)$, and*
- *an isomorphism $\alpha_\ell \in \mathrm{Isom}_{\overline{\mathbb{F}}_p}(\underline{A}_0(\ell), \underline{A}(\ell))$ for each ℓ*

such that $\phi_\ell = \phi \circ \alpha_\ell$ for all ℓ. Moreover, the map $\widetilde{\mathbf{d}}_\mathbf{1} : G_1(\mathbb{A}_f) \to \Lambda_g$ which sends $(\phi_\ell)_\ell$ to the isomorphism class $[\underline{A}]$ induces a well-defined and bijective map

$$\mathbf{d_1} : G_1(\mathbb{Q})\backslash G_1(\mathbb{A}_f)/G_1(\hat{\mathbb{Z}}) \simeq \Lambda_g.$$

Proof. See [35, Theorem 10.5] or [39, Theorem 2.2].

Let $(\phi_\ell)_\ell \in G_1(\mathbb{A}_f)$ be an element, and let $\underline{A}$, ϕ, α_ℓ be as in Proposition 4.3. Applying an element $\sigma \in \mathcal{G}$, we get

$$\sigma(\phi) \in \mathrm{Isog}_{\overline{\mathbb{F}}_p}({}^\sigma\underline{A}, \underline{A}_0), \quad \sigma(\alpha_\ell) \in \mathrm{Isom}_{\overline{\mathbb{F}}_p}(\underline{A}_0(\ell), {}^\sigma\underline{A}(\ell))$$

and

$$\sigma(\phi_\ell) = \sigma(\phi) \circ \sigma(\alpha_\ell), \quad \forall\, \ell.$$

This yields $\widetilde{\mathbf{d}}_\mathbf{1}(\sigma(\phi_\ell)_\ell) = [{}^\sigma\underline{A}]$, that is, the map $\widetilde{\mathbf{d}}_\mathbf{1}$ is $\mathcal{G}$-equivariant.

The inclusion $G_1(\mathbb{A}_f) \to G(\mathbb{A}_f)$ is $\mathcal{G}$-equivariant and it induces a $\mathcal{G}$-equivariant bijection

$$G_1(\mathbb{Q})\backslash G_1(\mathbb{A}_f)/G_1(\hat{\mathbb{Z}}) \simeq G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\hat{\mathbb{Z}}).$$

Let

$$\widetilde{\mathbf{d}} : G(\mathbb{A}_f) \to G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\hat{\mathbb{Z}}) \simeq G_1(\mathbb{Q})\backslash G_1(\mathbb{A}_f)/G_1(\hat{\mathbb{Z}}) \stackrel{\mathbf{d_1}}{\to} \Lambda_g$$

be the composition. Therefore, the induced map $\widetilde{\mathbf{d}} : G(\mathbb{A}_f) \to \Lambda_g$ is $\mathcal{G}$-equivariant. This proves Theorem 1.1.

Remark 4.4. For a suitable choice of the base point (A_0, λ_0) as the product of copies of E_0 with $\pi_{E_0}^2 = -p$, one easily sees that π_0 can be represented as the matrix

$$\begin{pmatrix} 0 & -pI_g \\ I_g & 0 \end{pmatrix},$$

for a suitable identification $\mathrm{End}^0(\overline{A}_0) \simeq M_g(B_{p,\infty}) \subset M_{2g}(\mathbb{Q}(\sqrt{-p}))$, where I_g is the identity matrix of size g. The action of Frobenius automorphism σ_p on $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\hat{\mathbb{Z}})$, according to Proposition 4.2, is an involution of Atkin-Lehner type.

5. Proofs of Theorems 1.2 and 1.3

In this and the next sections, we fix a base point (A_0,λ_0) over $\mathbb{F}_p$ as

$$(A_0,\lambda_0)=(E_0^g,\mu_0^g), \tag{5.1}$$

where E_0 is a supersingular elliptic curve over $\mathbb{F}_p$ satisfying $\pi_{E_0}^2=-p$, and μ_0 is the canonical polarization on E_0. Let G be the group scheme over $\mathbb{Z}$ associated to (A_0,λ_0) as in (1.1).

5.1. Proofs of Theorems 1.2 and 1.3 (1).

Proposition 5.1. *Every member (A,λ) in Λ_g has a unique model defined over $\mathbb{F}_{p^2}$, up to isomorphism over $\mathbb{F}_{p^2}$, such that the quasi-isogeny ϕ in Proposition 4.3 can be chosen defined over $\mathbb{F}_{p^2}$.*

Proof. This refines [12, Lemma 2.1]. Let $(\phi_\ell)\in G_1(\mathbb{A}_f)$ be an element such that the class $[(\phi_\ell)]$ corresponds to (A,λ). Let ϕ and α_ℓ for all ℓ be as in Proposition 4.3. If $\sigma\in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{p^2})$, then by Theorem 1.1 we have $\sigma(\phi)\circ\sigma(\alpha_\ell)=\phi\circ\alpha_\ell$, and hence $\phi_\sigma:=\phi^{-1}\circ\sigma(\phi):({}^\sigma A,{}^\sigma\lambda)\to(A,\lambda)$ is an isomorphism. For $\sigma,\tau\in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{p^2})$, put $f_{\tau,\sigma}=\phi_\tau^{-1}\circ\phi_\sigma:({}^\sigma A,\,{}^\sigma\lambda)\simeq({}^\tau A,\,{}^\tau\lambda)$. Then it is easy to check that the conditions (i) and (ii) of Theorem 2.1 for $f_{\tau,\sigma}$ are satisfied. Therefore by Weil's Theorem, there exist a model (A_1,λ_1) over $\mathbb{F}_{p^2}$ and an isomorphism $f:(A_1,\lambda_1)\otimes_{\mathbb{F}_{p^2}}\overline{\mathbb{F}}_p\simeq(A,\lambda)$ such that $\phi_\sigma=f\circ\sigma(f)^{-1}$. We get $\sigma(\phi\circ f)=\phi\circ f$, and hence $\phi_1:=\phi\circ f$ is a quasi-isogeny in $\mathrm{Isog}_{\mathbb{F}_{p^2}}(\underline{A}_1,\underline{A}_0)$

Suppose that (A_2,λ_2) is another model over $\mathbb{F}_{p^2}$ of (A,λ) such that the set $\mathrm{Isog}_{\mathbb{F}_{p^2}}(\underline{A}_2,\underline{A}_0)$ is non-empty. Then we can choose $\phi_2\in\mathrm{Isog}_{\mathbb{F}_{p^2}}(\underline{A}_2,\underline{A}_0)$ such that $\phi_2^{-1}\phi_1:\underline{A}_1\to\underline{A}_2$ is an isomorphism, which is defined over $\mathbb{F}_{p^2}$. ∎

Definition 5.2. We shall call the unique model $\underline{A}_1$ obtained in Proposition 5.1 the *canonical model* of (A,λ) over $\mathbb{F}_{p^2}$. Note that if $\underline{A}_1$ is a canonical model over $\mathbb{F}_{p^2}$, then the Frobenius endomorphism π_{A_1} of A_1 over $\mathbb{F}_{p^2}$ is equal to $-p$, and hence every endomorphism in $\mathrm{End}_{\overline{\mathbb{F}}_p}(A_1\otimes\overline{\mathbb{F}}_p)$ is defined over $\mathbb{F}_{p^2}$.

Let $\mathbf{\Lambda}_g\subset\mathcal{A}_g$ be the superspecial locus; $\Lambda_g=\mathbf{\Lambda}_p(\overline{\mathbb{F}}_p)$ classifies $\overline{\mathbb{F}}_p$-isomorphism class of g-dimensional superspecial principally polarized abelian varieties. The set $\mathbf{\Lambda}_g(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points consists objects in Λ_g that are fixed by σ_p. It follows from Theorem 1.1 that $\mathbf{\Lambda}_g(\mathbb{F}_{p^2})=\Lambda_g$.

Proposition 5.1 allows us to identify Λ_g with the set of $\mathbb{F}_{p^2}$-isomorphism classes of g-dimensional superspecial principally polarized abelian varieties (A_1,λ_1) over $\mathbb{F}_{p^2}$ such that the set $\mathrm{Isog}_{\mathbb{F}_{p^2}}(\underline{A}_1,\underline{A}_0)$ (see Section 4.2) is non-empty.

Recall that $U:=G(\hat{\mathbb{Z}})\subset G(\mathbb{A}_f)$ and $U(\pi_0):=U\pi_0=\pi_0U\subset G(\mathbb{A}_f)$.

Proposition 5.3.

(1) *Let (A,λ) be a member in Λ_g and let $[x]\in G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U$ be the double coset corresponding to (A,λ). Then (A,λ) lies in $\mathbf{\Lambda}_g(\mathbb{F}_p)$ if and only if*

$$G(\mathbb{Q})\cap xU(\pi_0)x^{-1}\neq\emptyset. \tag{5.2}$$

(2) *We have $|\mathbf{\Lambda}_g(\mathbb{F}_p)|=\mathrm{tr}\,R(\pi_0)$.*

PROOF. (1) The isomorphism class of (A,λ) is fixed by σ_p exactly when $[x] = [\pi_0 x \pi_0^{-1}] = [x\pi_0]$. Therefore, there are some elements $u \in U$ and $a \in G(\mathbb{Q})$ such that $x = a x \pi_0 u$. We get $a^{-1} = x\pi_0 u x^{-1}$. This is equivalent to condition (5.2).

(2) By Theorem 1.1, $R(\pi_0)$ is the operator induced by the action of σ_p^{-1}. Therefore, the number of fixed points of σ_p is equal to $\operatorname{tr} R(\pi_0)$. ∎

Lemma 5.4. *Let (A,λ) be a polarized abelian variety over $\overline{\mathbb{F}}_p$, and suppose that the field of moduli of (A,λ) is $\mathbb{F}_{p^a}$. Then (A,λ) has a model defined over $\mathbb{F}_{p^a}$. Particularly, any member $(A,\lambda) \in \mathbf{\Lambda}_g(\mathbb{F}_p)$ admits a model defined over $\mathbb{F}_p$.*

PROOF. Put $q := p^a$ and let $\sigma : x \mapsto x^q$ be the Frobenius automorphism in $\operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_q)$. Suppose (A,λ) has a model (A_1,λ_1) defined over $\mathbb{F}_{q^c}$ for some positive integer c divisible by a. Increasing c if necessary, we may assume that $\operatorname{End}_{\overline{\mathbb{F}}_p}(A) = \operatorname{End}_{\mathbb{F}_{p^c}}(A_1)$. As the field of moduli of (A,λ) is $\mathbb{F}_{p^a}$, there exists an isomorphism

$$a_\sigma : (A,\lambda) \simeq ({}^\sigma\! A, {}^\sigma\!\lambda)$$

of polarized abelian varieties over $\overline{\mathbb{F}}_p$. Let

$$b_\sigma := \sigma^{c-1}(a_\sigma)\cdots\sigma(a_\sigma)a_\sigma : (A,\lambda) \to (A,\lambda)$$

be the composition. Since b_σ is an automorphism of (A,λ), it is of finite order, say $b_\sigma^m = 1$ for some $m \ge 1$. It follows from $\operatorname{End}(A) = \operatorname{End}(A_1)$ that $\sigma^c(b_\sigma) = b_\sigma$. We get

$$\sigma^{mc-1}(a_\sigma)\cdots\sigma(a_\sigma)a_\sigma = 1. \tag{5.3}$$

Define $a_{\sigma^n} := \sigma(a_{\sigma^{n-1}})a_\sigma$ recursively. The collection of automorphisms a_{σ^n} satisfies the 1-cocycle condition for the Galois extension $\mathbb{F}_{q^{mc}}/\mathbb{F}_q$, by (5.3). Then by Weil's criterion (Theorem 2.1), there exist an abelian variety A' over $\mathbb{F}_q$ and an isomorphism $f : A' \otimes \overline{\mathbb{F}}_p \simeq A$ such that $a_\sigma = \sigma(f) \circ f^{-1}$. Set $\lambda' := f^*\lambda$. Using $\lambda = a_\sigma^* \sigma(\lambda)$, we get

$$\begin{aligned} \lambda' &= f^t \lambda f = f^t(a_\sigma^*\sigma(\lambda))f \\ &= f^t a_\sigma^t \sigma(\lambda) a_\sigma f = \sigma(f^t)\sigma(\lambda)\sigma(f) = \sigma(\lambda'). \end{aligned} \tag{5.4}$$

This shows that (A',λ') is a model defined over $\mathbb{F}_q$ of (A,λ). ∎

Theorems 1.2 and 1.3 (1) follow from Propositions 5.1, 5.3 and Lemma 5.4.

We remark that the same proof of Lemma 5.4 also shows the following generalization:

Proposition 5.5. *Let (X,ξ) be an (irreducible) variety over $\overline{\mathbb{F}}_p$ together with an additional structure ξ which is defined algebraically. If the automorphism group $\operatorname{Aut}_{\overline{\mathbb{F}}_p}(X,\xi)$ is finite and assume that the Weil descent datum for (X,ξ) is effective, then (X,ξ) has a model defined over the field of moduli of (X,ξ).*

When X is quasi-projective and ξ is a polarization (an algebraic equivalence class of an ample line bundle) and/or a morphism in $\operatorname{Mor}(X^m, X^n)$, where $X^m = X \times_k \cdots \times_k X$ is the m-fold fiber product of X, the assumption of the Weil descent datum holds for (X,ξ).

5.2. Proof of Theorem 1.3 (2). Let D be the group scheme over $\mathbb{Z}$ representing the following functor

$$R \to (\mathrm{End}(E_0 \otimes \overline{\mathbb{F}}_p) \otimes R)^\times,$$

where R is a commutative ring. In particular, $D(\mathbb{Q}_p) = (B_{p,\infty} \otimes \mathbb{Q}_p)^\times$. We regard D as a subgroup scheme of G through the diagonal embedding. Let Z be the center of G.

Lemma 5.6.
(1) *For any prime $\ell \neq p$, the subgroup N_ℓ of $G(\mathbb{Q}_\ell)$ which normalizes the maximal order* $\mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Z}_\ell$ *is $Z(\mathbb{Q}_\ell)G(\mathbb{Z}_\ell)$.*
(2) *The subgroup N_p of $G(\mathbb{Q}_p)$ which normalizes the maximal order* $\mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \mathbb{Z}_p$ *is $D(\mathbb{Q}_p)G(\mathbb{Z}_p)$.*

Proof. We sketch the proof; the omitted part is mere straightforward computation. Put $H_\ell := Z(\mathbb{Q}_\ell)G(\mathbb{Z}_\ell)$, for $\ell \neq p$, and $H_p := D(\mathbb{Q}_p)G(\mathbb{Z}_p)$. It is clear that the group H_v normalizes the order $\mathcal{O}_v := \mathrm{End}_{\overline{\mathbb{F}}_p}(A_0) \otimes \mathbb{Z}_v$. It suffices to show that any element $\bar{g}$ in N_v/H_v is the identity class. By the Iwasawa decomposition, we have $G(\mathbb{Q}_v) = P(\mathbb{Q}_v)G(\mathbb{Z}_v)$, where P is the standard minimal parabolic subgroup over $\mathbb{Q}_v$. We may assume that a representative g_ℓ (resp. g_p) is a upper triangular matrix in $G(\mathbb{Q}_\ell) \subset M_{2g}(\mathbb{Q}_\ell)$ (resp. in $G(\mathbb{Q}_p) \subset M_g(B_{p,\infty} \otimes \mathbb{Q}_p)$. Let E_{ij} denote the matrix in which the (i,j)-entry is 1 and others are zero. It follows from $g_v E_{ij} g_v^{-1} \in \mathcal{O}_v$ for all i, j (by looking at its (i,j)-entry) that the diagonal entries of g_v have the same valuation. Modulo H_v, we may assume that g_v lies in the group of upper triangular unipotent matrices. It follows from $g_v E_{ii} g_v^{-1} \in \mathcal{O}_v$ for all i that every entry of g_v is integral and hence $g_v \in G(\mathbb{Z}_v)$. This shows the lemma. ∎

Remark 5.7. One can also use the Cartan decomposition to show Lemma 5.6.

Let $\widetilde{U}$ be the open subgroup of $G(\mathbb{A}_f)$ generated by the open compact subgroup U and the element π_0. Since π_0 normalizes U and $\pi_0^m \notin U$ for $m \neq 0$, we have

$$\widetilde{U} = \bigcup_{m \in \mathbb{Z}} U \pi_0^m, \quad \text{(disjoint)}.$$

Consider $G(\mathbb{Q})$ as a subgroup of $G(\mathbb{Q}_v)$ for each place v, and identify π_0 with its image in $G(\mathbb{Q}_v)$. Note that $\pi_0 \in G(\mathbb{Z}_\ell)$ for $\ell \neq p$, and $\pi_0 \in D(\mathbb{Q}_p)$, which is also a uniformizer of the division quaternion algebra $B_{p,\infty} \otimes \mathbb{Q}_p$. We have

$$\widetilde{U} = \widetilde{U}_p \times U^p, \quad \widetilde{U}_p = \bigcup_{m \in \mathbb{Z}} G(\mathbb{Z}_p)\pi_0^m = D(\mathbb{Q}_p)G(\mathbb{Z}_p),$$

where $U^p = \prod_{\ell \neq p} G(\mathbb{Z}_\ell)$.

Corollary 5.8. *Notations as above. The natural map*

$$G(\mathbb{Q})\backslash G(\mathbb{A}_f)/\widetilde{U} \to \mathcal{T}(G) = G(\mathbb{Q})\backslash G(\mathbb{A}_f)/\mathfrak{N}$$

is bijective.

Proof. By Lemma 5.6, we have

$$G(\mathbb{Q})\backslash G(\mathbb{A}_f)/\mathfrak{N} = G(\mathbb{Q})\backslash G(\mathbb{A}_f)/(\widetilde{U}_p \times Z(\mathbb{A}_f^p)U^p).$$

The latter is equal to

$$G(\mathbb{Q})(\{1\} \times Z(\mathbb{A}_f^p))\backslash G(\mathbb{A}_f)/(\widetilde{U}_p \times U^p) = G(\mathbb{Q})(\{1\} \times Z(\hat{\mathbb{Z}}^p))\backslash G(\mathbb{A}_f)/\widetilde{U}.$$

Since $Z(\hat{\mathbb{Z}}^p)\subset U^p$, the latter is equal to $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/\widetilde{U}$. This finishes the proof. Note that the proof uses class number one of Z. ∎

Theorem 5.9. *The natural projection* $\mathrm{pr}: G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U=\Lambda_g\to\mathcal{T}(G)$ *induces a bijection between the set of* $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$*-orbits of* Λ_g *the set* $\mathcal{T}(G)$*.*

PROOF. By Corollary 5.8, the map $\Lambda_g\to\mathcal{T}(G)$ is simply the projection map $\mathrm{pr}: G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U\to G(\mathbb{Q})\backslash G(\mathbb{A}_f)/\widetilde{U}$, and the Frobenius $\sigma_p=\sigma_p^{-1}$ acts as $[x]\mapsto[x\pi_0]$ for $x\in G(\mathbb{A}_f)$. Since π_0 normalizes U, we have $\mathrm{pr}([x])=\mathrm{pr}([x\pi_0])$. Suppose $\mathrm{pr}([x])=\mathrm{pr}([y])$ for $x,y\in G(\mathbb{A}_f)$. Then $y=ax\pi_0^m u$ for some $m\in\mathbb{Z}$, $u\in U$ and $a\in G(\mathbb{Q})$. Since $\pi_0^2=-p$ is in the center, we may assume $m=0$ or 1. Then $[y]=[x\pi_0^m]$ for $m=0$ or 1. This completes the proof. ∎

Let $\Lambda_g':=\mathbf{\Lambda}_g(\mathbb{F}_p)^c$ be the complement of $\mathbf{\Lambda}_g(\mathbb{F}_p)$ in Λ_p. Theorem 5.9 shows that

$$\frac{1}{2}|\Lambda_g'|+|\mathbf{\Lambda}_g(\mathbb{F}_p)|=T. \tag{5.5}$$

By $H=|\Lambda_g|=|\Lambda_g'|+|\mathbf{\Lambda}_g(\mathbb{F}_p)|$ and $\mathrm{tr}\,R(\pi_0)=|\mathbf{\Lambda}_g(\mathbb{F}_p)|$, we get

$$\mathrm{tr}\,R(\pi_0)=2T-H.$$

Theorem 1.3 (2) is proved.

Remark 5.10. We discuss a bit some relationship between Proposition 5.1 and Lemma 5.4. We call a model (A',λ') over $\mathbb{F}_p$ of a member (A,λ) in $\mathbf{\Lambda}_g(\mathbb{F}_p)$ *nearly canonical* if the set $\mathrm{Isog}_{\mathbb{F}_{p^2}}(\underline{A}',\underline{A}_0)$ is non-empty, that is, the base change $(A',\lambda')\otimes_{\mathbb{F}_p}\mathbb{F}_{p^2}$ is the canonical model over $\mathbb{F}_{p^2}$ (Definition 5.2). We do not know whether or not any member (A,λ) in $\mathbf{\Lambda}_g(\mathbb{F}_p)$ admits a model over $\mathbb{F}_p$ which is nearly canonical. The object (A,λ) admits a nearly canonical model over $\mathbb{F}_p$ if and only if one can choose an automorphism $a_{\sigma_p}:(A,\lambda)\simeq({}^{\sigma_p}A,{}^{\sigma_p}\lambda)$ such that $\sigma_p(a_{\sigma_p})a_{\sigma_p}=1$.

For $g=1$ and $g=2,3$, the set Λ_1 has only one member E as the class number of $B_{p,\infty}$ is one. Therefore, $\mathbf{\Lambda}_1(\mathbb{F}_p)=\Lambda_1$ and any supersingular elliptic curve E_0 over $\mathbb{F}_p$ is a model of E. The Weil polynomial of E_0 is t^2+2, or $t^2\pm 2t+2$ for $p=2$, and t^2+2, or $t^2\pm 3t+3$ for $p=3$. Thus, we conclude that a model over $\mathbb{F}_p$ of a member $(A,\lambda)\in\mathbf{\Lambda}_g(\mathbb{F}_p)$ is not unique in general, and is not necessarily to be nearly canonical.

6. Variants with level structures

In this section, the ground field for abelian varieties, if not specified otherwise, is always $\overline{\mathbb{F}}_p$.

6.1. We keep the notation as in the previous sections. Let N be a prime-to-p positive integer. Let U_N^p be the kernel of the reduction map $G(\hat{\mathbb{Z}}^{(p)})\to G(\mathbb{Z}/N\mathbb{Z})$, $U_p:=G(\mathbb{Z}_p)$, and $U_N:=U_p\times U_N^p$, where $\hat{\mathbb{Z}}^{(p)}:=\prod_{\ell\neq p}\mathbb{Z}_\ell$.

Definition 6.1. Let (A,λ) be a member of Λ_g. A *level-N structure on* (A,λ) *with respect to* $\underline{A}_0$ (over $\overline{\mathbb{F}}_p$) is an isomorphism $\eta_N: A_0[N]\simeq A[N]$ over $\overline{\mathbb{F}}_p$ such that there exists an automorphism $\zeta\in\mathrm{Aut}_{\overline{\mathbb{F}}_p}(\mu_N)=(\mathbb{Z}/N\mathbb{Z})^\times$ such that

$$e_\lambda(\eta(x),\eta(y))=\zeta e_{\lambda_0}(x,y),\quad\forall\,x,y\in A_0[N], \tag{6.1}$$

where $e_\lambda: A[N]\times A[N]\to\mu_N$ denotes the Weil pairing induced by the polarization λ.

Denote by $\Lambda^*_{g,N}$ the set of isomorphism classes of objects (A,λ,η_N) over $\overline{\mathbb{F}}_p$, where

- $(A,\lambda)\in\Lambda_g$, and
- η_N is a level-N structure on (A,λ) with respect to $\underline{A}_0$.

Two objects (A,λ,η_N) and (A',λ',η'_N) are isomorphic, denoted as $(A,\lambda,\eta_N)\simeq(A',\lambda',\eta'_N)$, if there exists an isomorphism $\varphi: A\to A'$ such that $\varphi^*\lambda'=\lambda$ and $\varphi_*\eta_N=\eta'_N$. By an object (A,λ,η_N) over a subfield $k_0\subset\overline{\mathbb{F}}_p$ we mean that both (A,λ) and $\eta_N: A_0[N]\simeq A[N]$ are defined over k_0. As noted in Section 1, the main purpose of introducing $\Lambda^*_{g,N}$ is to make a precise meaning in the geometric side of (1.7).

For any prime ℓ, let

$$\mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}(\ell))$$

denote the set of isomorphisms $\eta: A_0[\ell^\infty]\to A[\ell^\infty]$ (over $\overline{\mathbb{F}}_p$) such that $\eta^*\lambda=\zeta\lambda_0$ for some $\zeta\in\mathbb{Z}_\ell^\times$; it is a right $G(\mathbb{Z}_\ell)$-torsor. (The letter "G" stands for preserving the (quasi-)polarizations up to scalars. Compare the definitions $\mathrm{Isog}(\cdot,\cdot)$ in Section 4.2 and $\mathrm{GIsog}(\cdot,\cdot)$ in Section 6.2.) For such η, one has

$$e_\lambda(\eta(x),\eta(y))=\zeta e_{\lambda_0}(x,y),\quad \forall\, x,y\in A_0[\ell^m],\ \forall\, m\geq 1\in\mathbb{Z}. \tag{6.2}$$

If η is an element in $\prod_\ell \mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}(\ell))$, where ℓ runs over all primes in $\mathbb{Q}$, then the restriction $\eta|_{A_0[N]}$ of η to $A_0[N]$ is a level-N structure on (A,λ) with respect to $\underline{A}_0$. Conversely, we have

Lemma 6.2. *Any level-N structure η_N on $(A,\lambda)\in\Lambda_g$ with respect to $\underline{A}_0$ can be lifted to an element η in $\prod_\ell \mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}(\ell))$.*

Proof. We may assume that $N=\ell^m$ is a power of ℓ and show that η_N can be lifted in $\mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}(\ell))$, where $\ell\neq p$. Since $\underline{A}_0(\ell)$ is isomorphic to $\underline{A}(\ell)$, we may also assume that $A=A_0$. We have $\mathrm{End}(A_0)\otimes\mathbb{Z}_\ell\simeq\mathrm{End}(A_0(\ell))$, and hence $G(\mathbb{Z}_\ell)=\mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}_0(\ell))$. On the other hand, the group $G(\mathbb{Z}/\ell^m\mathbb{Z})$ consists of elements $\bar\varphi\in\mathrm{End}(A_0(\ell))\otimes(\mathbb{Z}/\ell^m\mathbb{Z})$ such that $\bar\varphi'\bar\varphi=\zeta\in(\mathbb{Z}/\ell^m\mathbb{Z})^\times$. We shall show the natural map $\mathrm{End}(A_0(\ell))\otimes\mathbb{Z}/\ell^m\mathbb{Z}\to\mathrm{End}(A_0[\ell^m])$ is an isomorphism. It then follows that $G(\mathbb{Z}/\ell^m\mathbb{Z})$ is isomorphic to the group of elements $\eta\in\mathrm{End}(A_0[\ell^m])$ such that $\eta^*e_{\lambda_0}=\zeta e_{\lambda_0}$ for some $\zeta\in(\mathbb{Z}/\ell^m\mathbb{Z})^\times$. It follows from the smoothness of $G\otimes\mathbb{Z}_\ell$ (as $G\otimes\mathbb{Z}_\ell\simeq\mathrm{GSp}_{2g}$) that the reduction map $G(\mathbb{Z}_\ell)\to G(\mathbb{Z}/\ell^m\mathbb{Z})$ is surjective. Therefore, the element η can be lifted to an element $\varphi\in\mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}_0(\ell))$.

Since $\ell\neq p$, we have $\mathrm{End}(A_0(\ell))=\mathrm{End}(T_\ell(A_0))$. Since $T_\ell(A_0)$ is a finite free $\mathbb{Z}_\ell$-module, we have

$$\mathrm{End}(T_\ell(A_0))\otimes\mathbb{Z}/\ell^m\mathbb{Z}=\mathrm{End}(T_\ell(A_0)/\ell^mT_\ell(A_0))=\mathrm{End}(A_0[\ell^m]).$$

This proves the isomorphism $\mathrm{End}(A_0(\ell))\otimes\mathbb{Z}/\ell^m\mathbb{Z}\simeq\mathrm{End}(A_0[\ell^m])$ and hence the lemma. ∎

By Lemma 6.2, each level-N structure η_N on (A,λ) uniquely determines a U_N-orbit

$$[\eta]:=\left\{\eta\in\prod_\ell \mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}(\ell))\ \middle|\ \eta|_{A_0[N]}=\eta_N\right\}$$

in the $G(\hat{\mathbb{Z}})$-torsor $\prod_\ell \mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}(\ell))$.

Remark 6.3. (1) One can define the notion of level-N structure on an object (A,λ) in Λ_g with respect to $\underline{A}_0$ in the same way as Definition 6.1 without the assumption $(p,N)=1$. However, Lemma 6.2 fails if $p\,|N$ because the natural map $\mathrm{End}(A_0(p))\otimes\mathbb{Z}/p^m\mathbb{Z}\to\mathrm{End}(A_0[p^m])$ is not an isomorphism. For example, let E be a supersingular elliptic curve, then

$$\mathrm{End}(E[p])\simeq\left\{\begin{pmatrix} a & 0\\ b & a^p\end{pmatrix}\,\Big|\, a\in\mathbb{F}_{p^2}, b\in\overline{\mathbb{F}}_p\right\}$$

while

$$\mathrm{End}(E(p))\otimes\mathbb{Z}/p\mathbb{Z}\simeq\left\{\begin{pmatrix} a & 0\\ b & a^p\end{pmatrix}\,\Big|\, a,b\in\mathbb{F}_{p^2}\right\}.$$

(2) For any positive integer N, we call an element

$$[\eta]\in\left[\prod_{\ell}\mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}(\ell))\right]/U_N$$

an $(\underline{A}_0,U_N)$*-level structure on the object* (A,λ) (see [39, Section 2.2]). This is a better notion of level-N structure on $\underline{A}$. For any subfield k_0 of $\overline{\mathbb{F}}_p$, an *object* $(A,\lambda,[\eta])$ *over* k_0 is defined to be an superspecial principally polarized abelian variety (A,λ) over k_0 together with an $(\underline{A}_0,U_N)$-level structure $[\eta]$ on $(A,\lambda)\otimes\overline{\mathbb{F}}_p$ which is invariant under the $\mathrm{Gal}(\overline{\mathbb{F}}_p/k_0)$-action. One can prove that if the isomorphism class of an objective $(A,\lambda,[\eta])$ over $\overline{\mathbb{F}}_p$ is defined over k_0, then $(A,\lambda,[\eta])$ admits a model $(A',\lambda',[\eta'])$ over k_0. The proof is similar to those of Lemma 6.5 and of Theorem 6.6 (1).

6.2. For each object $\underline{A}=(A,\lambda)\in\mathcal{A}_g(\overline{\mathbb{F}}_p)$, we write

$$T^{(p)}(A):=\prod_{\ell\neq p}T_\ell(A)$$

for the prime-to-p Tate module of A, and $V^{(p)}(A):=T^{(p)}(A)\otimes_{\hat{\mathbb{Z}}^{(p)}}\mathbb{A}_f^p$, where $\mathbb{A}_f^p$ is the prime-to-p finite adele ring of $\mathbb{Q}$. Let

$$\langle\,,\rangle_\lambda: V^{(p)}(A)\times V^{(p)}(A)\to\mathbb{A}_f^p(1):=V^{(p)}(\mathbb{G}_{\mathrm{m}})$$

be the induced non-degenerate alternating pairing, for which $T^{(p)}(A)$ is a self-dual $\hat{\mathbb{Z}}^{(p)}$-lattice. For brevity, we write $V^{(p)}(\underline{A}):=(V^{(p)}(A),\langle\,,\rangle_\lambda)$. We introduce some more notation.

Notation. (1) For any two objects $\underline{A},\underline{A}'$ in $\mathcal{A}_g(\overline{\mathbb{F}}_p)$, we denote by

$$\mathrm{GIsom}(V^{(p)}(\underline{A}),V^{(p)}(\underline{A}'))$$

the set of isomorphisms $\eta: V^{(p)}(A)\to V^{(p)}(A')$ such that there exists an automorphism $\zeta\in\mathrm{Aut}(\mathbb{A}_f^p(1))=(\mathbb{A}_f^p)^\times$ such that

$$\langle\eta(x),\eta(y)\rangle_{\lambda'}=\zeta\langle\eta(x),\eta(y)\rangle_\lambda,\quad\forall\, x,y\in V^{(p)}(A).\tag{6.3}$$

The letter“G” stands for preserving polarizations up to scalars.

(2) For any field k and two objects $\underline{A}_1=(A_1,\lambda_1)$ and $\underline{A}_2=(A_2,\lambda_2)$ in $\mathcal{A}_g(k)$, denote by $\mathrm{GIsog}_k^{(p)}(\underline{A}_1,\underline{A}_2)$ the set of prime-to-p quasi-isogenies $\varphi: A_1\to A_2$ over k such that $\varphi^*\lambda_2=q\lambda_1$ for some $q\in\mathbb{Z}_{(p),+}^\times$, where $\mathbb{Z}_{(p),+}^\times\subset\mathbb{Z}_{(p)}^\times$ denotes the subset

consisting of all positive elements.

Let $\Lambda_{g,N}^{(p)}$ denote the set of equivalence classes of objects $(A,\lambda,[\eta]^p)$ over $\overline{\mathbb{F}}_p$, where $(A,\lambda)\in\Lambda_g$ and $[\eta]^p$ is an element in $\mathrm{GIsom}(V^{(p)}(\underline{A}_0),V^{(p)}(\underline{A}))/U_N^p$. Two objects $(A,\lambda,[\eta]^p)$ and $(A',\lambda',[\eta']^p)$ are equivalent, denoted as $(A,\lambda,[\eta]^p)\sim(A',\lambda',[\eta']^p)$, if there is a quasi-isogeny $\varphi\in\mathrm{GIsog}_{\overline{\mathbb{F}}_p}^{(p)}((A,\lambda),(A',\lambda'))$ such that $\varphi_*[\eta]^p=[\eta']^p$.

There is a natural map $f:\Lambda_{g,N}^*\to\Lambda_{g,N}^{(p)}$ which sends each object (A,λ,η_N) to $(A,\lambda,[\eta]^p)$, where $[\eta]^p$ is the class of maps η on $\prod_{\ell\neq p}A_0(\ell)$ whose restriction to $A_0[N]$ is equal to η_N, as we have the identification

$$\begin{aligned}\prod_{\ell\neq p}\mathrm{GIsom}(\underline{A}_0(\ell),\underline{A}(\ell))&=\mathrm{GIsom}(T^{(p)}(\underline{A}_0),T^{(p)}(\underline{A}))\\&\subset\mathrm{GIsom}(V^{(p)}(\underline{A}_0),V^{(p)}(\underline{A})).\end{aligned}$$

Theorem 6.4.

(1) *The natural map* $f:\Lambda_{g,N}^*\to\Lambda_{g,N}^{(p)}$ *is bijective and compatible with the action of the Galois group* $\mathcal{G}$.
(2) *There is a natural bijective map* $\mathbf{c}_N:\Lambda_{g,N}^{(p)}\to G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_N$ *for which the base point* $(A_0,\lambda_0,[\mathrm{id}])$ *is sent to the identity class* $[1]$ *and* $\mathbf{c}_N$ *is* $\mathcal{G}$-*equivariant.*

Proof. (1) Let (A,λ,η_N) and (A',λ',η'_N) be two objects in $\Lambda_{g,N}^*$ such that $(A,\lambda,[\eta]^p)\sim(A',\lambda',[\eta']^p)$. Then there is a prime-to-p quasi-isogeny $\varphi:A\to A'$ such that $\varphi^*\lambda'=q\lambda$ for some $q\in\mathbb{Z}_{(p),+}^\times$ such that $[\varphi\eta]^p=[\eta']^p$. We may assume $\eta'=\varphi\eta$. As $\eta'\eta^{-1}$ maps $T^{(p)}(A)$ onto $T^{(p)}(A')$, the map $\varphi=\eta'\eta^{-1}$ induces an isomorphism from $T^{(p)}(A)$ to $T^{(p)}(A')$. Therefore, $v_\ell(q)=0$ for all $\ell\neq p$, and hence we have $\varphi^*\lambda'=\lambda$ and $\varphi\eta_N=\eta'_N$. This shows the injectivity.

We show the surjectivity. Let $(A,\lambda,[\eta]^p)$ be an object in $\Lambda_{g,N}^{(p)}$, where $\eta\in\mathrm{GIsom}(V^{(p)}(\underline{A}_0),V^{(p)}(\underline{A}))$. Let $\zeta\in(\mathbb{A}_f^p)^\times$ such that $\eta^*\langle\,,\rangle_\lambda=\zeta\langle\,,\rangle_{\lambda_0}$. Choose a positive number $\alpha\in\mathbb{Z}_{(p)}^\times$ so that $\alpha\zeta\in(\hat{\mathbb{Z}}^{(p)})^\times$. Choose a prime-to-$p$ quasi-isogeny φ on A such that $\varphi^*\lambda=\alpha\lambda$. Then $(A,\lambda,[\eta]^p)\sim(A,\lambda,[\varphi\eta]^p)$. Replacing η by $\varphi\eta$, we may assume that $\zeta\in(\hat{\mathbb{Z}}^{(p)})^\times$. Let $L:=\eta(T^{(p)}(A_0))\subset V^{(p)}(A))$ be the image of $T^{(p)}(A_0)$ under η. By a theorem of Tate, there are a abelian variety A' and a prime-to-p quasi-isogeny $\varphi':A'\to A$ such that the map φ' induces an isomorphism

$$T^{(p)}(A')\xrightarrow{\varphi'}T^{(p)}(A)\simeq L\subset V^{(p)}(A);$$

the pair (A',φ') is uniquely determined up to isomorphism by this property. Let $\lambda':=\varphi'^*\lambda$, considered as an element in $\mathrm{Hom}(A',(A')^t)\otimes\mathbb{Z}_{(p)}$; one has $\langle\,,\rangle_{\lambda'}=\varphi'^*\langle\,,\rangle_\lambda$. We have the following diagram:

$$\begin{tikzcd}
& T^{(p)}(A_0),\zeta\langle\,,\rangle_{\lambda_0} \arrow[dl, "\varphi'^{-1}\eta"'] \arrow[d, "\eta"] \\
T^{(p)}(A'),\langle\,,\rangle_{\lambda'} \arrow[r, "\varphi'"] & L,\langle\,,\rangle_\lambda
\end{tikzcd}$$

It follows from $\varphi'^{-1}\circ\eta\in\mathrm{GIsom}(T^{(p)}(\underline{A}_0),T^{(p)}(\underline{A}))$ that λ' is a principal polarization. Then $(A,\lambda,[\eta]^p)\sim(A',\lambda',[\varphi'^{-1}\circ\eta]^p)$ and the latter comes from an element in $\Lambda^*_{g,N}$. This shows the surjectivity. It is obvious that the map f is compatible with the action of $\mathcal{G}$.

(2) We define the map $\mathbf{c}_N$. Given an object $(A,\lambda,[\eta]^p)$ in $\Lambda^{(p)}_{g,N}$, there is a prime-to-p quasi-isogeny $\varphi : A \to A_0$ such that $\varphi^*\lambda_0 = q\lambda$ for some $q \in \mathbb{Z}^\times_{(p),+}$. Then $[\varphi\eta]^p \in G(\mathbb{A}^p_f)/U^p_N$. If φ' is another such a morphism, the $\varphi' = a\varphi$ for some $a \in G(\mathbb{Z}_{(p)})$. Then the map $(A,\lambda,[\eta]^p) \mapsto [\varphi\eta]^p$ induces a well-defined map, denoted by $\mathbf{c}^p_N$, from $\Lambda^{(p)}_{g,N}$ to $G(\mathbb{Z}_{(p)})\backslash G(\mathbb{A}^p_f)/U^p_N$. Using the isomorphism $G(\mathbb{Z}_{(p)})\backslash G(\mathbb{A}^p_f)/U^p_N \simeq G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_N$, we get a map

$$\mathbf{c}_N : \Lambda^{(p)}_{g,N} \to G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_N.$$

We need to show that the map $\mathbf{c}^p_N$ is bijective and $\mathcal{G}$-equivariant. Let $\underline{A} = (A,\lambda,[\eta]^p)$ and $\underline{A}' = (A',\lambda',[\eta']^p)$ be two objects in $\Lambda^{(p)}_{g,N}$, and let φ, φ' be prime-to-p quasi-isogenies to A_0, respectively. Suppose that $[\varphi\eta]^p = [\varphi'\eta']^p$, that is $\mathbf{c}^p_N(\underline{A}) = \mathbf{c}^p_N(\underline{A}')$. Then the morphism $a := \varphi'^{-1}\varphi : A \to A'$ is a prime-to-p quasi-isogeny such that $a^*\lambda' \in \mathbb{Z}^\times_{(p),+}\lambda$ and $a_*[\eta]^p = [\eta']^p$. This shows the injectivity.

We show the surjectivity. Let $[\phi] \in G(\mathbb{Z}_{(p)})\backslash G(\mathbb{A}^p_f)/U^p_N$ be a class, where $\phi \in G(\mathbb{A}^p_f)$. Let $\zeta := \nu(\phi) \in (\mathbb{A}^p_f)^\times$. Replacing ϕ by $a\phi$ for a suitable $a \in G(\mathbb{Q})$, we may assume that $\zeta \in (\hat{\mathbb{Z}}^{(p)})^\times$. Let $L := \phi(T^{(p)}(A)) \subset V^{(p)}(A)$ be the image of $T^{(p)}(A)$ under ϕ. By a theorem of Tate, there exist an abelian variety A and a prime-to-p quasi-isogeny $\varphi : A \to A_0$ such that $\varphi : T^{(p)}(A) \simeq L \subset V^{(p)}(A)$. As φ is a prime-to-p quasi-isogeny, A is superspecial. Put $\lambda := \varphi^*\lambda_0$, considered as an element in $\mathrm{Hom}(A,A^t)\otimes\mathbb{Z}_{(p)}$. We have an isomorphism $\eta := \varphi^{-1}\phi : (T^{(p)}(A_0),\langle\, ,\rangle_{\lambda_0}) \simeq (T^{(p)}(A),\zeta\langle\, ,\rangle_\lambda)$. This shows that λ is a principal polarization. Then we get an object $(A,\lambda,[\eta]^p)$ and this is sent to the class $[\phi]$ by the construction.

We check the compatibility with the Galois action. Let $\phi \in G(\mathbb{A}^p_f)$ and $\underline{A} = (A,\lambda,[\eta]^p) \in \Lambda^{(p)}_{g,N}$ be the element such that $\mathbf{c}^p_N(\underline{A}) = [\phi]$. Then there exist an element $\varphi \in \mathrm{GIsog}^{(p)}_{\overline{\mathbb{F}}_p}(\underline{A},\underline{A}_0)$ and an element $\eta \in [\eta]^p$ such that $\phi = \varphi\circ\eta$. Applying any element σ in $\mathcal{G}$, we get

$$\sigma(\phi) \in \mathrm{GIsog}^{(p)}_{\overline{\mathbb{F}}_p}({}^\sigma\underline{A},\underline{A}_0), \quad \sigma(\eta) \in \mathrm{GIsom}(V^{(p)}(\underline{A}_0),V^{(p)}({}^\sigma\underline{A})),$$

and $\sigma(\phi) = \sigma(\varphi)\circ\sigma(\eta)$. This yields $\mathbf{c}^p_N({}^\sigma\underline{A}) = [\sigma(\phi)]$. ∎

Lemma 6.5. *Every member $(A,\lambda,\eta_N) \in \Lambda^*_{g,N}$ has a unique model (A',λ',η'_N), up to isomorphism, over $\mathbb{F}_{p^2}$ such that there exists a prime-to-p quasi-isogeny $\varphi : A' \to A_0\otimes\mathbb{F}_{p^2}$ such that $\varphi^*\lambda_0 \in \mathbb{Z}^\times_{(p),+}\cdot\lambda'$.*

Proof. By Proposition 5.1, (A,λ) has a unique model (A',λ') over $\mathbb{F}_{p^2}$ with the property. Since the Frobenius endomorphism $\pi_{A'}$ of A' over $\mathbb{F}_{p^2}$ is $-p$, the pull-back level structure η'_N is defined over $\mathbb{F}_{p^2}$. ∎

As Definition 5.2, we call the unique model over $\mathbb{F}_{p^2}$ in Lemma 6.5 the *canonical model* over $\mathbb{F}_{p^2}$. By Lemma 6.5, we may identify the set $\Lambda^*_{g,N}$ with the set of $\mathbb{F}_{p^2}$-isomorphism classes of superspecial g-dimensional principally polarized abelian varieties $\underline{A} = (A,\lambda,\eta_N)$ over $\mathbb{F}_{p^2}$ with level-N structure with respect to $\underline{A}_0$ such that the set $\mathrm{GIsog}^{(p)}_{\mathbb{F}_{p^2}}(\underline{A}, \underline{A}_0)$ is non-empty.

For any prime-to-p positive integers $N|M$, we have a natural projection $\Lambda^*_{g,M} \to \Lambda^*_{g,N}$. Let

$$\widetilde{\Lambda}^*_g := (\Lambda^*_{g,N})_{p\nmid N}$$

be the tower of all superspecial loci with prime-to-p level structures. Elements of $\widetilde{\Lambda}^*_g$ can be represented as $(A, \lambda, \widetilde{\eta})$, where (A, λ) is an element in Λ_g and $\widetilde{\eta} \in \mathrm{GIsom}(T^{(p)}(\underline{A}_0), T^{(p)}(\underline{A}))$ is a trivialization. It follows from Theorem 6.4 that the tower $\widetilde{\Lambda}^*_g$ admits a right action of $G(\mathbb{A}^p_f)$ and we have a natural isomorphism

$$\mathbf{d}^p : G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\mathbb{Z}_p) \simeq \widetilde{\Lambda}^*_g \tag{6.4}$$

of pointed profinite sets which is compatible with the actions of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ from the left, and of $G(\mathbb{A}^p_f)$ from the right.

6.3. The Hecke operator $R(\pi_0)$ and type number. We define the operator $R(\pi_0)$ and the type number with level structure, which are almost identical with those in Section 1.

Let $M_0(U_N)$ the vector space of functions $f : G(\mathbb{A}_f) \to \mathbb{C}$ satisfying $f(axu) = f(x)$ for all $a \in G(\mathbb{Q})$ and $u \in U_N$. Let $\mathcal{H}(G, U_N)$ be the Hecke algebra of bi-U_N-invariant functions, which acts on the space $M_0(U_N)$ in the same way as (1.5) but the Haar measure takes volume one on U_N. Let $R(\pi_0)$ be the operator corresponding to the double coset $U_N(\pi_0) := U_N\pi_0 = \pi_0 U_N$.

Let $\mathcal{T}_N$ be the double coset space

$$\mathcal{T}_N := G(\mathbb{Q})\backslash G(\mathbb{A}_f)/\mathfrak{N}_N,$$

where $\mathfrak{N}_N$ is the (open) subgroup of $G(\mathbb{A}_f)$ consisting of elements x such that

(1) $\mathrm{Int}(x)(\mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \hat{\mathbb{Z}}) = \mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes \hat{\mathbb{Z}}$, and
(2) the induced map

$$\mathrm{Int}(x) : \mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes (\mathbb{Z}/N\mathbb{Z}) \to \mathrm{End}(A_0 \otimes \overline{\mathbb{F}}_p) \otimes (\mathbb{Z}/N\mathbb{Z})$$

is the identity map.

It is not hard to show (see Lemma 5.6) that

$$\mathfrak{N}_N = D(\mathbb{Q}_p)G(\mathbb{Z}_p) \times Z(\mathbb{A}^p_f)U^p_N. \tag{6.5}$$

We call $\mathcal{T}_N$ the set of G-types with level U_N and the cardinality T_N of $\mathcal{T}_N$ the type number of the group G with level group U_N. Let $\mathbf{\Lambda}^*_{g,N}(\mathbb{F}_p) \subset \Lambda^*_{g,N}$ be the subset of the fixed points by σ_p.

Theorem 6.6.

(1) *Every member $(A, \lambda, \eta_N) \in \mathbf{\Lambda}^*_{g,N}(\mathbb{F}_p)$ has a model (A', λ', η'_N) defined over $\mathbb{F}_p$. Moreover, if $N \geq 3$, then the model (A', λ', η'_N) is unique up to isomorphism over $\mathbb{F}_p$ and the base change $(A', \lambda', \eta'_N) \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ is the canonical model over $\mathbb{F}_{p^2}$ of (A, λ, η_N).*
(2) *A member $(A, \lambda, \eta_N) \in \Lambda^*_{g,N}$ lies in $\mathbf{\Lambda}^*_{g,N}(\mathbb{F}_p)$ if and only if $G(\mathbb{Q}) \cap xU_N(\pi_0)x^{-1} \neq \emptyset$, where $[x] \in G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_N$ is the class corresponding to (A, λ, η_N).*
(3) *We have $\mathrm{tr}\, R(\pi_0) = |\Lambda^*_{g,N}(\mathbb{F}_p)|$.*
(4) *The natural map $\mathrm{pr} : \Lambda^*_{g,N} \to \mathcal{T}_N$ induces a bijection between the set of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-orbits of $\Lambda^*_{g,N}$ with the set $\mathcal{T}_N$.*

(5) *We have*

$$\operatorname{tr} R(\pi_0) = 2T_N - H_N,$$

where $H_N := |\Lambda^*_{g,N}|$ *is the class number of* G *with level group* U_N.

PROOF. (1) We may assume that $N \geq 2$ as the case $N = 1$ is treated in Section 5. By Lemma 6.5, we may assume that (A, λ, η_N) is the canonical model over $\mathbb{F}_{p^2}$ in its isomorphism class. Then its conjugation $({}^{\sigma_p}A, {}^{\sigma_p}\lambda, {}^{\sigma_p}\eta_N)$ is also a canonical model over $\mathbb{F}_{p^2}$ in its isomorphism class. By assumption, there exists an isomorphism $a_{\sigma_p} : (A, \lambda, \eta_N) \simeq ({}^{\sigma_p}A, {}^{\sigma_p}\lambda, {}^{\sigma_p}\eta_N)$ over $\mathbb{F}_{p^2}$, as they are canonical models over $\mathbb{F}_{p^2}$ in the same isomorphism class. Then $\sigma_p(a_{\sigma_p})a_{\sigma_p}$ is an automorphism of (A, λ, η) and is equal to ± 1 ($= 1$ if $N \geq 3$). Using the same argument as in Lemma 5.4, we define recursively $a_{\sigma_p^i} := \sigma_p(a_{\sigma_p^{i-1}})a_{\sigma_p}$ and show that the map $\sigma \mapsto a_\sigma$ satisfies the 1-cocycle condition for the field extension $\mathbb{F}_{p^4}/\mathbb{F}_p$ (for $\mathbb{F}_{p^2}/\mathbb{F}_p$ if $N \geq 3$). Then by Weil's theorem, there exist a model (A', λ', η'_N) over $\mathbb{F}_p$ and an isomorphism $b : (A', \lambda', \eta'_N) \simeq (A', \lambda', \eta'_N)$ over $\mathbb{F}_{p^4}$ (over $\mathbb{F}_{p^2}$ if $N \geq 3$) such that $a_{\sigma_p} = \sigma_p(b) \circ b^{-1}$. When $N \geq 3$, we have shown that this model is compatible with the canonical model over $\mathbb{F}_{p^2}$. The uniqueness follows from a theorem of Serre (cf. [23, Lemma p. 207]) that the automorphism group $\operatorname{Aut}(A, \lambda, \eta_N)$ is trivial.

The proofs for the statements (2), (3), (4) and (5) are the same as before. ∎

Remark 6.7.

(1) Similar to Remark 5.10, we discuss a bit about models over $\mathbb{F}_p$. Let $\boldsymbol{\Lambda}^{*,\mathrm{nc}}_{g,N}(\mathbb{F}_p) \subset \boldsymbol{\Lambda}^*_{g,N}(\mathbb{F}_p)$ denote the subset consisting of isomorphism classes for which a model $\underline{A}'$ over $\mathbb{F}_p$ can be chosen so that $\underline{A}' \otimes \mathbb{F}_{p^2}$ is the canonical model over $\mathbb{F}_{p^2}$. We have $\boldsymbol{\Lambda}^{*,\mathrm{nc}}_{g,N}(\mathbb{F}_p) \subset \boldsymbol{\Lambda}^*_{g,N}(\mathbb{F}_p)$ and $\boldsymbol{\Lambda}^{*,\mathrm{nc}}_{g,N}(\mathbb{F}_p) = \boldsymbol{\Lambda}^*_{g,N}(\mathbb{F}_p)$ if $N \geq 3$. We do not know whether this equality holds when $N \leq 2$.

(2) For $N \geq 3$, we have the following explicit formula (cf. Section 1)

$$H_N = |\operatorname{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})| \frac{(-1)^{g(g+1)/2}}{2^g} \left\{ \prod_{k=1}^{g} \zeta(1-2k) \right\} \cdot \prod_{k=1}^{g} \left\{ (p^k + (-1)^k \right\}. \tag{6.6}$$

6.4. Proof of Proposition 1.5. Let $(\mathbb{Z}^{2g}, \psi)$ be the standard symplectic $\mathbb{Z}$-module of rank $2g$, and let GSp_{2g} be the group of symplectic similitudes defined over $\mathbb{Z}$. Let $\mathcal{A}_{g,1,N}$ denote the moduli space over $\mathbb{F}_p$ of g-dimensional principally polarized abelian varieties (A, λ, α) with a (full) symplectic level-N structure. Recall that a full symplectic level-N structure on a g-dimensional principally polarized abelian scheme (A, λ) over a connected $\mathbb{F}_p$-scheme S is an isomorphism $\alpha : (\mathbb{Z}/N\mathbb{Z})^{2g} \simeq A[N](S)$ such that there is an element $\zeta \in \mu_N(S)$ such that

$$e_\lambda(\alpha(x), \alpha(y)) = \zeta\psi(x, y), \quad \forall\, x, y \in (\mathbb{Z}/N\mathbb{Z})^{2g}. \tag{6.7}$$

We denote by $\Lambda_{g,1,N} \subset \mathcal{A}_{g,1,N} \otimes \overline{\mathbb{F}}_p$ the superspecial locus. Put

$$H^p_f := \operatorname{GIsom}(((\mathbb{A}^p_f)^{2g}, \psi), V^{(p)}(\underline{A}_0)). \tag{6.8}$$

The set H^p_f is a $(G(\mathbb{A}^p_f), \operatorname{GSp}_{2g}(\mathbb{A}^p_f))$-bi-torsor together with an action of the Galois group $\mathcal{G} = \operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ from the left. The action of $\mathcal{G}$ on $T^{(p)}(A_0)$ gives rise to a Galois representation

$$\rho : \mathcal{G} \to G(\hat{\mathbb{Z}}^{(p)}).$$

Using Lemma 3.3 (3), the action of $\mathcal{G}$ on H^p_f is given as follows:

$$\sigma \cdot f = \rho(\sigma) \circ f, \quad \forall\, \sigma \in \mathcal{G}, f \in H^p_f. \tag{6.9}$$

Let $\widetilde{\mathcal{A}}^{(p)}_g := (\mathcal{A}_{g,1,N})_{p\nmid N}$ and $\widetilde{\Lambda}_g = (\Lambda_{g,1,N})_{p\nmid N}$ be as in Section 1. Elements in $\widetilde{\Lambda}_g$ can be represented as $(A, \lambda, \widetilde{\alpha})$, where $(A, \lambda) \in \Lambda_g$ and $\widetilde{\alpha} \in \mathrm{GIsom}(((\hat{\mathbb{Z}}^{(p)})^{2g}, \psi), T^{(p)}(\underline{A}))$.

Let $(A, \lambda, \widetilde{\alpha}) \in \widetilde{\Lambda}_g$ be an object. We can choose a quasi-isogeny $\varphi \in \mathrm{GIsog}^{(p)}_{\overline{\mathbb{F}}_p}(\underline{A}, \underline{A}_0)$. The composition $\varphi \circ \widetilde{\alpha}$

$$(\mathbb{A}^p_f)^{2g} \xrightarrow{\ \widetilde{\alpha}\ } V^{(p)}(A) \xrightarrow{\ \varphi\ } V^{(p)}(A_0)$$

defines a well-defined map

$$\mathbf{b}^p : \widetilde{\Lambda}_g \to G(\mathbb{Z}_{(p)})\backslash H^p_f, \quad (A, \lambda, \widetilde{\alpha}) \mapsto \varphi \circ \widetilde{\alpha}$$

which is compatible with the $\mathrm{GSp}_{2g}(\mathbb{A}^p_f)$-action. Using the same argument in the proof of Theorem 6.4, one shows that the map $\mathbf{b}^p$ is bijective and $\mathcal{G}$-equivariant.

If we fix a trivialization

$$\widetilde{\alpha}_0 \in \mathrm{GIsom}(((\hat{\mathbb{Z}}^{(p)})^{2g}, \psi), T^{(p)}(\underline{A}_0)),$$

then we get

- a Galois representation

$$\rho_0 : \mathcal{G} \to \mathrm{GSp}_{2g}(\hat{\mathbb{Z}}^{(p)})$$

  such that the following diagram

$$\begin{tikzcd} (\hat{\mathbb{Z}}^{(p)})^{2g} \arrow[r, "\widetilde{\alpha}_0"] \arrow[d, "\rho_0(\sigma)"] & T^{(p)}(A_0) \arrow[d, "\rho(\sigma)"] \\ (\hat{\mathbb{Z}}^{(p)})^{2g} \arrow[r, "\widetilde{\alpha}_0"] & T^{(p)}(A_0), \end{tikzcd} \tag{6.10}$$

  commutes,
- an isomorphism

$$j_0 : \mathrm{GSp}_{2g}(\mathbb{A}^p_f) \longrightarrow H^p_f, \quad \phi' \mapsto \widetilde{\alpha}_0 \circ \phi', \tag{6.11}$$

  and
- an isomorphism

$$i_0 : G(\mathbb{A}^p_f) \longrightarrow \mathrm{GSp}_{2g}(\mathbb{A}^p_f), \quad \phi \mapsto \widetilde{\alpha}_0^{-1} \circ \phi \circ \widetilde{\alpha}_0. \tag{6.12}$$

Let $\mathcal{G}$ act on $\mathrm{GSp}_{2g}(\mathbb{A}^p_f)$ by the action ρ_0. One checks that

$$\sigma \cdot j_0(\phi') = \sigma \cdot \widetilde{\alpha}_0 \circ \phi' = \rho(\sigma) \circ \widetilde{\alpha}_0 \circ \phi' = \widetilde{\alpha}_0 \circ \rho_0(\sigma)\phi'.$$

That is, the following diagram

$$\begin{tikzcd} \mathrm{GSp}_{2g}(\mathbb{A}^p_f) \arrow[r, "j_0"] \arrow[d, "\sigma"] & H^p_f \arrow[d, "\sigma"] \\ \mathrm{GSp}_{2g}(\mathbb{A}^p_f) \arrow[r, "j_0"] & H^p_f \end{tikzcd}$$

commutes. Therefore, we obtain an isomorphism (depending on the choice of $\widetilde{\alpha}_0$)

$$\mathbf{b}^p_0 : \widetilde{\Lambda}_g \simeq i_0(G(\mathbb{Z}_{(p)}))\backslash \mathrm{GSp}_{2g}(\mathbb{A}^p_f) \tag{6.13}$$

which is compatible with the $\mathrm{GSp}_{2g}(\mathbb{A}_f^p)$-action and the $\mathcal{G}$-action by ρ_0. This completes the proof of Proposition 1.5.

7. The non-principal genus case

In previous sections we investigate arithmetic properties of *principally polarized* superspecial abelian varieties, as well as the relationship to the trace of certain Hecke operator on the space of automorphic forms of weight zero. These abelian varieties correspond to the principal genus of the group G. Since the non-principal genus case is of equal importance (see Section 7.1), we include the analogous results for these superspecial abelian varieties as well. The proofs of most results are the same as the principal genus case and are omitted.

7.1. The class numbers $H_n(p,1)$ and $H_n(1,p)$. We start with the arithmetic aspect of polarized superspecial abelian varieties which are related to components of the supersingular locus of $\mathcal{A}_g\otimes\overline{\mathbb{F}}_p$, the coarse moduli space over $\overline{\mathbb{F}}_p$ of g-dimensional principally polarized abelian varieties. Our references are Ibukiyama-Katsura-Oort [13, Section 2] and Li-Oort [21, Section 4].

Let B be the quaternion algebra over $\mathbb{Q}$ ramified exactly at $\{p,\infty\}$, and let $\mathcal{O}$ be a maximal order of B. Put $V=B^{\oplus n}$, regarded as a left B-module of row vectors, and let $\psi(x,y)=\sum_{i=1}^n x_i\bar{y}_i$ be the standard Hermitian form on V, where the map $y_i\mapsto \bar{y}_i$ is the canonical involution on B. Let G be the algebraic group of ψ-similitudes over $\mathbb{Q}$; the group of $\mathbb{Q}$-points of G is

$$G(\mathbb{Q}):=\{h\in M_n(B)\,|\,h\bar{h}^t=rI_n \text{ for some } r\in\mathbb{Q}^\times\}.$$

(Note that the group G here is isomorphic to the generic fiber $G_{\mathbb{Q}}$ of the group scheme G over $\operatorname{Spec}\mathbb{Z}$ defined in Introduction when $n=g$. Thus, we use the same notation.)

Two $\mathcal{O}$-lattices L and L' in $B^{\oplus n}$ are called *globally equivalent* (denoted by $L\sim L'$) if $L'=Lh$ for some element $h\in G(\mathbb{Q})$. For any finite place v of $\mathbb{Q}$, we write $B_v:=B\otimes\mathbb{Q}_v$, $\mathcal{O}_v:=\mathcal{O}\otimes\mathbb{Z}_v$ and $L_v:=L\otimes\mathbb{Z}_v$. Two $\mathcal{O}$-lattices L and L' in $B^{\oplus n}$ are called *locally equivalent at v* (denoted by $L_v\sim L'_v$) if $L'_v=L_vh_v$ for some element $h_v\in G(\mathbb{Q}_v)$. A *genus* of $\mathcal{O}$-lattices is a maximal set of (global) $\mathcal{O}$-lattices in $B^{\oplus n}$ which are equivalent to each other locally at every finite place v.

We define an $\mathcal{O}_p$-lattice $N_p\subset B_p^{\oplus n}$ as follows:

$$N_p:=\mathcal{O}_p^{\oplus n}\cdot\begin{pmatrix} I_r & 0\\ 0 & \pi I_{n-r}\end{pmatrix}\cdot\xi\subset B_p^{\oplus n},$$

where r is the integer $[n/2]$, π is a uniformizer in $\mathcal{O}_p$, and ξ is an element in $\mathrm{GL}_n(B_p)$ such that

$$\xi\bar{\xi}^t=\text{anti-diag}(1,1,\dots,1).$$

Definition 7.1.

(1) Let $\mathcal{L}_n(p,1)$ denote the set of $\mathcal{O}$-lattices L in $B^{\oplus n}$ such that $L_v\sim\mathcal{O}_v^{\oplus n}$ at every finite place v. The set $\mathcal{L}_n(p,1)$ is called the *principal genus*. Let $\mathcal{L}_n(p,1)/\!\sim$ denote the set of global equivalence classes in $\mathcal{L}_n(p,1)$. As a well-known fact, $\mathcal{L}_n(p,1)/\!\sim$ is a finite set. The cardinality $H_n(p,1):=\#\mathcal{L}_n(p,1)/\!\sim$ is called the *class number* of the principal genus.

(2) Let $\mathcal{L}_n(1,p)$ denote the set of $\mathcal{O}$-lattices L in $B^{\oplus n}$ such that $L_p\sim N_p$ and $L_v\sim\mathcal{O}_v^{\oplus n}$ at every finite place $v\neq p$. The set $\mathcal{L}_n(1,p)$ is called the *non-principal*

genus. Let $\mathcal{L}_n(1,p)/\sim$ denote the set of global equivalence classes in $\mathcal{L}_n(1,p)$. Similarly, $\mathcal{L}_n(1,p)/\sim$ is a finite set, and its cardinality, called the *class number* of the non-principal genus, is denoted by $H_n(1,p)$.

Recall that Λ_g is the set of isomorphism classes of g-dimensional principally polarized superspecial abelian varieties over $\overline{\mathbb{F}}_p$. When $g = 2d > 0$ is even, we denote by Σ_g the set of isomorphism classes of g-dimensional polarized superspecial abelian varieties (A,λ) of degree $\deg\lambda = p^{2d}$ over $\overline{\mathbb{F}}_p$ satisfying $\ker\lambda = A[F]$. Here F is the relative Frobenius morphism $A \to A^{(p)}$ over $\overline{\mathbb{F}}_p$.

Let $\mathcal{S}_g$ denote the supersingular locus of the Siegel moduli space $\mathcal{A}_g \otimes \overline{\mathbb{F}}_p$; it is a closed reduced subscheme of finite type over $\overline{\mathbb{F}}_p$. Let $\Pi_0(\mathcal{S}_g)$ denote the set of irreducible components of $\mathcal{S}_g$.

Theorem 7.2 (Li-Oort [21])**.** *We have*

$$\Pi_0(\mathcal{S}_g) \simeq \begin{cases} \Lambda_g & \text{if } g \text{ is odd;} \\ \Sigma_g & \text{if } g = 2d \text{ is even.} \end{cases}$$

The arithmetic aspect for the supersingular locus $\mathcal{S}_g$ is given by the following proposition.

Proposition 7.3.
(1) *For any positive integer g, one has $|\Lambda_g| = H_g(p,1)$.*
(2) *For any even positive integer $g = 2d$, one has $|\Sigma_g| = H_g(1,p)$.*

Proof. (1) See [13, Theorem 2.10]. (2) See [21, Proposition 4.7].

7.2. In the remainder of this section, let $g = 2d$ be an even positive integer. Suppose that there exists a g-dimensional superspecial polarized abelian variety $\underline{A}'_0 = (A'_0, \lambda'_0)$ over $\mathbb{F}_p$ such that the polarization degree is p^{2d},

$$\ker\lambda'_0 = A'_0[F], \quad \text{and} \quad (\pi'_0)^2 = -p, \tag{7.1}$$

where π'_0 is the Frobenius endomorphism of A'_0. The existence of such an object may depend on p and g; for example it exists if $\left(\frac{-1}{p}\right) = 1$ or $4|g$; see [41, Lemmas 3.1 and 3.2]. Nevertheless we fix one when it exists. Let $G'_1 \subset G'$ be the automorphism group schemes over $\operatorname{Spec}\mathbb{Z}$ associated to the object (A'_0, λ'_0), defined similarly as in Section 4.1. Let N be a positive *prime-to-p* integer, and let U'_N be the kernel of the reduction map $G'(\hat{\mathbb{Z}}) \to G'(\mathbb{Z}/N\mathbb{Z})$. The generic fiber $G'_{\mathbb{Q}}$ of G' is isomorphic to $G_{\mathbb{Q}}$, so we can also consider U'_N as an open compact subgroup of $G(\mathbb{A}_f)$.

Denote by $\Sigma^*_{g,N}$ the set of isomorphism classes of objects (A,λ,η_N) over $\overline{\mathbb{F}}_p$, where (A,λ) is an object in Σ_g and η_N is a level-N structure on (A,λ) with respect to $\underline{A}'_0$ (defined in the same way as in Section 6.1).

The Galois group $\mathcal{G} = \operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ acts naturally on the topological group $G'(\mathbb{A}_f)$ and this action is given by (cf. Theorem 1.1)

$$\sigma_p(x_\ell)_\ell = (\pi'_0 x_\ell {\pi'_0}^{-1})_\ell, \quad (x_\ell)_\ell \in G'(\mathbb{A}_f). \tag{7.2}$$

Theorem 7.4. *There is a natural $\mathcal{G}$-equivariant bijective map*

$$\mathbf{c}'_N : \Sigma^*_{g,N} \to G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/U'_N$$

for which the base point $(A'_0, \lambda'_0, \mathrm{id})$ is sent to the identity class [1].

PROOF. This is the analogue of Theorem 6.4. The proof is the same and is omitted. ∎

Lemma 7.5. *Every member $(A,\lambda,\eta_N)\in\Sigma^*_{g,N}$ has a unique model (A',λ',η'_N), up to isomorphism, over $\mathbb{F}_{p^2}$ such that there exists a prime-to-p quasi-isogeny $\varphi: A'\to A'_0\otimes\mathbb{F}_{p^2}$ such that $\varphi^*\lambda'_0\in\mathbb{Z}^\times_{(p),+}\cdot\lambda'$.*

PROOF. This is the analogue of Lemma 6.5. The proof is the same and is omitted. ∎

Let $\widetilde{\Sigma}^*_g := (\Sigma^*_{g,N})_{p\nmid N}$ the tower of the superspecial loci $\Sigma^*_{g,N}$; it admits a right action of $G'(\mathbb{A}^p_f)$. By Theorem 7.4, one has a natural isomorphism

$$\mathbf{d}'^p : G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/G'(\mathbb{Z}_p)\simeq\widetilde{\Sigma}^*_g \tag{7.3}$$

of pointed profinite sets which is compatible with the actions of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ and of $G'(\mathbb{A}^p_f)$.

As in Section 6.3, et $R(\pi'_0)$ be the operator corresponding to the double coset $U'_N(\pi'_0):=U'_N\pi'_0=\pi'_0U'_N$ on the space $M_0(U'_N)$ of automorphic forms of level U'_N. Let $\mathcal{T}'_N$ be the set of G'-types with level U'_N, and call $T'_N:=|\mathcal{T}'_N|$ the type number of the group G' with level group U'_N. Let $\mathbf{\Sigma}^*_{g,N}(\mathbb{F}_p)\subset\Sigma^*_{g,N}$ be the subset of fixed points of the Frobenius map σ_p.

Theorem 7.6.

(1) *Every member $(A,\lambda,\eta_N)\in\mathbf{\Sigma}^*_{g,N}(\mathbb{F}_p)$ has a model (A',λ',η'_N) defined over $\mathbb{F}_p$. Moreover, if $N\ge 3$, then the model (A',λ',η'_N) is unique up to isomorphism over $\mathbb{F}_p$ and the base change $(A',\lambda',\eta'_N)\otimes_{\mathbb{F}_p}\mathbb{F}_{p^2}$ is the canonical model over $\mathbb{F}_{p^2}$ of (A,λ,η_N).*
(2) *A member $(A,\lambda,\eta_N)\in\Sigma^*_{g,N}$ lies in $\mathbf{\Sigma}^*_{g,N}(\mathbb{F}_p)$ if and only if $G'(\mathbb{Q})\cap xU'_N(\pi'_0)x^{-1}\ne\emptyset$, where $[x]\in G'(\mathbb{Q})\backslash G'(\mathbb{A}_f)/U'_N$ is the class corresponding to (A,λ,η_N).*
(3) *We have $\mathrm{tr}\,R(\pi'_0)=|\mathbf{\Sigma}^*_{g,N}(\mathbb{F}_p)|$.*
(4) *The natural map $\mathrm{pr}:\Sigma^*_{g,N}\to\mathcal{T}'_N$ induces a bijection between the set of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-orbits of $\Sigma^*_{g,N}$ with the set $\mathcal{T}'_N$.*
(5) *We have*

$$\mathrm{tr}\,R(\pi'_0)=2T'_N-H'_N, \tag{7.4}$$

where $H'_N=|\Sigma^*_{g,N}|$ is the class number of G' with level group U'_N.

PROOF. This is the analogue of Theorem 6.6. The proof is the same and is omitted. ∎

For $N\ge 3$, we have the following explicit formula (see [38, Theorem 6.6]; note that in [38] one fixes a choice of a primitive Nth root of unity ζ_N.)

$$H'_N=|\,\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})|\frac{(-1)^{g(g+1)/2}}{2^g}\left\{\prod_{k=1}^{g}\zeta(1-2k)\right\}\cdot\prod_{k=1}^{d}(p^{4k-2}-1). \tag{7.5}$$

Remark 7.7. Our results in this section rely on the existence of a base point (A'_0,λ'_0) with property (7.1). We do not know whether such a base point always exists. However, for Theorem 7.4 and Lemma 7.5, we only need the existence of a base point (A_0', λ_0') which is defined over $\mathbb{F}_p$, i.e. $\mathbf{\Sigma}_g(\mathbb{F}_p) \neq \emptyset$. For Theorem 7.6, we only require in addition that its Frobenius endomorphism π_0' is square central in $G'(\mathbb{Q})$.

8. Trace formula for groups of compact type

The goal of this section is to calculate the trace of the Hecke operator $R(\pi_0)$ (or $R(\pi_0'))$ for the groups G (or G') arising from the previous sections using the Selberg trace formula. Since one has explicit formulas for the class numbers H_N and H_N' (see (6.6) and (7.5)), Theorems 6.6 and 7.6 would provide information for the type numbers T_N and T_N'. For other possible applications, we work on slightly more general groups and study the trace of specific Hecke operators. The majority of this section (up to Subsection 8.5) is independent from the previous sections; some notations are different.

8.1. Hecke operators $R(\pi)$. Let G be a connected reductive group over $\mathbb{Q}$ such that $G(\mathbb{Q})$ is a discrete subgroup of $G(\mathbb{A}_f)$. We know that $G(\mathbb{Q})$ is discrete in $G(\mathbb{A}_f)$ if and only the quotient space $G(\mathbb{Q})\backslash G(\mathbb{A}_f)$ is compact; see [8, Proposition 1.4] for more equivalent conditions.

We fix a $\mathbb{Z}$-structure on G. For simplicity, we assume that this $\mathbb{Z}$-structure is induced by a rational faithful representation $\rho : G \to \mathrm{GL}_m$ of G. For any positive integer N, one defines an open compact subgroup U_N as the kernel of the reduction map

$$\mathrm{Red}_N : G(\hat{\mathbb{Z}}) \to G(\mathbb{Z}/N\mathbb{Z}) \subset \mathrm{GL}_m(\mathbb{Z}/N\mathbb{Z}).$$

Denote by $L^2(G) = L^{2,\infty}(G(\mathbb{Q})\backslash G(\mathbb{A}_f))$ the vector space of locally constant $\mathbb{C}$-valued functions on $G(\mathbb{Q})\backslash G(\mathbb{A}_f)$, endowed with an inner product defined by

$$\langle f, g\rangle := \int_{G(\mathbb{Q})\backslash G(\mathbb{A}_f)} f(x)\overline{g(x)}dx,$$

for a Haar measure dx on $G(\mathbb{A}_f)$ which we shall specify later. This is a pre-Hilbert space as the limit of locally constant functions need not to be locally constant. For example, the limit of the sequence of characteristic functions $\mathbf{1}_{G(\mathbb{Q})U_n}$ for a decreasing separated sequence of open compact subgroups U_n is the delta function $\delta_{[1]}$ supported on the identity class [1].

The group $G(\mathbb{A}_f)$ acts on the space $L^2(G)$ by right translation, denoted by R. Since the topological space $G(\mathbb{Q})\backslash G(\mathbb{A}_f)$ is compact, every function f in $L^2(G)$ is invariant under an open subgroup $U \subset G(\mathbb{A}_f)$, that is, f is a smooth vector. Also for any open compact subgroup U, the invariant subspace

$$L^2(G)^U = L^{2,\infty}(G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U) = \mathcal{C}(G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U)$$

consisting of constant functions on the finite set $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U$ is finite-dimensional. In other words, the representation $L^2(G)$ of $G(\mathbb{A}_f)$ is admissible. Denote by $\mathcal{H}(G)$ the Hecke algebra of $\mathbb{C}$-valued, locally constant, compactly supported functions on $G(\mathbb{A}_f)$; the multiplication is given by the convolution. The Hecke algebra $\mathcal{H}(G)$ acts on the space $L^2(G)$ as follows: For $\varphi \in \mathcal{H}(G)$, $f \in L^2(G)$,

$$R(\varphi)f(x) := \int_{G(\mathbb{A}_f)} \varphi(y)R(y)f(x)dx = \int_{G(\mathbb{A}_f)} \varphi(y)f(xy)dx.$$

Fix an element π of $G(\mathbb{Q})$ which normalizes U_N for all N. For example, if π normalizes U_{p^m} for all powers of a prime p and $\pi \in G(\hat{\mathbb{Z}}^{(p)})$, then π satisfies this property. Let $\varphi_{\pi,N}$ be the characteristic function of the double coset $U_N\pi U_N = \pi U_N = U_N\pi$ and we write $R_N(\pi) = R(\varphi_{\pi,N})$, where N is a positive integer. The goal is to calculate the trace of the Hecke operator $R_N(\pi)$. Here we normalize the Haar measure so that it takes volume one on the open compact subgroup U_N. The meaning of the trace $\operatorname{tr} R_N(\pi)$ can be interpreted as the number of fixed points in the double coset space $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_N$ under the translation $[x] \mapsto [x\pi]$. Note that the translation is well-defined as π normalizes U_N. Indeed, the image of $R_N(\pi)$ is contained in the U_N-invariant subspace $\mathcal{C}(G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_N)$. So $\operatorname{tr} R_N(\pi)$ is equal to the trace of its restriction

$$R_N(\pi) : \mathcal{C}(G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_N) \to \mathcal{C}(G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_N).$$

This map is induced by the translation $[x] \mapsto [x\pi]$ and hence its trace is equal to the number of fixed points.

To simplify notation we shall write φ_π for $\varphi_{\pi,N}$ and $R(\pi)$ for $R_N(\pi)$, respectively, keeping in mind that these also depend on N.

8.2. Trace of $R(\pi)$. The standard argument in the theory of trace formulas (cf. [6]) shows that the operator $R(\pi)$ is of trace class and its trace can be calculated by the following integral

$$\operatorname{tr} R(\pi) = \int_{G(\mathbb{Q})\backslash G(\mathbb{A}_f)} K_\pi(x,x)dx,$$

where

$$K_\pi(x,y) := \sum_{\gamma\in G(\mathbb{Q})} \varphi_\pi(x^{-1}\gamma y).$$

Note that when x and y vary in a fixed open compact subset, there are only finitely many non-zero terms in the sum of $K_\pi(x,y)$. Regrouping the terms in the standard way (cf. [6]), we get

$$\operatorname{tr} R(\pi) = \sum_{\gamma\in G(\mathbb{Q})/\sim} a(G_\gamma)O_\gamma(\varphi_\pi), \tag{8.1}$$

where

- $G(\mathbb{Q})/\sim$ denotes the set of conjugacy classes of $G(\mathbb{Q})$,
- G_γ denotes the centralizer of γ in G, and
- $a(G_\gamma) := \operatorname{vol}(G_\gamma(\mathbb{Q})\backslash G_\gamma(\mathbb{A}_f))$, and

$$O_\gamma(\varphi_\pi) := \int_{G_\gamma(\mathbb{A}_f)\backslash G(\mathbb{A}_f)} \varphi_\pi(x^{-1}\gamma x)\frac{dx}{dx_\gamma}, \tag{8.2}$$

where dx_γ is a Haar measure on $G_\gamma(\mathbb{A}_f)$.

Note that the whole term $a(G_\gamma)O_\gamma(\varphi_\pi)$ does not depend on the choice of the Haar measure dx_γ. As the closed subgroup $G_\gamma(\mathbb{A}_f)$ is unimodular, the right $G(\mathbb{A}_f)$-invariant Radon measure dx/dx_r is defined and it is characterized by the following property:

$$\int_{G(\mathbb{A}_f)} f dx = \int_{G_\gamma(\mathbb{A}_f)\backslash G(\mathbb{A}_f)} \int_{G_\gamma(\mathbb{A}_f)} f(x_\gamma x)dx_\gamma \frac{dx}{dx_\gamma} \tag{8.3}$$

for all functions $f \in C_o^\infty(G(\mathbb{A}_f))$. Using this formula, one easily shows that

$$\operatorname{vol}_{dx/dx_\gamma}(G_\gamma(\mathbb{A}_f)\backslash G_\gamma(\mathbb{A}_f)U) = \frac{\operatorname{vol}_{dx}(U)}{\operatorname{vol}_{dx_\gamma}(G_\gamma(\mathbb{A}_f)\cap U)} \tag{8.4}$$

for any open compact subgroup $U \subset G(\mathbb{A}_f)$, or more generally,

$$\mathrm{vol}_{dx/dx_\gamma}(G_\gamma(\mathbb{A}_f)\backslash G_\gamma(\mathbb{A}_f)aU) = \frac{\mathrm{vol}_{dx}(U)}{\mathrm{vol}_{dx_\gamma}(G_\gamma(\mathbb{A}_f) \cap aUa^{-1})} \tag{8.5}$$

for any element $a \in G(\mathbb{A}_f)$; see Kottwitz [19, Section 2.4]. In our situation, any element $\gamma \in G(\mathbb{Q})$ is semi-simple. Therefore, any $G(\mathbb{A}_f)$-conjugacy class is closed and the orbital integral $O_\gamma(\varphi_\pi)$ is a finite sum.

For elements x and γ in $G(\mathbb{Q})$ (resp. in $G(\mathbb{Q}_v)$ or in $G(\mathbb{A}_f)$), we write $x \cdot \gamma = x^{-1}\gamma x$, the conjugation of γ by x. Put

$$\Delta_N := \{\gamma \in G(\mathbb{Q}) \,|\, G(\mathbb{A}_f) \cdot \gamma \cap \pi U_N \neq \emptyset\}/\sim_{G(\mathbb{Q})} . \tag{8.6}$$

We show that Δ_N is a finite set.

Let $C \subset G(\mathbb{A}_f)$ be an open compact subset such that $G(\mathbb{A}_f) = G(\mathbb{Q})C$. For example, if we write $G(\mathbb{A}_f)$ as a finite disjoint union of double coset:

$$G(\mathbb{A}_f) := \coprod_{i=1}^{h} G(\mathbb{Q})c_i U_1,$$

then take C to be the union of $c_i U_1$ for $i = 1, \dots, h$. Put

$$X_N := \bigcup_{c \in C} c^{-1} \cdot \pi U_N.$$

Since X_N is an image of the compact set $C \times \pi U_N$, it is compact. If γ is an element of $G(\mathbb{Q})$ which lies in $G(\mathbb{A}_f) \cdot \pi U_N$, then there exists an element $a \in G(\mathbb{Q})$ such that $a \cdot \gamma \in X_N$. The element $a \cdot \gamma$ lies in the intersection $G(\mathbb{Q}) \cap X_N$, which is a finite set. Since Δ_N consists of elements γ as above modulo the $G(\mathbb{Q})$-conjugation, the set Δ_N is finite.

For each class $\bar\gamma \in \Delta_N$, we select a representative γ in $X_N \cap G(\mathbb{Q})$ and choose the Haar measure dx_γ so that

$$\mathrm{vol}(U_{\gamma,N}) = 1, \quad \text{where } U_{\gamma,N} := G_\gamma(\mathbb{A}_f) \cap U_N. \tag{8.7}$$

Put

$$\mathcal{E}_\gamma := \{x \in G(\mathbb{A}_f) \,|\, x^{-1}\gamma x \in \pi U_N\},$$

which is the support of the function $\phi_\gamma(x) := \varphi_\pi(x^{-1}\gamma x)$. It is clear that $\mathcal{E}_\gamma$ is stable under the left $G_\gamma(\mathbb{A}_f)$-action and the right U_N-action. By our choice of Haar measures on $G(\mathbb{A}_f)$ and $G_\gamma(\mathbb{A}_f)$, the orbital integral $O_\gamma(\varphi_\pi)$ can be calculated using the formula (see (8.5))

$$O_\gamma(\varphi_\pi) = \sum_{[a] \in G_\gamma(\mathbb{A}_f)\backslash \mathcal{E}_\gamma / U_N} \mathrm{vol}(G_\gamma(\mathbb{A}_f) \cap aUa^{-1})^{-1}.$$

We have shown the following result.

Proposition 8.1. *Let $\Delta_N \subset G(\mathbb{Q})/\sim$ be the subset of $G(\mathbb{Q})$-conjugacy classes defined in* (8.6).

(1) *The set Δ_N is finite.*
(2) *We have*

$$\mathrm{tr}\, R(\pi) = \sum_{\bar\gamma \in \Delta_N} a(G_\gamma) O_\gamma(\varphi_\pi) \tag{8.8}$$

and

$$O_\gamma(\varphi_\pi) = \sum_{[a]\in G_\gamma(\mathbb{A}_f)\backslash \mathcal{E}_\gamma/U_N} \mathrm{vol}(G_\gamma(\mathbb{A}_f)\cap aUa^{-1})^{-1}. \tag{8.9}$$

8.3. Trace of $R(\pi)$ with U_N small. Put

$$\Delta_f(\pi) := \{\gamma \in G(\mathbb{Q})\,|\gamma \in G(\mathbb{A}_f)\cdot \pi\}/\sim_{G(\mathbb{Q})} .$$

Clearly we have $\Delta_f(\pi) \subset \Delta_N$.

Lemma 8.2. *There exists a positive integer N_0 such that for all positive integers N divisible by N_0, we have $\Delta_N = \Delta_f(\pi)$.*

Proof. Since $G(\mathbb{Q})\cap X_N$ is finite, there is a positive integer N_0 such that $G(\mathbb{Q})\cap X_N$ remains the same for all N with $N_0|N$. Let γ be an element in $G(\mathbb{Q})\cap X_N$. Then for all n with $N_0|n$, we have $\gamma = c_n\pi u_n c_n^{-1}$ for some $c_n \in C$ and $u_n \in U_n$. Since C is compact, there is a subsequence $\{c_{m_i}\}$ of $\{c_n\}$ which converges to an element $c_0 \in C$. As $i \to \infty$, we get $\gamma = c_0\pi c_0^{-1}$. This shows the lemma. ∎

Suppose an element $\gamma \in G(\mathbb{Q})$ has the form $y^{-1}\pi y$ for some $y \in G(\mathbb{A}_f)$. We show that the term $a(G_\gamma)O_\gamma(\varphi_\pi)$ in (8.8) is equal to $a(G_\pi)O_\pi(\varphi_\pi)$. First, it is easy to show that an element $x \in G(\mathbb{Q})$ lies in $G_\gamma(\mathbb{Q})$ if and only if $yxy^{-1} \in G_\pi(\mathbb{Q})$; thus $yG_\gamma(\mathbb{Q})y^{-1} = G_\pi(\mathbb{Q})$. Let $t = yx$. The map $x \mapsto t$ induces an homeomorphism

$$G_\gamma(\mathbb{Q})\backslash G(\mathbb{A}_f) \simeq G_\pi(\mathbb{Q})\backslash G(\mathbb{A}_f).$$

We have

$$\begin{aligned} a(G_\gamma)O_\gamma(\varphi_\pi) &= \int_{G_\gamma(\mathbb{Q})\backslash G(\mathbb{A}_f)} \varphi_\pi(x^{-1}y^{-1}\pi yx)dx \\ &= \int_{G_\pi(\mathbb{Q})\backslash G(\mathbb{A}_f)} \varphi_\pi(t^{-1}\pi t)dt = a(G_\pi)O_\pi(\varphi_\pi). \end{aligned} \tag{8.10}$$

Lemma 8.2 and the equality (8.10) show that when U_N is small, the trace of the Hecke operator $R(\pi)$ can be simplified significantly.

Proposition 8.3. *There exists a positive integer N_0 such that for all positive integers N divisible by N_0, we have*

$$\mathrm{tr}\, R(\pi) = |\Delta_f(\pi)|\, a(G_\pi)\, O_\pi(\varphi_\pi) \tag{8.11}$$

Remark 8.4. Using either the results of G. Prasad [25] on the volumes of fundamental domains or the results of Shimura [30] on the exact mass formulas, one can determine the term $a(G_\pi)$ explicitly. The orbital integral $O_\pi(\varphi_\pi)$ is purely local in nature, that is, it is expressed as the product of the local orbital integrals $O_\pi(\varphi_{\pi,v})$. There is also a similar local description as in (8.9). Using this description, it is not hard to show that the local integral integral $O_\pi(\varphi_{\pi,v})$ is equal to 1 for almost all finite places. We were wondering whether after shrinking the level subgroups U_N at these bad places, each local orbital integral in bad places becomes 1 or becomes an easily computable term. Nevertheless, we continue to study the global term $|\Delta_f(\pi)|$.

8.4. A cohomological meaning for $\Delta_f(\pi)$. Put

$$\Delta(\pi) := \{\gamma \in G(\mathbb{Q}) \,|\, \gamma \in G(\mathbb{A}) \cdot \pi\}/ \sim_{G(\mathbb{Q})} .$$

Lemma 8.5. *Let G be a connected reductive group over $\mathbb{R}$ such that the derived subgroup G_{der} is anisotropic. Then for any two elements x and y in $G(\mathbb{R})$, x and y are $G(\mathbb{R})$-conjugate if and only if they are $G(\mathbb{C})$-conjugate.*

PROOF. We first show the case where $G(\mathbb{R})$ is compact. Choose an anisotropic maximal torus T. Then any element can be $G(\mathbb{R})$-conjugate to an element in $T(\mathbb{R})$. Any two elements in $T(\mathbb{R})$ are conjugate if and only if they are in the same W_T-orbit, where W_T is the Weyl group of G relative to T. Two elements in $T(\mathbb{R})$ are $G(\mathbb{C})$-conjugate if and only if they are in the same $W_{T_\mathbb{C}}$-orbit, where $W_{T_\mathbb{C}}$ is the Weyl group of $G_\mathbb{C}$ relative to $T_\mathbb{C}$. From our compactness assumption of $G(\mathbb{R})$, one has $W_T \simeq W_{T_\mathbb{C}}$. The statement then follows from the injectivity of the map $T(\mathbb{R})/W_T \hookrightarrow T(\mathbb{C})/W_{T_\mathbb{C}}$.

We reduce to the above special case. Let Z be the connected center of G. Let $S \subset Z$ (resp. $T \subset Z$) be the maximal split (resp. anisotropic) torus of Z. Put $M := G_{\text{der}} \cdot T \cdot S[2]$, where $S[2]$ is the 2-torsion subgroup of S. One has $G = SM = SM^0$ and the subgroup $M(\mathbb{R})$ meets every component of $G(\mathbb{R})$. We also have $G(\mathbb{R}) = M(\mathbb{R}) \times S(\mathbb{R})^0$; write $x = (x_M, x_S)$ into the M-component and S-component of x. Then two elements x and y are $G(\mathbb{C})$-conjugate if and only if $x_S = y_S$, and x_M and y_M are $M(\mathbb{C})$-conjugate. The condition that x_M and y_M are $M(\mathbb{C})$-conjugate implies that they are in the same connected component of $M(\mathbb{R})$. Multiplying them by a suitable element in $S[2]$, we may assume that x_M and y_M are in the connected component $M^0(\mathbb{R})$. Since M^0 is connected and anisotropic, we are done. ∎

Lemma 8.6. *We have $\Delta_f(\pi) = \Delta(\pi)$.*

PROOF. We have the inclusion $\Delta(\pi) \subset \Delta_f(\pi)$, and need to show that if $\gamma G(\mathbb{Q}) \cap G(\mathbb{A}_f) \cdot \pi$, then $\gamma G(\mathbb{Q}) \cap G(\mathbb{A}) \cdot \pi$, that is, γ and π are $G(\mathbb{R})$-conjugate. Since the set of $G(\bar{K})$-conjugacy classes is independent of the algebraically closed field $\bar{K}$ of characteristic zero, one immediately sees that γ and π are $G(\mathbb{C})$-conjugate, and the lemma follows from Lemma 8.5. ∎

Lemma 8.7. *There is a natural bijection*

$$\Delta(\pi) \simeq \ker\left[\ker^1(\mathbb{Q}, G_\pi) \to H^1(\mathbb{Q}, G)\right], \tag{8.12}$$

where $\ker^1(\mathbb{Q}, G_\pi)$ *is the kernel of the local-global map*

$$H^1(\mathbb{Q}, G_\pi) \to \prod_v H^1(\mathbb{Q}_v, G_\pi)$$

of pointed sets.

PROOF. This is a special case of a well-known ingredient in the stabilization of the trace formula; see [17, (9.6.2)]. The proof is elementary and omitted. ∎

8.5. Application to the superspecial locus. Let G, $\pi_0 \in G(\mathbb{Q})$, U_N and $R_N(\pi_0) = R(\pi_0)$ be those in Section 6, also see Theorem 6.6. In this subsection, we apply results of previous subsections for computing the trace $\operatorname{tr} R(\pi_0)$. Note that this computes the number of $\mathbb{F}_p$-rational points of $\Lambda^*_{g,N}$ (see Theorem 6.6 (3) and Remark 8.10). The centralizer G_{π_0} is isomorphic to the group of unitary similitudes of a Hermitian space V over the imaginary quadratic field $\mathbb{Q}(\pi_0) = \mathbb{Q}(\sqrt{-p})$. This group G_{π_0} satisfies the Hasse principle; see a proof below.

Lemma 8.8. *Let E be an imaginary quadratic field and $G = GU(V, \psi)$ be the group of unitary similitudes of a Hermitian space V over E. Then G satisfies the Hasse principle.*

PROOF. This is certainly known to the experts. We indicate how this follows from a result of Kottwitz. Consider the short exact sequence

$$1 \longrightarrow G_{\mathrm{der}} \xrightarrow{\ i\ } G \xrightarrow{\det} D = E^\times \longrightarrow 1.$$

By Shapiro's lemma and Hilbert's theorem 90, one has $H^1(\mathbb{Q}, D) = 1$ and the torus D satisfies the Hasse principle. By [18, p. 393], one has $\ker^1(\mathbb{Q}, G) = \ker^1(\mathbb{Q}, D)$. Therefore, G also satisfies the Hasse principle. ∎

It follows from Lemmas 8.6, 8.7 and 8.8 that $|\Delta_f(\pi_0)| = |\Delta(\pi_0)| = 1$. By Proposition 8.3, we have proven the following result.

Theorem 8.9. *Let G, $\pi_0 \in G(\mathbb{Q})$, U_N and $R_N(\pi_0)$ be as in Section 6. There exists a positive integer N_0 such that for all positive integers N divisible by N_0, we have* (*see* (8.1))

$$\operatorname{tr} R_N(\pi_0) = a(G_{\pi_0})\, O_{\pi_0}(\varphi_{\pi_0,N}), \tag{8.13}$$

where the Haar measure on $G_{\pi_0}(\mathbb{A}_f)$ is defined by (8.7).

Remark 8.10. (1) Theorem 8.9 is not very useful in practice yet as we do not have good control for N_0. For example, we do not know whether N_0 can be prime-to-p. Note that we defined the cover $\Lambda^*_{g,N}$ by modular interpretation only for prime-to-p level. When $p\,|N$, we still can define $\boldsymbol{\Lambda}^*_{g,N}$ as a finite étale $\mathbb{F}_p$-scheme: let $\Lambda^*_{g,N} := G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_N$ with Galois action given by

$$\sigma_p \cdot (x_\ell)_\ell = (\pi_0 x_\ell \pi_0^{-1})_\ell, \quad (x_\ell)_\ell \in G(\mathbb{A}_f).$$

This agrees with $\boldsymbol{\Lambda}^*_{g,N}$ in Section 6 when $p \nmid N$ and one also has $\operatorname{tr} R_N(\pi_0) = |\boldsymbol{\Lambda}^*_{g,N}(\mathbb{F}_p)|$, except that the geometric meaning for the set $\boldsymbol{\Lambda}^*_{g,N}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points is less clear.

We report some progress since the present paper was submitted in 2012. In [11] Ibukiyama generalized his results with Katsura (Theorems 1.1 and 1.2) to the non-principal genus case (cf. Theorem 7.6 (2) (3) (5) for $N = 1$ without any assumption). Ibukiyama's proof is more arithmetic, which treats the geometric problems by quaternion Hermitian forms. As an application, he describes the number of components of the supersingular locus that are defined over $\mathbb{F}_p$ for all g by the work of Li and Oort. He also proves an explicit formula for $|\boldsymbol{\Sigma}_2(\mathbb{F}_p)|$ and $\boldsymbol{\Sigma}_2(\mathbb{F}_p) \neq \emptyset$ as a consequence (see [10]). In [41] the author constructs directly a polarized abelian surface (A_0, λ_0) over $\mathbb{F}_p$ in $\boldsymbol{\Sigma}_2(\mathbb{F}_p)$ with Frobenius endomorphism $\pi_0^2 = p$ (not $\pi_0^2 = -p$). Taking the self-product of this point, we get a base point

(A_0'', λ_0'') over $\mathbb{F}_p$ with Frobenius π_0'' square central in $G(\mathbb{Q})$. As a result, Theorem 7.6 holds true (cf. Remark 7.7) without any assumption, except with different covers $\Sigma_{g,N}^*$ due to the choice of the new base point. It is also not difficult to check that $G_{\pi_0''}$ satisfies the Hasse principle. Therefore, we have analogue of Theorem 8.9 for the non-principal genus case.

Acknowledgments

The author thanks Professors Ibukiyama and Katsura for their inspiring work [12], especially Ibukiyama for his interest and discussions. He thanks Jiu-Kang Yu and Wen-Wei Li for helpful discussions. The manuscript was prepared during the author's stay at l'Institut des Hautes Études Scientifiques in 2010. He acknowledges the institution for kind hospitality and excellent working conditions. The author was partially supported by the grants NSC 100-2628-M-001-006-MY4 and AS-99-CDA-M01. The author thanks the referees for careful reading and helpful comments that improve the exposition significantly.

References

[1] M. Borovoi,*Abelian Galois cohomology of reductive groups.* Mem. Amer. Math. Soc. **132** (1998), no. 626, 50 pp.

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg* **14** (1941), 197–272.

[3] M. Deuring, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl. *Jber. Deutsch. Math.* **54** (1950). 24–41.

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

[5] L. Fargues, Cohomologie des espaces de modules de groupes p-divisibles et correspondances de Langlands locales. *Astériques* **291** (2004), 1–199.

[6] S. Gelbart, *Automorphic forms on adele groups.* Annals of Mathematics Studies, No. 83. Princeton University Press, 1975.

[7] A. Ghitza, Hecke eigenvalues of Siegel modular forms (mod p) and of algebraic modular forms. *J. Number Theory* **106** (2004), no. 2, 345–384.

[8] B. H. Gross, Algebraic modular forms. *Israel J. Math.* **113** (1999), 61–93.

[9] K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms, *J. Fac. Sci. Univ. Tokyo* **27** (1980), 549–601.

[10] T. Ibukiyama, Quinary lattices and binary quaternion hermitian lattices. Preprint, 2016, 14 pp. To appear in *Tohoku Math. J.*

[11] T. Ibukiyama, Type numbers of quaternion hermitian forms and supersingular abelian varieties. Preprint, 2016, 18 pp. To appear in *Osaka J. Math.*

[12] T. Ibukiyama and T. Katsura, On the field of definition of superspecial polarized abelian varieties and type numbers. *Compositio Math.* **91** (1994), 37–46.

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

[14] T. Katsura and F. Oort, Families of supersingular abelian surfaces, *Compositio Math.* **62** (1987), 107–167.

[15] R. E. Kottwitz, Rational conjugacy classes in reductive groups. *Duke Math. J.* **49** (1982), no. 4, 785–806.

[16] R. E. Kottwitz, Stable trace formula: cuspidal tempered terms. *Duke Math. J.* **51** (1984), no. 3, 611–650.

[17] R. E. Kottwitz, Stable trace formula: elliptic singular terms. *Math. Ann.* **275** (1986), 365–399.

[18] R. E. Kottwitz, Points on some Shimura varieties over finite fields. *J. Amer. Math. Soc.* **5** (1992), 373–444.

[19] R.E. Kottwitz, Harmonic analysis on reductive p-adic groups and Lie algebras. *Harmonic analysis, the trace formula, and Shimura varieties*, 393–522, Clay Math. Proc. 4, Amer. Math. Soc., Providence, RI, 2005.

[20] S. Lang, *Algebraic number theory.* Graduate Texts in Mathematics, **110**. Springer-Verlag, New York, 1986. 354 pp.

[21] K.-Z. Li and F. Oort, *Moduli of Supersingular Abelian Varieties.* Lecture Notes in Math., vol. 1680, Springer-Verlag, 1998.

[22] E. Mantovan, On certain unitary group Shimura varieties. *Astériques* **291** (2004), 201–331.

[23] D. Mumford, *Abelian Varieties.* Oxford University Press, 1974.

[24] F. Oort, A stratification of a moduli space of abelian varieties. *Moduli of Abelian Varieties*, 345–416. (ed. by C. Faber, G. van der Geer and F. Oort), Progress in Mathematics **195**, Birkhäuser 2001.

[25] G. Prasad, Volumes of S-arithmetic quotients of semi-simple groups. *Inst. Hautes Études Sci. Publ. Math.* **69** (1989), 91–117.

[26] V. Platonov and A. Rapinchuk, Algebraic groups and number theory. *Pure and Applied Mathematics, 139.* Academic Press, Inc., Boston, MA, 1994.

[27] M. Rapoport and Th. Zink, *Period Spaces for p-divisible groups.* Ann. Math. Studies 141, Princeton Univ. Press, 1996.

[28] D. A. Reduzzi, Hecke eigensystems for (mod p) modular forms of PEL type and algebraic modular forms. *Int. Math. Res. Not. IMRN* 2013, no. 9, 2133–2178.

[29] J.-P. Serre, Two letters on quaternions and modular forms (mod p). *Israel J. Math.* **95** (1996), 281–299.

[30] G. Shimura, *Euler product and Eisenstein series.* CBMS Regional Conference Series in Math., 93, *Published for the Conference Board of the Mathematical Sciences, Washington, DC*, 1997.

[31] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory.* Publ. Math. Soc. Japan 6, Tokyo, 1961.

[32] J. Tate, Classes d'isogenie de variétés abéliennes sur un corps fini (d'après T. Honda). *Sém. Bourbaki Exp.* 352 (1968/69). Lecture Notes in Math., vol. 179, Springer-Verlag, 1971.

[33] E. Viehmann and T. Wedhorn, Ekedahl-Oort and Newton strata for Shimura varieties of PEL type. *Math. Ann.* **356** (2013), no. 4, 1493–1550.

[34] A. Weil, The field of definition of a variety. *Amer. J. Math.* **78** (1956), 509–524.

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

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

[37] C.-F. Yu, On the slope stratification of certain Shimura varieties. *Math. Z.* **251** (2005), 859–873.

[38] C.-F. Yu, The supersingular loci and mass formulas on Siegel modular varieties. *Doc. Math.* **11** (2006), 449–468.

[39] C.-F. Yu, Simple mass formulas on Shimura varieties of PEL-type. *Forum Math.* **22** (2010), no. 3, 565–582.

[40] C.-F. Yu, On the existence of maximal orders. *Int. J. Number Theory* **7** (2011), no. 8, 2091–2114.

[41] C.-F. Yu, On fields of definition of components of the Siegel supersingular locus, arXiv:1608.03416, 6 pp. To appear in *Proc. Amer. Math. Sci.*

Institute of Mathematics, Academia Sinica and NCTS,, Astronomy Mathematics Building, No. 1, Roosevelt Rd. Sec. 4, Taipei, Taiwan, 10617

E-mail address: `chiafu@math.sinica.edu.tw`