ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 106 (2004) 345–384

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Hecke eigenvalues of Siegel modular forms (mod p) and of algebraic modular forms

Alexandru Ghitza*

Department of Mathematics and Statistics, McGill University, 805 Sherbrooke W., Montreal, Que., Canada H3A 2K6

Received 25 August 2003

Communicated by W. Duke

Abstract

In his letter (Israel J. Math. 95 (1996) 281), Serre proves that the systems of Hecke eigenvalues given by modular forms (mod p) are the same as the ones given by locally constant functions $\mathbb{A}_B^\times/B^\times \to \overline{\mathbb{F}}_p$, where B is the endomorphism algebra of a supersingular elliptic curve. We generalize this result to Siegel modular forms, proving that the systems of Hecke eigenvalues given by Siegel modular forms (mod p) of genus g are the same as the ones given by algebraic modular forms (mod p) on the group $\mathrm{GU}_g(B)$, as defined in Gross (Math. Res. Notices (16) (1998) 865; Israel J. Math. 113 (1999) 61). The correspondence is obtained by restricting to the superspecial locus of the moduli space of abelian varieties.

MSC: 11F46; 11F55

Keywords: Siegel modular forms; Algebraic modular forms; Hecke eigenvalues

1. Introduction

Fix positive integers g, p, and N, where $N \geqslant 3$ and p is a prime not dividing N. We study the space of Siegel modular forms (mod p) of genus g, level N, and all weights; more precisely, we are interested in the systems of Hecke eigenvalues that occur in this space. The approach that we take is largely inspired by a result of Serre [21] in genus 1, linking Hecke eigenvalues of (elliptic) modular forms (mod p) and quaternion algebras. Our main result is

*Fax: 1-514-398-3899.

E-mail address: aghitza@alum.mit.edu.

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2003.12.009

Theorem 1. *The systems of Hecke eigenvalues coming from Siegel modular forms* $(\mathrm{mod}\, p)$ *of genus* g, *level* N *and any weight* ρ, *are the same as the systems of Hecke eigenvalues coming from algebraic modular forms* $(\mathrm{mod}\, p)$ *of level* U *and any weight* ρ_Σ *on the group* $\mathrm{GU}_g(B)$, *where* $\mathcal{O}$ *is the endomorphism algebra of a supersingular elliptic curve over* $\overline{\mathbb{F}}_p$, $B \coloneqq \mathcal{O} \otimes \mathbb{Q}$, *and*

$$U \coloneqq U_p \times \prod_{\ell \neq p} U_\ell(N),$$
$$U_p \coloneqq \ker(\mathrm{GU}_g(\mathcal{O}_p) \to \mathrm{GU}_g(\mathbb{F}_{p^2})),$$
$$U_\ell(N) \coloneqq \{x \in \mathrm{GU}_g(\mathcal{O}_\ell) : x \equiv 1 \,(\mathrm{mod}\, \ell^n), \ell^n || N\}.$$

How does this result improve our understanding of Siegel modular forms? As an example, it is a direct consequence of Theorem 1 that there are only finitely many systems of Hecke eigenvalues coming from the space of Siegel modular forms $(\mathrm{mod}\, p)$ of genus g, level N. Moreover, one can derive an explicit (albeit far from sharp) upper bound on this number, which in turn can be applied to the study of the structure of the Siegel–Hecke algebra, in a manner similar to Jochnowitz [11,12]. In the other direction, one can use Theorem 1 to study the relation between algebraic modular forms and Galois representations in the case $g = 2$, by employing results of Weissauer and Taylor on the construction of Galois representations associated to Siegel modular forms of genus 2. This suggests an approach to Conjectures 8.1 and 9.14 of Gross [7] in this particular case. Both these applications are subject of work in progress by the author.

The paper is organized as follows. Section 2 contains preliminary results on three topics: the definition of algebraic modular forms, the geometric theory of Siegel modular forms $(\mathrm{mod}\, p)$, and the properties of superspecial abelian varieties. Section 3 contains the main technical result on which the approach of the paper is based. It links a finite set constructed from the superspecial locus to a finite set constructed from the algebraic group $\mathrm{GU}_g(B)$, in a way that is compatible with the Hecke action. We encourage the reader to skip the proof of this result and go directly to Section 4, which puts everything together and is quite different from Serre's approach for the case $g = 1$. Here we prove that the operation of restricting Siegel modular forms to the superspecial locus preserves the systems of Hecke eigenvalues.

2. Preliminaries

The following notation will be fixed throughout the paper: $g > 1$ is a positive integer, p is a prime, and N is a positive integer not divisible by p.

2.1. Algebraic modular forms

2.1.1. Quaternion hermitian forms

Let B be a quaternion algebra over a field F. Let $\bar{\cdot}$ denote the canonical involution of B (i.e. conjugation) and let N denote the norm map. Let V be a left B-module which is free of dimension g. A *quaternion hermitian form* on V is an F-bilinear map $f : V \times V \to B$ such that

$$f(bx, y) = bf(x, y), \quad \overline{f(x, y)} = f(y, x)$$

for all $b \in B$, $x, y \in V$. We say f is non-degenerate if $f(x, V) = 0$ implies $x = 0$.

The following result says that any such form is diagonalizable [22, Section 2.2]:

Proposition 2. *For every quaternion hermitian form f on V, there exists a basis $\{x_1, \ldots, x_g\}$ of V over B such that $f(x_i, x_j) = \alpha_i \delta_{ij}$ for $1 \leqslant i, j \leqslant n$, where $\alpha_i \in F$. Moreover if f is non-degenerate and the norm map $N : B \to F$ is surjective, then there exists a basis $\{y_1, \ldots, y_g\}$ of V over B such that $f(y_i, y_j) = \delta_{ij}$.*

Furthermore, we have the following result [25, Section 3.4]:

Theorem 3 (The norm theorem). *Let B be a quaternion algebra over a field F, and let F_B be the set of elements of F which are positive at all the real places of F which ramify in B. Then the image of the reduced norm map $n : B \to F$ is precisely F_B.*

We conclude that if B is the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞, then $n(B) = \mathbb{Q}_{>0}$.

2.1.2. The similitude groups

Let B be a quaternion algebra over a field F. We define the group of unitary $g \times g$ matrices and its similitude group by

$$\mathrm{U}_g(B) \coloneqq \{M \in \mathrm{GL}_g(B) : M^* M = I\},$$

$$\mathrm{GU}_g(B) \coloneqq \{M \in \mathrm{GL}_g(B) : M^* M = \gamma(M) I, \gamma(M) \in F^\times\}.$$

These are algebraic groups over F: let $(f_{ij}) \coloneqq M^* M$, then $\mathrm{U}_g(B)$ is defined by the equations $f_{ij} = 0$ $(i \neq j)$, $f_{ii} = 1$, and $\mathrm{GU}_g(B)$ is defined by the equations

$$f_{ij} = 0 \text{ for } i \neq j, \quad f_{11} = f_{22} = \cdots = f_{gg}$$

(these are automatically in F because they are sums of norms of elements of B).

We define the group of symplectic $2g \times 2g$ matrices and its similitude group as follows:

$$\mathrm{Sp}_{2g}(F) := \{M \in \mathrm{GL}_{2g}(F) : M^t J_{2g} M = J_{2g}\},$$

$$\mathrm{GSp}_{2g}(F) := \{M \in \mathrm{GL}_{2g}(F) : M^t J_{2g} M = \gamma(M) J_{2g}, \gamma(M) \in F^\times\},$$

where $J_{2g} = \left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right)$.

Lemma 4. *Let K be a field. The subgroups $\mathrm{GU}_g(M_2(K))$ and $\mathrm{GSp}_{2g}(K)$ are conjugate inside $\mathrm{GL}_{2g}(K)$. In particular, they are isomorphic and the F-algebraic group $\mathrm{GU}_g(B)$ is an F-form of GSp_{2g}.*

Proof. If $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(K)$, then the conjugate of A is $\bar{A} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, therefore the adjoint of A is

$$A^* = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = J_2^{-1} A J_2.$$

Set $\tilde{J}_{2g} := \mathrm{diag}(J_2, \ldots, J_2)$ and let $M = (A_{ij})_{1 \leqslant i, j \leqslant g} \in M_g(M_2(K))$. We have

$$M^* = \tilde{J}_{2g}^{-1} M^t \tilde{J}_{2g},$$

therefore

$$M^* M = \tilde{J}_{2g}^{-1} M^t \tilde{J}_{2g} M.$$

It is clear that there exists a permutation matrix P such that $P^t \tilde{J}_{2g} P = J_{2g}$. We have $J_{2g} = P^t \tilde{J}_{2g} P$, so $\tilde{J}_{2g} = P J_{2g} P^t$ and

$$M^* M = P J_{2g}^{-1} P^t M^t P J_{2g} P^t M.$$

Now if $M \in \mathrm{GU}_g(M_2(K))$, then $M^* M = \gamma I$ for some $\gamma \in K^\times$ and a little manipulation gives

$$(P^t M P)^t J_{2g} (P^t M P) = \gamma J_{2g},$$

i.e. $P^t M P \in \mathrm{GSp}_{2g}(K)$. Conversely, if $P^t M P \in \mathrm{GSp}_{2g}(K)$ then

$$M^* M = P J_{2g}^{-1} (P^t M P)^t J_{2g} P^t M = P J_{2g}^{-1} \gamma J_{2g} P^t = \gamma I$$

so $M \in \mathrm{GU}_g(M_2(K))$. Therefore $P^{-1} \mathrm{GU}_g(M_2(K)) P = \mathrm{GSp}_{2g}(K)$, as desired. Since $B \otimes \bar{F} \cong M_2(\bar{F})$, we conclude that $\mathrm{GU}_g(B) \otimes \bar{F} \cong \mathrm{GSp}(\bar{F})$. □

2.1.3. Algebraic modular forms (mod p)

We give the definition of algebraic modular forms (mod p) on the group $G \coloneqq \mathrm{GU}_g(B)$, where B is the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. See [8,9] for more details.

The definition given by Gross requires that G be a reductive algebraic group over $\mathbb{Q}$ satisfying a technical condition for which it sufficient to know that $G_0(\mathbb{R})$ is a compact Lie group. Our G is reductive, being a form of the reductive group GSp_{2g}. We also know that $G_0(\mathbb{R})$ is compact, since it is a subgroup of the orthogonal group $\mathrm{O}(4g)$.

Let $\mathcal{O}_p$ be the maximal order of $B \otimes \mathbb{Q}_p$. We define U_p to be the kernel of the reduction modulo a uniformizer π of $\mathcal{O}_p$, i.e.

$$1 \to U_p \to G(\mathcal{O}_p) \xrightarrow{\bmod \pi} \mathrm{GU}_g(\mathbb{F}_{p^2}) \to 1.$$

For $\ell \neq p$, we set

$$U_\ell(N) \coloneqq \{x \in G(\mathcal{O}_\ell) : x \equiv 1 \ (\mathrm{mod}\ \ell^n), \ell^n || N\}.$$

The product

$$U \coloneqq U_p \times \prod_{\ell \neq p} U_\ell(N)$$

is an open compact subgroup of $G(\hat{\mathbb{Q}})$, called the level ($\hat{\mathbb{Q}}$ is the ring of finite adèles). Set $\Omega(N) \coloneqq U \backslash G(\hat{\mathbb{Q}}) / G(\mathbb{Q})$. By Gross [9, Proposition 4.3], the double coset space $\Omega(N)$ is finite.

Now let $\rho : \mathrm{GU}_g(\mathbb{F}_{p^2}) \to \mathrm{GL}(W)$ be an irreducible representation, where W is a finite-dimensional $\mathbb{F}_p$-vector space. We define the space of *algebraic modular forms* (mod p) of weight ρ and level U on G as follows:

$$M(\rho, U) \coloneqq \{f : \Omega(N) \to W : f(\lambda g) = \rho(\lambda)^{-1} f(g) \text{ for all } \lambda \in \mathrm{GU}_g(\mathbb{F}_{p^2})\}.$$

Since $\Omega(N)$ is a finite set and W is finite dimensional, $M(\rho, U)$ is a finite-dimensional $\mathbb{F}_p$-vector space.

Given a prime ℓ not dividing pN, we have the local Hecke algebra $\mathscr{H}_\ell = \mathscr{H}(\mathrm{GSp}_{2g}(\mathbb{Q}_\ell), \mathrm{GSp}_{2g}(\mathbb{Z}_\ell))$ acting naturally on $\Omega(N)$, and hence on $M(\rho, U)$ (see Section 3.2.1 for details).

2.2. The geometric theory of Siegel modular forms

We review the basic definitions and results from Chai [3].

All the schemes we consider are locally noetherian. A g-dimensional *abelian scheme* A over a scheme S is a proper smooth group scheme

$$\begin{array}{c} A \\ {\scriptstyle\pi}\downarrow\uparrow{\scriptstyle 0} \\ S, \end{array}$$

whose (geometric) fibers are connected of dimension g.

A *polarization* of A is an S-homomorphism $\lambda : A \to A^t := \mathrm{Pic}^0(A/S)$ such that for any geometric point s of S, the homomorphism $\lambda_s : A_s \to A_s^t$ is of the form $\lambda_s(a) = t_a^* \mathscr{L}_s \otimes \mathscr{L}_s^{-1}$ for some ample invertible sheaf $\mathscr{L}_s$ on A_s. Such λ is necessarily an isogeny. In this case, $\lambda_* \mathscr{O}_A$ is a locally free $\mathscr{O}_{A^t}$-module whose rank is constant over each connected component of S. This rank is called the *degree* of λ; if this degree is 1 (so λ is an isomorphism) then λ is said to be *principal*. Any polarization is symmetric: $\lambda^t = \lambda$ via the canonical isomorphism $A \cong A^{tt}$.

Let $\phi : A \to B$ be an isogeny of abelian schemes over S. Cartier duality [19, Theorem III.19.1] states that $\ker \phi$ is canonically dual to $\ker \phi^t$. There is a canonical non-degenerate pairing

$$\ker \phi \times \ker \phi^t \to \mathbb{G}_m.$$

An important example is $\phi = [N]$ for an integer N. The kernel $A[N]$ of multiplication by N on A is a finite flat group scheme of rank N^{2g} over S; it is étale over S if and only if S is a scheme over $\mathbb{Z}[\frac{1}{N}]$. We get the *Weil pairing*

$$A[N] \times A^t[N] \to \mathbb{G}_m.$$

A principal polarization λ on A induces a canonical non-degenerate skew-symmetric pairing

$$A[N] \times A[N] \to \boldsymbol{\mu}_N,$$

which is also called the *Weil pairing*.

For our purposes, a *level N structure* on (A, λ) is a symplectic similitude from $A[N]$ with the Weil pairing to $(\mathbb{Z}/N\mathbb{Z})^{2g}$ with the standard symplectic pairing, i.e. an isomorphism of group schemes $\alpha : A[N] \to (\mathbb{Z}/N\mathbb{Z})^{2g}$ such that the following diagram commutes:

$$\begin{array}{ccc} A[N] \times A[N] & \xrightarrow{(\alpha,\alpha)} & (\mathbb{Z}/N\mathbb{Z})^{2g} \times (\mathbb{Z}/N\mathbb{Z})^{2g} \\ {\scriptstyle\text{Weil}}\downarrow & & \downarrow{\scriptstyle\text{std}} \\ \boldsymbol{\mu}_N & \xrightarrow{\sim} & \mathbb{Z}/N\mathbb{Z} \end{array}$$

for some isomorphism $\boldsymbol{\mu}_N \cong \mathbb{Z}/N\mathbb{Z}$.

If $N \geqslant 3$, the functor "isomorphism classes of principally polarized g-dimensional abelian varieties with level N structure" is representable by a scheme $\mathscr{A}_{g,1,N}$ which is faithfully flat over $\mathbb{Z}$, smooth and quasi-projective over $\mathbb{Z}[\frac{1}{N}]$. Let

$$\begin{array}{ccc} Y & & \\ {\scriptstyle\pi}\downarrow & \nwarrow & \\ \mathscr{A}_{g,1,N} & & {\scriptstyle 0}\end{array}$$

be the corresponding universal abelian variety. Let $\mathbb{E} \coloneqq 0^*(\Omega_{Y/\mathscr{A}_{g,1,N}})$; this is called the *Hodge bundle*.

2.2.1. Twisting the sheaf of differentials

Let X be a scheme and let $\mathscr{F}$ be a locally free $\mathscr{O}_X$-module whose rank is the same integer n on all connected components of X. Let $\{U_i : i \in I\}$ be an open cover of X that trivializes $\mathscr{F}$, then we have $\mathscr{F}|_{U_i} \cong (\mathscr{O}_X|_{U_i})^n$, and for all i and j we have isomorphisms $\mathscr{F}|_{U_i \cap U_j} \cong \mathscr{F}|_{U_j \cap U_i}$ given by $g_{ij} \in \mathrm{GL}_n(\mathscr{O}_X|_{U_i \cap U_j})$ satisfying the usual cocycle identities.

Now suppose we are given a rational linear representation $\rho : \mathrm{GL}_n \to \mathrm{GL}_m$. We construct a new locally free $\mathscr{O}_X$-module $\mathscr{F}_\rho$ as follows: set $(\mathscr{F}_\rho)_i = (\mathscr{O}_X|_{U_i})^m$, and for any i,j define an isomorphism $(\mathscr{F}_\rho)_i|_{U_i \cap U_j} \to (\mathscr{F}_\rho)_j|_{U_i \cap U_j}$ by $\rho(g_{ij}) \in \mathrm{GL}_m(\mathscr{O}_X|_{U_i \cap U_j})$. Since the transition functions $\rho(g_{ij})$ satisfy the required properties, we can glue the $(\mathscr{F}_\rho)_i$ together to get the locally free $\mathscr{O}_X$-module $\mathscr{F}_\rho$. We say that it was obtained by *twisting* $\mathscr{F}$ *by* ρ. It is obvious that $\mathscr{F} = \mathscr{F}_{\mathrm{std}}$, where $\mathrm{std} : \mathrm{GL}_n \to \mathrm{GL}_n$ is the standard representation.

The correspondence $\rho \mapsto \mathscr{F}_\rho$ is a covariant functor from the category of rational linear representations of GL_n to the category of locally free $\mathscr{O}_X$-modules. This functor is exact and it commutes with tensor products.

Let $X \coloneqq \mathscr{A}_{g,1,N} \otimes \overline{\mathbb{F}}_p$. This is a smooth quasi-projective variety over $\overline{\mathbb{F}}_p$, with $\phi(N)$ connected components. Given a rational representation $\rho : \mathrm{GL}_g \to \mathrm{GL}_m$, the global sections of $\mathbb{E}_\rho$ are called *Siegel modular forms* $(\mathrm{mod}\, p)$ of weight ρ and level N and they can be written

$$M_\rho(N) \coloneqq \mathrm{H}^0(X, \mathbb{E}_\rho) = \{f : \{[A,\lambda,\alpha,\eta]\} \to \overline{\mathbb{F}}_p^m \text{ satisfying}$$

$$f(A,\lambda,\alpha,M\eta) = \rho(M)^{-1} f(A,\lambda,\alpha,\eta),\ \forall M \in \mathrm{GL}_g(\overline{\mathbb{F}}_p)\},$$

where η is a basis of invariant differentials on A.

2.2.2. Hecke action

Suppose we have a correspondence

$$X \xleftarrow{a} Z \xrightarrow{b} X,$$

where a and b are finite étale, and suppose that we are given a coherent sheaf $\mathscr{F}$ on X together with a morphism of $\mathscr{O}_Z$-modules $z : a^*\mathscr{F} \to b^*\mathscr{F}$.

We claim that this induces an operator $T_{Z,\mathscr{F}} : \mathrm{H}^0(X,\mathscr{F}) \to \mathrm{H}^0(X,\mathscr{F})$.

Since b is finite flat, $b_*\mathscr{O}_Z$ is a locally free sheaf of $\mathscr{O}_X$-algebras, and therefore we can define $\mathrm{Trace}_b : b_*\mathscr{O}_Z \to \mathscr{O}_X$ via the diagram

$$\begin{array}{ccc} b_*\mathscr{O}_Z & \longrightarrow & \mathscr{H}om_{\mathscr{O}_X}(b_*\mathscr{O}_Z, b_*\mathscr{O}_Z) \\ & \searrow^{\mathrm{Trace}_b} & \downarrow \mathrm{Trace} \\ & & \mathscr{O}_X. \end{array}$$

We want to extend this trace map to $\mathscr{F}$. By the projection formula, we have $b_*b^*\mathscr{F} = b_*(b^*\mathscr{F} \otimes \mathscr{O}_Z) = \mathscr{F} \otimes b_*\mathscr{O}_Z$. We can now define $\mathrm{Trace}_b : b_*b^*\mathscr{F} \to \mathscr{F}$ via the diagram

$$\begin{array}{ccc} \mathscr{F} \otimes b_*\mathscr{O}_Z & \xrightarrow{1\otimes \mathrm{Trace}_b} & \mathscr{F} \otimes \mathscr{O}_X \\ \| & & \| \\ b_*b^*\mathscr{F} & \xrightarrow{\mathrm{Trace}_b} & \mathscr{F}. \end{array}$$

It remains to put these together:

$$\begin{aligned} T_{Z,\mathscr{F}} : \mathrm{H}^0(X,\mathscr{F}) &\to \mathrm{H}^0(X,\mathscr{F}) \\ s &\mapsto \mathrm{Trace}_b(b_*z(a^*s)). \end{aligned}$$

The Hecke operators considered in this paper are special cases of the $T_{Z,\mathscr{F}}$, with $X = \mathscr{A}_{g,1,N} \otimes \overline{\mathbb{F}}_p$. The sheaf $\mathscr{F}$ will typically be $\mathbb{E}_\rho$. In order to say what Z is we need some definitions.

Let ℓ be a fixed prime not dividing pN. A quasi-isogeny of polarized abelian varieties $\phi : (A_1,\lambda_1) \to (A_2,\lambda_2)$ is said to be an *ℓ-quasi-isogeny* if its degree is a (possibly negative) power of ℓ. Such ϕ induces a symplectic similitude

$$T_\ell\phi : (T_\ell A_1, e_1) \to (T_\ell A_2, e_2)$$

which gives an element $g \in G := \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$. Since g is defined only up to changes of symplectic bases for $T_\ell A_1$ and $T_\ell A_2$, ϕ actually defines a double coset HgH, where $H := \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. We say that ϕ is *of type HgH*. Since $(\mathrm{GSp}_{2g}(\mathbb{Q}_\ell), \mathrm{GSp}_{2g}(\mathbb{Z}_\ell))$ is a Hecke pair [1, Section 3.3.1], we can talk about the local Hecke algebra $\mathscr{H}_\ell := \mathscr{H}(G,H)$. Finally, we will say that two ℓ-quasi-isogenies are equivalent if they have the same kernel.

Given some $HgH \in \mathscr{H}_\ell$, we let Z be the moduli space of quadruples $(A,\lambda,\alpha;\phi)$, where (A,λ) is a g-dimensional principally polarized abelian variety over $\overline{\mathbb{F}}_p$, α is a level N structure, and ϕ is an equivalence class of ℓ-quasi-isogenies of type HgH.

This has two natural maps to the moduli space X, namely

$$\begin{aligned} a: \quad & Z \to X \\ & (A, \lambda, \alpha; \phi) \mapsto (A, \lambda, \alpha) \end{aligned}$$

and

$$\begin{aligned} b: \quad & Z \to X \\ & (A, \lambda, \alpha; \phi) \mapsto (\phi(A), \lambda_\phi, \alpha_\phi), \end{aligned}$$

where λ_ϕ, respectively α_ϕ are the principal polarization, respectively the level N structure induced by ϕ on $\phi(A)$.

Both a and b are finite étale. The operators $T_{Z,\mathscr{F}}$ defined in this context are our Hecke operators.

2.2.3. The Kodaira–Spencer isomorphism

We recall the properties of the Kodaira–Spencer isomorphism. For a detailed account see [4, Sections III.9 and VI.4].

If $\pi : A \to S$ is projective and smooth, there is a *Kodaira–Spencer map*

$$\kappa : \mathscr{T}_S \to \mathrm{R}^1\pi_*(\mathscr{T}_{A/S}).$$

If

$$\begin{array}{ccc} A & & \\ {\scriptstyle\pi}\downarrow & \nwarrow & \\ S, & \xrightarrow{0} & \end{array}$$

is an abelian scheme, set $\mathbb{E}_{A/S} \coloneqq 0^*(\Omega^1_{A/S})$. Then

$$\mathscr{T}_{A/S} = \pi^*(0^*(\mathscr{T}_{A/S})) = \pi^*(\mathbb{E}^\vee_{A/S}).$$

The projection formula gives

$$\mathrm{R}^1\pi_*(\pi^*(\mathbb{E}^\vee_{A/S})) = (\mathrm{R}^1\pi_*\mathscr{O}_A) \otimes_{\mathscr{O}_S} \mathbb{E}^\vee_{A/S}.$$

Let $\pi^t : A^t \to S$ be the dual abelian scheme, then

$$\mathrm{R}^1\pi_*\mathscr{O}_A = 0^*(\mathscr{T}_{A^t/S}) = \mathbb{E}^\vee_{A^t/S}.$$

So the Kodaira–Spencer map can be written as follows:

$$\kappa : \mathscr{T}_S \to \mathbb{E}^\vee_{A^t/S} \otimes_{\mathscr{O}_S} \mathbb{E}^\vee_{A/S},$$

which after dualizing gives

$$\kappa^\vee : \mathbb{E}_{A^t/S} \otimes_{\mathcal{O}_S} \mathbb{E}_{A/S} \to \Omega^1_S.$$

Now suppose that $\lambda : A/S \to A^t/S$ is a principal polarization, i.e. an isomorphism. Then the pullback map $\lambda^* : \mathbb{E}_{A^t/S} \to \mathbb{E}_{A/S}$ is an isomorphism and we get a map $\mathbb{E}_{A/S}^{\otimes 2} \to \Omega^1_S$. This factors through the projection map to $\mathrm{Sym}^2(\mathbb{E}_{A/S})$, and the resulting map $\mathrm{Sym}^2(\mathbb{E}_{A/S}) \to \Omega^1_S$ is an isomorphism. In particular, in the notation of Section 2.2.1 we have a Hecke isomorphism $\mathbb{E}_{\mathrm{Sym}^2\mathrm{std}} \cong \Omega^1_X$.

2.3. Superspecial abelian varieties

For a commutative group scheme A over a perfect field K we define the *a-number* of A by $a(A) := \dim_K \mathrm{Hom}(\alpha_p, A)$. If $K \subset L$ with L perfect, then $\dim_K \mathrm{Hom}(\alpha_p, A) = \dim_L \mathrm{Hom}(\alpha_p, A \otimes L)$ so $a(A)$ does not depend on the base field.

An abelian variety A over K of dimension $g \geqslant 2$ is said to be *superspecial* if $a(A) = g$. Let k be an algebraic closure of K. By Oort [20, Theorem 2], $a(A) = g$ if and only if $A \otimes k \cong E_1 \times \cdots \times E_g$, where the E_i are supersingular elliptic curves over k. On the other hand, for any $g \geqslant 2$ and any supersingular elliptic curves $E_1, \ldots, E_{2g}$ over k we have [23, Theorem 3.5]

$$E_1 \times \cdots \times E_g \cong E_{g+1} \times \cdots \times E_{2g}.$$

We conclude that A is superspecial if and only if $A \otimes k \cong E^g$ for some (and therefore any) supersingular elliptic curve E over k.

Any abelian subvariety of a superspecial abelian variety A is also superspecial. If A is superspecial and $G \subset A$ is a finite étale subgroup scheme, then A/G is also superspecial.

An *$\mathbb{F}_q$-structure* on a scheme S over $\overline{\mathbb{F}}_p$ is a scheme S' over $\mathbb{F}_q$ such that S is isomorphic to $S' \otimes \overline{\mathbb{F}}_p$.

Lemma 5. *Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Then E has a canonical $\mathbb{F}_{p^2}$-structure E', namely the one whose geometric Frobenius is $[-p]$. The correspondence $E \mapsto E'$ is functorial.*

Proof. This is a well-known result which is stated in [21, p. 284]. For a detailed proof, see [6, Lemma 2.1]. □

Proposition 6. *Let A be a superspecial abelian variety over $\overline{\mathbb{F}}_p$. Then A has a canonical $\mathbb{F}_{p^2}$-structure A', namely the one whose geometric Frobenius is $[-p]$. The correspondence $A \mapsto A'$ is functorial.*

Proof. Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$, then $A \cong E^g$. By Lemma 5 we know that E has an $\mathbb{F}_{p^2}$-structure E' with $\pi_{E'} = [-p]_{E'}$, therefore $A' := (E')^g$ is an $\mathbb{F}_{p^2}$-structure for A such that

$$\pi_{A'} = \pi_{E'} \times \pi_{E'} \times \cdots \times \pi_{E'} = [-p]_{E'} \times [-p]_{E'} \times \cdots \times [-p]_{E'} = [-p]_{A'}.$$

The functoriality statement follows from the corresponding functoriality statement in Lemma 5. Since any superspecial abelian variety over $\overline{\mathbb{F}}_p$ is isomorphic to E^g, it suffices to consider a morphism $f : E^g \to E^g$. This is built out of a bunch of morphisms $E \to E$, which by Lemma 5 come from morphisms $E' \to E'$. These piece together to give a morphism $f' : (E')^g \to (E')^g$ over $\mathbb{F}_{p^2}$, which is just f after tensoring with $\overline{\mathbb{F}}_p$. □

An easy consequence of the functoriality is that if λ is a principal polarization on A, there exists a principal polarization λ' of the canonical $\mathbb{F}_{p^2}$-structure A' of A such that $\lambda' \otimes \overline{\mathbb{F}}_p = \lambda$. We say that (A', λ') is the canonical $\mathbb{F}_{p^2}$-structure of (A, λ).

2.3.1. Isogenies

We need to define what it means for two principally polarized abelian varieties (A_1, λ_1) and (A_2, λ_2) to be isogenous. The natural tendency is to consider isogenies $\phi : A_1 \to A_2$ such that the following diagram commutes:

$$\begin{array}{ccc} A_1 & \xrightarrow{\phi} & A_2 \\ {\scriptstyle\lambda_1}\downarrow{\scriptstyle\sim} & & {\scriptstyle\lambda_2}\downarrow{\scriptstyle\sim} \\ A_1^t & \xleftarrow{\phi^t} & A_2^t, \end{array}$$

i.e. $\phi^t \circ \lambda_2 \circ \phi = \lambda_1$. But then $\deg \phi = 1$ so the only isogenies that satisfy this condition are isomorphisms. We therefore relax the condition by requiring ϕ to satisfy

$$\phi^t \circ \lambda_2 \circ \phi = m\lambda_1,$$

where $m \in \mathbb{N}$. By computing degrees we get $(\deg \phi)^2 = m^g$.

2.3.2. Pairings

We now consider the local data given by the presence of a principal polarization. Let (A, λ) be a g-dimensional principally polarized abelian variety defined over $\overline{\mathbb{F}}_p$. Let ℓ be a prime different from p and set as usual $\mathbb{Z}_\ell(1) := \varprojlim \boldsymbol{\mu}_{\ell^n}$. We have the canonical Weil pairing [15, Section 16]

$$e_\ell : T_\ell A \times T_\ell A^t \to \mathbb{Z}_\ell(1),$$

which is a non-degenerate $\mathbb{Z}_\ell$-bilinear map. When combined with a homomorphism of the form $\alpha : A \to A^t$ it gives

$$e_\ell^\alpha : T_\ell A \times T_\ell A \to \mathbb{Z}_\ell(1)$$

$$(a, a') \mapsto e_\ell(a, \alpha a').$$

If α is a polarization then e_ℓ^α is an alternating (also called symplectic) form, i.e. $e_\ell^\alpha(a', a) = e_\ell^\alpha(a, a')^{-1}$ for all $a, a' \in T_\ell A$. If $f : A \to B$ is a homomorphism, then

$$e_\ell^{f^t \circ \alpha \circ f}(a, a') = e_\ell^\alpha(f(a), f(a'))$$

for all $a, a' \in T_\ell A$, $\alpha : B \to B^t$.

An isogeny $\phi : (A_1, \lambda_1) \to (A_2, \lambda_2)$ of principally polarized abelian varieties induces an injective $\mathbb{Z}_\ell$-linear map on Tate modules $T_\ell \phi : T_\ell A_1 \to T_\ell A_2$, with finite cokernel $T_\ell A_2 / (T_\ell \phi)(T_\ell A_1)$ isomorphic to the ℓ-primary part $(\ker \phi)_\ell$ of $\ker \phi$. Since $\phi^t \circ \lambda_2 \circ \phi = m\lambda_1$, we have

$$\begin{aligned} e_\ell^{\lambda_2}((T_\ell \phi)a, (T_\ell \phi)a') &= e_\ell^{\phi^t \circ \lambda_2 \circ \phi}(a, a') = e_\ell^{m\lambda_1}(a, a') \\ &= e_\ell(a, m\lambda_1 a') = e_\ell(a, \lambda_1 a')^m = e_\ell^{\lambda_1}(a, a')^m. \end{aligned}$$

We say that the map $T_\ell \phi$ is a *symplectic similitude* between the symplectic modules $(T_\ell A_1, e_\ell^{\lambda_1})$ and $(T_\ell A_2, e_\ell^{\lambda_2})$.

In order to deal with the prime p, we will use Dieudonné theory. Let $W := W(k)$ for k a perfect field of characteristic p and let M be a free W-module with semi-linear maps F and V satisfying

$$FV = VF = p, \quad Fx = x^p F, \quad Vx = x^{1/p} V.$$

A *principal quasi-polarization* on M is an alternating form $e : M \times M \to W$ which is a perfect pairing over W, such that F and V are adjoints:

$$e(Fx, y) = e(x, Vy)^p.$$

Such a principal quasi-polarization induces a pairing

$$\langle , \rangle : M/FM \times M/FM \to k$$

$$(x, y) \mapsto e(\tilde{x}, F\tilde{y}) \bmod p,$$

where $\tilde{x}, \tilde{y} \in M$ are lifts of $x, y \in M/FM$. The pairing $\langle , \rangle$ is non-degenerate, linear in x and σ-linear in y. Note that if $k = \mathbb{F}_{p^2}$ then $\langle , \rangle$ is a hermitian form.

Let $M(\cdot)$ be the contravariant Dieudonné module functor on the category of p-divisible groups over $\mathbb{F}_{p^2}$ (see [5]). If A is a superspecial abelian variety we say that the *Dieudonné module* of A is $M(A'[p^\infty])$, where A' is the canonical $\mathbb{F}_{p^2}$-structure on A. A

principal polarization on A defines a principal quasi-polarization e_p on the Dieudonné module M of A [18, Proposition 3.24]. Since A is superspecial we get as above a hermitian form on M/FM.

An isogeny $\phi : (A_1, \lambda_1) \to (A_2, \lambda_2)$ induces a symplectic similitude $\phi^* : M_2 \to M_1$ of principally quasi-polarized Dieudonné modules.

2.3.3. Dieudonné module of a superspecial abelian variety

Let (A, λ) be a principally polarized superspecial abelian variety over $\overline{\mathbb{F}}_p$, and let (A', λ') be the canonical $\mathbb{F}_{p^2}$-structure given by Proposition 6. We want to describe the structure of the Dieudonné module $M = M(A'[p^\infty])$, together with the principal quasi-polarization e induced by λ'.

We first need to recall the structure of the Dieudonné module of a supersingular elliptic curve E. This is well-known, and mentioned for instance in [17, Section 3] or [16, Appendix]. Define the following Dieudonné module:

$$A_{1,1} \coloneqq \left(W^2, F = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix} \sigma, V = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} \sigma^{-1} \right).$$

Corollary 7. *Let E be a supersingular elliptic curve, let E' be its canonical $\mathbb{F}_{p^2}$-structure and let $M \coloneqq M(E'[p^\infty])$.*

(a) *We have $M \cong A_{1,1}$.*
(b) *We have $\mathrm{End}(M) = \mathcal{O}_p \coloneqq \mathcal{O} \otimes \mathbb{Z}_p$, where $\mathcal{O} \coloneqq \mathrm{End}(E')$. Moreover,*

$$\mathcal{O}_p^\times(1) \coloneqq \ker(\mathcal{O}_p^\times \xrightarrow{\text{reduction}} \mathbb{F}_{p^2}^\times)$$

can be identified with the group of automorphisms of M which lift the identity map on M/FM.
(c) *If M_i are the Dieudonné modules of the supersingular elliptic curves E_i, $i = 1, 2$, then any isomorphism $M_1/FM_1 \cong M_2/Fm_2$ lifts to an isomorphism $M_1 \cong M_2$.*

Proof. (a) As we mentioned, this is well-known. Unfortunately, we do not know a reference for the proof, so we refer to Ghitza [6, Section 2.3.1] for the computations.

(b) Let $g \in \mathrm{End}(M)$; it is a W-linear map that commutes with F and V. Suppose g is given by a matrix $(g_{ij}) \in M_2(W)$. We have

$$F \circ g = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix} \sigma \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} = \begin{pmatrix} g_{21}^p & g_{22}^p \\ -pg_{11}^p & -pg_{12}^p \end{pmatrix} \sigma,$$

$$g \circ F = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix} \sigma = \begin{pmatrix} -pg_{12} & g_{11} \\ -pg_{22} & g_{21} \end{pmatrix} \sigma.$$

These should be equal so we get $g_{21}^p = -pg_{12}$, $g_{11} = g_{22}^p$. We also impose the condition $V \circ g = g \circ V$, but this does not give anything new. Therefore

$$\begin{aligned}\mathrm{End}(M) &= \left\{ \begin{pmatrix} x & y \\ -py^p & x^p \end{pmatrix} : x, y \in W(\mathbb{F}_{p^2}) \right\} \\ &= \left\{ \begin{pmatrix} x & 0 \\ 0 & x^p \end{pmatrix} + F \begin{pmatrix} y & 0 \\ 0 & y^p \end{pmatrix} : x, y \in W(\mathbb{F}_{p^2}) \right\}.\end{aligned}$$

But $W(\mathbb{F}_{p^2})$ is the ring of integers of the unique unramified quadratic extension L of $\mathbb{Q}_p$. Let π be a solution of $X^2 + p = 0$ in $\bar{L}$. The map $\sigma : x \mapsto x^p$ is the unique non-trivial automorphism of L. It is now easy to see that the map

$$\begin{array}{rccc} \varphi : & \mathrm{End}(M) & \to & B_p = \{L, -p\} = B \otimes \mathbb{Q}_p \\ \begin{pmatrix} x & 0 \\ 0 & x^p \end{pmatrix} + F \begin{pmatrix} y & 0 \\ 0 & y^p \end{pmatrix} & & \mapsto & x + \pi y \end{array}$$

is an injective ring homomorphism. It identifies $\mathrm{End}(M)$ with $\mathcal{O}_p = \{x + \pi y : x, y \in \mathcal{O}_L\}$, the unique maximal order of B_p.

It remains to prove the statement about $\mathcal{O}_p^\times(1)$. Let $g := \left(\begin{smallmatrix} x & y \\ -py^p & x^p \end{smallmatrix}\right) \in \mathrm{End}(M)^\times = \mathcal{O}_p^\times$. Note that $M/FM = \{\binom{0}{a} + FM : a \in \mathbb{F}_{p^2}\}$. Let $\bar{x}$ be the reduction of x modulo π, then g restricts to multiplication by $\bar{x}^p$ on M/FM.

Therefore g restricts to the identity if and only if $\bar{x} = 1$, which means that the group of such automorphisms is identified with the kernel of the reduction modulo π, i.e. with $\mathcal{O}_p^\times(1)$.

(c) It suffices to show that any automorphism of M/FM lifts to an automorphism of M. From the description of M/FM in part (b) of the proof we know that the automorphisms are given by multiplication by some $\lambda \in \mathbb{F}_{p^2}^\times$. But then the matrix $\left(\begin{smallmatrix} \lambda^p & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ represents an automorphism of M which restricts to multiplication by λ on M/FM, which is what we wanted to show. □

We now use the following result [14, Proposition 6.1]:

Proposition 8. *Let K be a perfect field containing $\mathbb{F}_{p^2}$, and suppose $\{M, e\}$ is a quasi-polarized superspecial Dieudonné module of genus g over $W := W(K)$ such that $M \cong A_{1,1}^g$. Then one can decompose*

$$M \cong M_1 \oplus M_2 \oplus \cdots \oplus M_d \quad (e(M_i, M_j) = 0 \text{ if } i \neq j),$$

where each M_i is of either of the following types:

(i) *a genus 1 quasi-polarized superspecial Dieudonné module over W generated by some x such that $e(x, Fx) = p^r \varepsilon$ for some $r \in \mathbb{Z}$ and $\varepsilon \in W \backslash pW$ with $\varepsilon^\sigma = -\varepsilon$; or*

(ii) *a genus* 2 *quasi-polarized superspecial Dieudonné module over* W *generated by some* x, y *such that* $e(x,y)=p^r$ *for some* $r\in\mathbb{Z}$, *and* $e(x,Fx)=e(y,Fy)=e(x,Fy)=e(y,Fx)=0$.

Corollary 9. *We have* $M(A'[p^\infty])\cong A_{1,1}^g$ *as principally quasi-polarized Dieudonné modules, where* $A_{1,1}^g$ *is endowed with the product quasi-polarization.*

Proof. In the direct sum decomposition of the proposition, the degree of the quasi-polarization on M is the product of the degrees of the quasi-polarizations of each of the summands. Since our M is principally quasi-polarized we conclude that each summand is also principally quasi-polarized, i.e. the bilinear form $\langle\,,\rangle$ is a perfect pairing on each summand.

Let M_0 be such a summand and suppose M_0 is of type (ii) from the proposition. This gives a W-basis for M_0 consisting of x, Fx, y and Fy. The quasi-polarization e defines a map $M_0\to M_0^t$ given by $z\mapsto f_z$, where $f_z(v):=e(z,v)$. Let x^t, $(Fx)^t$, y^t and $(Fy)^t$ be the dual basis to x, Fx, y and Fy. It is an easy computation to see that $f_x=p^ry^t$, $f_{Fx}=p^{r+1}(Fy)^t$, $f_y=-p^rx^t$ and $f_{Fy}=-p^{r+1}(Fx)^t$. For instance

$$f_{Fy}(Fx)=e(Fy,Fx)=e(y,VFx)^\sigma=e(y,px)^\sigma=-pe(x,y)^\sigma=-p^{r+1}.$$

But the map $M_0\to M_0^t$ given by $z\mapsto f_z$ is an isomorphism, hence $p^r=p^{r+1}=1$, contradiction.

So M has only summands of type (i). A similar (but even simpler) computation shows that each summand must have $e(x,Fx)=1$. □

Corollary 10. *Let* $M:=M(A'[p^\infty])$. *There exists an isomorphism between* $\mathrm{End}(M,e_0)^\times$ *and* $\mathrm{GU}_g(\mathcal{O}_p)$, *such that the subgroup of symplectic automorphisms which lift the identity map on* $(M/FM,e_0)$ *is identified with* U_p *defined by the short exact sequence*

$$1\to U_p\to \mathrm{GU}_g(\mathcal{O}_p)\to \mathrm{GU}_g(\mathbb{F}_{p^2})\to 1,$$

where the surjective map is reduction modulo the uniformizer π *of* $\mathcal{O}_p$.

Proof. Recall the identification $\mathrm{End}(A_{1,1})\cong\mathcal{O}_p$ from the proof of part (b) of Corollary 7:

$$\varphi:\ \mathrm{End}(A_{1,1})\to\mathcal{O}_p$$

$$\begin{pmatrix} x & y\\ -py^p & x^p\end{pmatrix}\mapsto x+\pi y.$$

On the other hand, any $T \in \mathrm{End}(M) = \mathrm{End}(A_{1,1}^g)$ is a $2g \times 2g$ matrix made of 2×2 blocks of the form $T_{ij} := \left(\begin{smallmatrix} x_{ij} & y_{ij} \\ -py_{ij}^p & x_{ij}^p \end{smallmatrix}\right)$. Therefore we have an isomorphism

$$\varphi: \quad \mathrm{End}(M)^\times \to \mathrm{GL}_g(\mathcal{O}_p)$$

$$T = (T_{ij})_{i,j} \mapsto (x_{ij} + \pi y_{ij})_{i,j}.$$

We want to prove that under this isomorphism, $\mathrm{End}(M, e_0)^\times$ corresponds to $\mathrm{GU}_g(\mathcal{O}_p)$. For this we use Corollary 9, which says that the bilinear form e_0 is given by the block-diagonal matrix

$$E_0 := \begin{pmatrix} 0 & 1 & & & & \\ -1 & 0 & & & & \\ & & \ddots & & & \\ & & & & 0 & 1 \\ & & & & -1 & 0 \end{pmatrix}.$$

Therefore we have

$$\mathrm{End}(M, e_0)^\times = \{T \in \mathrm{End}(M)^\times : T^t E_0 T = \gamma E_0,\ \gamma \in \mathbb{Z}_p\}.$$

Note that for the 2×2 block T_{ij} we have

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} T_{ij}^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} x_{ij}^p & -y_{ij} \\ py_{ij}^p & x_{ij} \end{pmatrix},$$

which maps under φ to $x_{ij}^p - \pi y_{ij} = \overline{x_{ij} + \pi y_{ij}} = \overline{\varphi(T_{ij})}$, where $\bar{\cdot}$ denotes the conjugation in the quaternion algebra $B_p := \mathcal{O}_p \otimes \mathbb{Q}_p$. This means that $E_0^{-1} T^t E_0$ maps to $\varphi(T)^*$, where we write $U^* = \overline{U^t}$. Putting it all together we conclude that for any $T \in \mathrm{End}(M)^\times$ we have

$$T \in \mathrm{End}(M, e_0)^\times \Leftrightarrow E_0^{-1} T^t E_0 T = \gamma \Leftrightarrow \varphi(T)^* \varphi(T) = \gamma$$

$$\Leftrightarrow \varphi(T) \in \mathrm{GU}_g(\mathcal{O}_p),$$

which is precisely what we wanted to show.

For the second part of the statement note that

$$M/FM = \{(0, a_1, 0, a_2, \ldots, 0, a_g)^t + FM : a_i \in \mathbb{F}_{p^2}\}.$$

Let $T = (T_{ij}) \in \mathrm{End}(M, e_0)^\times$, then its induced map on M/FM is

$$T((0, a_1, 0, a_2, \ldots, 0, a_g)^t + FM) = \left(0, \sum_j a_j \bar{x}_{1j}^p, \ldots, 0, \sum_j a_j \bar{x}_{gj}^p\right) + FM,$$

where $\bar{x}_{ij}$ denotes the reduction modulo π of x_{ij}. Therefore T induces the identity map on M/FM if and only if

$$\begin{pmatrix} \bar{x}_{11} & \bar{x}_{12} & \dots & \bar{x}_{1g} \\ \bar{x}_{21} & \bar{x}_{22} & \dots & \bar{x}_{2g} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{g1} & \bar{x}_{g2} & \dots & \bar{x}_{gg} \end{pmatrix} = 1.$$

But the matrix above is precisely the matrix of the reduction of $\varphi(T)$ modulo π, so T induces the identity on M/FM if and only if $\varphi(T) \in U_p$. □

2.3.4. Differentials defined over $\mathbb{F}_{p^2}$

We know from Proposition 6 that a principally polarized superspecial abelian variety (A, λ) has a canonical $\mathbb{F}_{p^2}$-structure (A', λ'). We therefore have a well-defined notion of invariant differentials on A defined over $\mathbb{F}_{p^2}$.

Lemma 11. *Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Then a non-zero invariant differential on E defined over $\mathbb{F}_{p^2}$ is equivalent to a choice of non-zero element of M/FM, where $M := M(E'[p^\infty])$ and E' is the canonical $\mathbb{F}_{p^2}$-structure of E.*

Proof. Differentials of E defined over $\mathbb{F}_{p^2}$ are by definition differentials of E', i.e. elements of the cotangent space $\omega(E')$. Since $E'[p]$ is a closed subgroup-scheme of E', there is a canonical surjection on cotangent spaces $\omega(E') \to \omega(E'[p]) \to 0$. Since both vector spaces have dimension one, this map is actually an isomorphism. Similarly, we get a canonical isomorphism $\omega(E'[p^\infty]) \cong \omega(E'[p])$, so we have identified $\omega(E')$ with $\omega(E'[p^\infty])$. By Fontaine [5, Proposition III.4.3], $\omega(E'[p^\infty])$ is canonically isomorphic to M/FM, so $\omega(E')$ is identified with M/FM. □

Proposition 12. *Let A be a superspecial abelian variety over $\overline{\mathbb{F}}_p$, let A' be its canonical $\mathbb{F}_{p^2}$-structure and $M := M(A'[p^\infty])$. Then giving a basis of invariant differentials on A defined over $\mathbb{F}_{p^2}$ is equivalent to giving a basis of M/FM over $\mathbb{F}_{p^2}$.*

Proof. The space of invariant differentials on A defined over $\mathbb{F}_{p^2}$ is by definition $\omega(A')$. We have $\omega(A') \cong \omega(E'^g) \cong \omega(E')^g$. By Lemma 11 we know that $\omega(E') \cong M(E'[p^\infty])/FM(E'[p^\infty])$, and since $M(A'[p^\infty]) \cong M(E'[p^\infty])^g$ we conclude that $\omega(A') \cong M/FM$. □

Note that as we have seen in Section 2.3.2, the presence of a principal polarization λ' on an $\mathbb{F}_{p^2}$-abelian variety A' induces a hermitian form on the g-dimensional $\mathbb{F}_{p^2}$-vector space M/FM. We say that a basis of invariant differentials on A defined over $\mathbb{F}_{p^2}$ is a basis of invariant differentials on (A, λ) if it respects this hermitian structure. We can therefore conclude that

Corollary 13. *Let (A,λ) be a principally polarized superspecial abelian variety over $\overline{\mathbb{F}}_p$, let (A',λ') be its canonical $\mathbb{F}_{p^2}$-structure and $M \coloneqq M(A'[p^\infty])$. Then giving a basis of invariant differentials on (A,λ) defined over $\mathbb{F}_{p^2}$ is equivalent to giving a hermitian basis of M/FM over $\mathbb{F}_{p^2}$.*

3. Construction of the bijection

Let A be a superspecial abelian variety of dimension g over $\overline{\mathbb{F}}_p$. Let $A' \cong E'^g$ be its canonical $\mathbb{F}_{p^2}$-structure, then $A \cong E^g$ for $E \coloneqq E' \otimes \overline{\mathbb{F}}_p$. Until further notice, we will write A to mean E^g and A' to mean E'^g. Let ${\lambda_0}'$ be the principal polarization on A' defined by the $g \times g$ identity matrix, let $\lambda_0 \coloneqq {\lambda_0}' \otimes \overline{\mathbb{F}}_p$, let $\alpha_0 : A[N] \to (\mathbb{Z}/N\mathbb{Z})^{2g}$ be a level N structure on A, and let η_0 be a basis of invariant differentials on (A,λ_0) defined over $\mathbb{F}_{p^2}$ (i.e. a hermitian basis of M/FM), where $M = M(A'[p^\infty])$. The various Weil pairings induced by λ_0, resp. ${\lambda_0}'$ will be denoted e_0, resp. ${e_0}'$.

Let Σ denote the finite set of isomorphism classes of pairs (λ,α), where λ is a principal polarization on A and α is a level N structure. Σ is a subscheme of X. We also define $\tilde{\Sigma}$ to be the set of isomorphism classes of triples (λ,α,η) with λ and α as above and η a basis of invariant differentials on (A,λ) defined over $\mathbb{F}_{p^2}$. Isomorphism is given by the condition $f'(\eta_2) = \eta_1$ and the commutativity of the diagrams

$$\begin{array}{ccc} A & \xrightarrow[\sim]{f} & A \\ {\scriptstyle\lambda_1}\downarrow{\scriptstyle\sim} & & {\scriptstyle\lambda_2}\downarrow{\scriptstyle\sim} \\ A^t & \xleftarrow[\sim]{f^t} & A^t \end{array} \qquad \begin{array}{ccc} (A[N],e_1) & \xrightarrow[\sim]{f} & (A[N],e_2) \\ {\scriptstyle\alpha_1}\downarrow{\scriptstyle\sim} & & {\scriptstyle\alpha_2}\downarrow{\scriptstyle\sim} \\ ((\mathbb{Z}/N\mathbb{Z})^{2g},\mathrm{std}) & = & ((\mathbb{Z}/N\mathbb{Z})^{2g},\mathrm{std}) \end{array},$$

where std denotes the standard symplectic pairing on the various modules.

Let $\mathcal{O} \coloneqq \mathrm{End}(E)$ and $B \coloneqq \mathcal{O} \otimes \mathbb{Q}$. Let $G \coloneqq \mathrm{GU}_g(B)$, and recall the notation of Section 2.1.3. The purpose of this section is to construct a bijection between the finite sets $\tilde{\Sigma}$ and $\Omega \coloneqq \Omega(N)$.

This construction is rather long, but the basic idea is that all principally polarized superspecial abelian varieties are isogenous, and that one can obtain local data by studying these isogenies at each prime ℓ (including p). The reader is encouraged to skip to Section 4.

Lemma 14. *Given any principal polarization λ on A, there exists an isogeny of principally polarized abelian varieties $\phi : (A,\lambda_0) \to (A,\lambda)$.*

Proof. We want an isogeny $\phi : A \to A$ such that $\phi^t \circ \lambda \circ \phi = m\lambda_0$ for some $m \in \mathbb{N}$.

There is an obvious bijective correspondence associating to a homomorphism $\psi : A \to A$ a matrix $\Psi \in M_g(\mathcal{O})$. Under this bijection, $\psi^t : A^t \to A^t$ corresponds to the

adjoint Ψ^*. If $\phi : A \to A$ is an isogeny, then $\Phi \in \mathrm{GL}_g(B)$. If $\lambda : A \to A^t$ is a polarization, then $\lambda^t = \lambda$ so $\Lambda^* = \Lambda$. Also Λ is positive-definite. If λ is a principal polarization, then $\Lambda \in \mathrm{GL}_g(\mathcal{O})$ defines a positive-definite quaternion hermitian form f. By Proposition 2 we know that Λ can be diagonalized, i.e. there exists $M \in \mathrm{GL}_g(B)$ such that $M^{-1}\Lambda M = \mathrm{diag}(\alpha_1, \ldots, \alpha_g)$, with $\alpha_i \in \mathbb{Q}$. The form f is positive-definite so $\alpha_i \in \mathbb{Q}_{>0}$. But the norm theorem (Theorem 3) says that the norm map is surjective onto $\mathbb{Q}_{>0}$, so by the last part of Proposition 2 there exists $M' \in \mathrm{GL}_g(B)$ such that $(M')^{-1}\Lambda M' = I$.

So there is a basis of B^g such that the quaternion hermitian form f is represented by the matrix I. But the matrices representing f are all of the form $Q^*\Lambda Q$ for $Q \in \mathrm{GL}_g(B)$. Now $B = \mathcal{O} \otimes \mathbb{Q}$ so there exists a positive integer n such that nQ has coefficients in $\mathcal{O}$. Let $\Phi = nQ$ and let $\phi : A \to A$ be the homomorphism corresponding to Φ. Since $\Phi \in \mathrm{GL}_g(B)$ and the fixed principal polarization λ_0 corresponds to the identity matrix, we conclude that ϕ is an isogeny and $\phi^t \circ \lambda \circ \phi = n^2$. □

Lemma 14 allows us to identify $\tilde{\Sigma}$ with the set $\tilde{\Sigma}^0$ consisting of isomorphism classes of triples

$$\phi : ((A, \lambda_0) \to (A, \lambda), \alpha : A[N] \to (\mathbb{Z}/N\mathbb{Z})^{2g}, \eta),$$

where $(A, \lambda_0) \xrightarrow{\phi} (A, \lambda)$ is an isogeny of principally polarized abelian varieties and isomorphism is defined by diagrams (1).

Proposition 15. *An isogeny $\phi_1 : (A, \lambda_0) \to (A, \lambda_1)$ defines for any prime $\ell \neq p$ an element $[x_\ell] \in U_\ell(N) \backslash G_\ell$. If $\ell \nmid \deg \phi_1$ then $[x_\ell] = 1$.*

Proof. Pick a prime $\ell \neq p$ and let n satisfy $\ell^n || N$. As we have seen in Section 2.3.2, ϕ induces an injective symplectic similitude $T_\ell \phi_1 : (T_\ell A, e_\ell^{\lambda_0}) \to (T_\ell A, e_\ell^{\lambda_1})$, with finite cokernel isomorphic to $(\ker \phi_1)_\ell$. To ease notation, we will just write e_0 for $e_\ell^{\lambda_0}$ and e_1 for $e_\ell^{\lambda_1}$ (and we use the same letters for the corresponding Weil pairings on $A[\ell^n]$).

Let $k_{\ell,1} : (T_\ell A, e_0) \to (T_\ell A, e_1)$ be a symplectic isomorphism whose restriction gives a commutative diagram

$$\begin{array}{ccc} (A[\ell^n], e_0) & \xrightarrow{k_{\ell,1}}_{\sim} & (A[\ell^n], e_1) \\ \alpha_0 \downarrow \sim & & \alpha_1 \downarrow \sim \\ (\mathbb{Z}/\ell^n\mathbb{Z})^{2g} & = & (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}. \end{array}$$

Let $x_\ell = k_{\ell,1}^{-1} \circ T_\ell \phi_1$, then $x_\ell : (T_\ell A, e_0) \to (T_\ell A, e_0)$ is a symplectic similitude and sits in the commutative diagram

$$\begin{array}{ccc} (T_\ell A, e_0) & \xrightarrow{T_\ell \phi_1} & (T_\ell A, e_1) \\ {\scriptstyle x_\ell}\downarrow & \overset{k_{\ell,1}}{\nearrow}_{\sim} & \\ (T_\ell A, e_0). & & \end{array} \tag{2}$$

The map x_ℓ is not necessarily invertible, but since its injective with finite cokernel it defines a symplectic automorphism of $(V_\ell A, e_0)$, i.e. $x_\ell \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) = G_\ell$. If $\ell \nmid \deg \phi$ then $T_\ell \phi$ is a symplectic isomorphism so we can take $x_\ell = 1$.

How does this depend on the particular choice of $k_{\ell,1}$? Let $\tilde{k}_{\ell,1} : (T_\ell A, e_0) \xrightarrow{\sim} (T_\ell A, e_1)$ be some other symplectic isomorphism that restricts to $\alpha_1^{-1} \circ \alpha_0$. Let

$$u := (\tilde{k}_{\ell,1})^{-1} \circ k_{\ell,1} \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) = U_\ell.$$

Note that u restricts to the identity on $A[\ell^n]$ so actually $u \in U_\ell(N)$. Conversely, if $u \in U_\ell(N)$ then $k_{\ell,1} \circ u^{-1} : (T_\ell A, e_0) \to (T_\ell A, e_1)$ is a symplectic isomorphism restricting to $\alpha_1^{-1} \circ \alpha$. Therefore ϕ_1 gives us a well-defined element $[x_\ell] \in U_\ell(N) \backslash G_\ell$. □

What happens at p? The isogeny ϕ_1 induces an injective symplectic similitude

$$M(\phi_1') : (M, e_1) \to (M, e_0)$$

with finite cokernel. Let $k_{p,1} : (M, e_1) \to (M, e_0)$ be a symplectic isomorphism whose reduction $(M/FM, e_1) \to (M/FM, e_0)$ maps η_1 to η_0. Set $x_p := M(\phi_1') \circ k_{p,1}^{-1}$, then the map $x_p : (M, e_0) \to (M, e_0)$ is an injective symplectic similitude with finite cokernel. Hence x_p induces a symplectic isomorphism of $(M \otimes \mathbb{Q}_p, e_0)$, so by Corollary 10, x_p gives an element of $\mathrm{GU}_g(B_p)$. Since $k_{p,1}$ is well-defined up to multiplication by U_p, we have that ϕ_1 defines a element $[x_p] \in U_p \backslash \mathrm{GU}_g(B_p)$.

Lemma 16. *Any two isogenies $\phi_1, \tilde{\phi}_1 : (A, \lambda_0) \to (A, \lambda_1)$ are related by $\tilde{\phi}_1 = \phi_1 \circ u$, where u corresponds to a matrix $U \in \mathrm{GU}_g(B)$.*

Proof. Suppose ϕ_1, $\tilde{\phi}_1$ satisfy

$$\phi_1^t \circ \lambda_1 \circ \phi_1 = m\lambda_0,$$

$$\tilde{\phi}_1^t \circ \lambda_1 \circ \tilde{\phi}_1 = \tilde{m}\lambda_0.$$

We treat $\phi_1, \tilde{\phi}_1$ as quasi-isogenies, i.e. elements of $\mathrm{End}(A) \otimes \mathbb{Q}$. Let $n = \deg \phi_1$, then we have that as quasi-isogenies:

$$\left(\hat{\phi}_1 \otimes \frac{1}{n}\right) \circ \phi_1 = n \otimes \frac{1}{n} = 1 = \phi_1 \circ \left(\hat{\phi}_1 \otimes \frac{1}{n}\right).$$

We can therefore write $\phi_1^{-1} = \hat{\phi}_1 \otimes \frac{1}{n}$ and we have shown that any isogeny has an inverse quasi-isogeny—actually a trivial modification of the argument shows that any quasi-isogeny is invertible. Set $u \coloneqq \phi_1^{-1} \circ \tilde{\phi}_1 \in (\mathrm{End}(A) \otimes \mathbb{Q})^\times$.

Denote by capital letters the matrices corresponding to the various maps. We have

$$U^* U = \tilde{\Phi}_1^* (\Phi_1^{-1})^* \Phi_1^{-1} \tilde{\Phi}_1 = \tilde{\Phi}_1^* \left(\frac{1}{m} \Lambda_1\right) \tilde{\Phi}_1 = \frac{\tilde{m}}{m} I$$

so $U \in \mathrm{GU}_g(B)$. □

The next lemma says that we have indeed constructed a map

$$\gamma : \tilde{\Sigma}^0 \to \Omega = U \backslash G(\hat{\mathbb{Q}}) / G(\mathbb{Q}).$$

Lemma 17. *The map γ is well-defined.*

Proof. We need to show that γ only depends on the isomorphism class $[\phi_1, \alpha_1, \eta_1]$. Suppose $f : (\phi_1, \alpha_1, \eta_1) \to (\phi_2, \alpha_2, \eta_2)$ is an isomorphism of triples. By Lemma 16 we can assume without loss of generality that $\phi_2 = f \circ \phi_1$. For $\ell \neq p$, we get the following diagrams

$$\begin{array}{ccccc}
 & & T_\ell\phi_2 & & \\
 & \overset{}{\nearrow} & & \overset{}{\searrow} & \\
(T_\ell A, e_0) & \xrightarrow{T_\ell\phi_1} & (T_\ell A, e_1) & \xrightarrow[\sim]{T_\ell f} & (T_\ell A, e_2) \\
{\scriptstyle x_\ell}\downarrow & & \uparrow{\scriptstyle k_{\ell,1}}\sim & & \uparrow{\scriptstyle k_{\ell,2}}\sim \\
(T_\ell A, e_0) & = & (T_\ell A, e_0) & = & (T_\ell A, e_0)
\end{array}
\qquad
\begin{array}{ccccc}
 & & k_{\ell,2} & & \\
 & \overset{}{\nearrow} & \sim & \overset{}{\searrow} & \\
(A[\ell^n], e_0) & \xrightarrow[\sim]{k_{\ell,1}} & (A[\ell^n], e_1) & \xrightarrow[\sim]{T_\ell f} & (A[\ell^n], e_2) \\
{\scriptstyle \alpha_0}\downarrow\sim & & {\scriptstyle \alpha_1}\downarrow\sim & & {\scriptstyle \alpha_2}\downarrow\sim \\
(\mathbb{Z}/\ell^n\mathbb{Z})^{2g} & = & (\mathbb{Z}/\ell^n\mathbb{Z})^{2g} & = & (\mathbb{Z}/\ell^n\mathbb{Z})^{2g},
\end{array}$$

where $k_{\ell,2} \coloneqq T_\ell f \circ k_{\ell,1}$. It is now clear that we end up with the same $x_\ell \in \mathcal{C}_\ell^\times(N) \backslash B_\ell^\times$ as the one obtained from ϕ_1. The exact same thing happens at the prime p. □

3.1. The inverse map

We need to construct an inverse. Let $[x] \in \Omega$ and pick a representative $x = (x_v) \in G(\hat{\mathbb{Q}})$. Let $\ell \neq p$. We have $x_\ell \in G(\mathbb{Q}_\ell) = \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) = \mathrm{Aut}(V_\ell, e_0)$. Let $n_\ell \in \mathbb{Z}$ be the smallest integer such that $y_\ell \coloneqq \ell^{n_\ell} x_\ell \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) = \mathrm{End}(T_\ell A, e_0)$. The endomorphism y_ℓ is injective with finite cokernel C_ℓ. Let ℓ^k be the order of C_ℓ. Let K_ℓ be

the kernel of the map induced by y_ℓ on $A[\ell^k]$:

$$0 \to K_\ell \to A[\ell^k] \xrightarrow{y_\ell} A[\ell^k] \to C_\ell \to 0.$$

For $\ell = p$ we have $x_p \in \mathrm{GU}_g(B_p) = (\mathrm{End}(M, e_0) \otimes \mathbb{Q}_p)^\times$. Write $x_p = a + \pi b$, where $a, b \in M_g(L_p)$ and $\pi^2 = -p$. We have $a = \sum_i a_i \otimes \frac{1}{p^i}$ and $b = \sum_j b_j \otimes \frac{1}{p^j}$, with $a_i, b_j \in \mathrm{End}(M, e_0)$. Let $n_p \in \mathbb{Z}$ be the smallest integer such that

$$p^{n_p} x_p = (a' \otimes 1) + \pi(b' \otimes 1)$$

and set $y_p := a' + \pi b' \in \mathrm{End}(M, e_0)$. This y_p is an endomorphism of the Dieudonné module M which induces an automorphism of $M \otimes \mathbb{Q}_p$, therefore this endomorphism must be injective with finite cokernel C_p. Let p^k be the order of C_p, then y_p induces a map

$$M(A[p^k]) \xrightarrow{y_p} M(A[p^k]) \to C_p \to 0.$$

Then C_p is the Dieudonné module of a subgroup scheme K_p of A of rank p^k.

Since $x \in G(\hat{\mathbb{Q}})$, $n_\ell = 0$ for all but finitely many ℓ. Therefore, it makes sense to set $q := \prod \ell^{n_\ell} \in \mathbb{Q}^\times$ and $y := xq$; the ℓth component of y is precisely the y_ℓ above, and clearly $[x] = [y]$. Now set $K := \oplus K_\ell$, then K is a finite subgroup of A. So to the given $[x] \in \Omega$ we can associate the quotient isogeny $A \to A/K$. After picking an isomorphism $A/K \cong A$ we get an isogeny $\phi : A \to A$, and this induces a principal polarization λ on A such that ϕ is an isogeny of polarized abelian varieties. For $\ell \neq p$, our construction gives for any positive integer m

$$\begin{array}{ccccccc}
0 & \longrightarrow & \ker & \longrightarrow & (A[\ell^m], e_0) & \xrightarrow{\phi} & (A[\ell^m], e) \\
 & & \| & & \| & & \\
0 & \longrightarrow & \ker & \longrightarrow & (A[\ell^m], e_0) & \xrightarrow{y_\ell} & (A[\ell^m], e_0).
\end{array}$$

Due to the structure of ℓ^m-torsion, it is not hard to see that one can construct a symplectic isomorphism (actually, there exist many of them) $(A[\ell^m], e_0) \cong (A[\ell^m], e)$ which makes the above diagram commute. On the level of Tate modules, we get

$$\begin{array}{ccccc}
0 & \longrightarrow & (T_\ell A, e_0) & \xrightarrow{T_\ell \phi} & (T_\ell A, e) \\
 & & \| & & \uparrow{\scriptstyle k_\ell}\,{\scriptstyle \sim} \\
0 & \longrightarrow & (T_\ell A, e_0) & \xrightarrow{y_\ell} & (T_\ell A, e_0).
\end{array}$$

In particular, we can set $\alpha := \alpha_0 \circ k_\ell^{-1}$, then the symplectic isomorphisms

$$\alpha : (A[\ell^n], e) \xrightarrow{\sim} ((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \text{std})$$

for $\ell | N$ piece together to give a level N structure on (A, λ).

For $\ell = p$ we have similarly

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (M, e) & \xrightarrow{M(\phi)} & (M, e_0) & \longrightarrow & \operatorname{coker} M(\phi) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle k_p}\wr & & \| & & \downarrow\wr & & \\ 0 & \longrightarrow & (M, e_0) & \xrightarrow{y_p} & (M, e_0) & \longrightarrow & C_p & \longrightarrow & 0, \end{array}$$

and $\eta := k_p^{-1}(\eta_0)$ gives a non-zero invariant differential on (A, λ).

The next result tells us that we have indeed constructed a map $\delta : \Omega \to \tilde{\Sigma}^0$.

Proposition 18. *The map δ is well-defined.*

Proof. First suppose that $\bar{x} = xu$, where $u \in \operatorname{End}(A, \lambda_0)$ is not divisible by any rational prime. Let $\ell \neq p$, then $\bar{x}_\ell = x_\ell u$, so $\bar{y}_\ell = y_\ell u$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (T_\ell A, e_0) & \xrightarrow{y_\ell} & (T_\ell A, e_0) & \longrightarrow & C_\ell & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle u} & & \| & & \uparrow{\scriptstyle v_\ell} & & \\ 0 & \longrightarrow & (T_\ell A, e_0) & \xrightarrow{\bar{y}_\ell} & (T_\ell A, e_0) & \longrightarrow & \bar{C}_\ell & \longrightarrow & 0. \end{array}$$

The snake lemma gives $\operatorname{coker} v_\ell = 0$, $\ker v_\ell \cong \operatorname{coker} u$. Let ℓ^k be the order of $\bar{C}_\ell$, then we can restrict the above diagram to the ℓ^k-torsion and get

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_\ell & \longrightarrow & (A[\ell^k], e_0) & \xrightarrow{y_\ell} & (A[\ell^k], e_0) & \longrightarrow & C_\ell & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle g_\ell} & & \uparrow{\scriptstyle u_\ell} & & \| & & \uparrow{\scriptstyle v_\ell} & & \\ 0 & \longrightarrow & \bar{K}_\ell & \longrightarrow & (A[\ell^k], e_0) & \xrightarrow{\bar{y}_\ell} & (A[\ell^k], e_0) & \longrightarrow & \bar{C}_\ell & \longrightarrow & 0, \end{array}$$

where u_ℓ is the restriction of u to $A[\ell^k]$ and g_ℓ is the restriction of u to $\bar{K}_\ell$. Note that $\operatorname{coker}(u_\ell : T_\ell A \to T_\ell A) = \operatorname{coker}(u : A[\ell^k] \to A[\ell^k])$. Since there is no snake lemma for diagrams of long exact sequences, we split the above diagram in two:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_\ell & \longrightarrow & (A[\ell^k], e_0) & \longrightarrow & (A[\ell^k], e_0)/\ker y_\ell & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle g_\ell} & & \uparrow{\scriptstyle u_\ell} & & \uparrow{\scriptstyle h_\ell} & & \\ 0 & \longrightarrow & \bar{K}_\ell & \longrightarrow & (A[\ell^k], e_0) & \longrightarrow & (A[\ell^k], e_0)/\ker \bar{y}_\ell & \longrightarrow & 0, \end{array} \tag{3}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Im} y_\ell & \longrightarrow & (A[\ell^k], e_0) & \longrightarrow & C_\ell & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle h_\ell} & & \| & & \uparrow{\scriptstyle v_\ell} & & \\ 0 & \longrightarrow & \operatorname{Im} \bar{y}_\ell & \longrightarrow & (A[\ell^k], e_0) & \longrightarrow & \bar{C}_\ell & \longrightarrow & 0, \end{array} \tag{4}$$

where we have taken the liberty of using the same label h_ℓ for two maps which are canonically isomorphic. We first apply the snake lemma to diagram 4 and get $\ker h_\ell = 0$, $\operatorname{coker} h_\ell \cong \ker v_\ell$. Using this information together with the snake lemma in diagram 3 gives

$$\ker g_\ell \cong \ker u_\ell, \quad 0 \to \operatorname{coker} g_\ell \to \operatorname{coker} u_\ell \to \operatorname{coker} h_\ell \to 0.$$

But we already have $\operatorname{coker} u_\ell = \operatorname{coker} u \cong \ker v_\ell \cong \operatorname{coker} h_\ell$ so the short exact sequence above becomes $0 \to \operatorname{coker} g_\ell \to 0$, i.e. $\operatorname{coker} g_\ell = 0$.

Let $g \coloneqq \oplus g_\ell : \bar{K} \to K$ and let $f : (A, \bar{\lambda}) \to (A, \lambda)$ be defined by the diagram

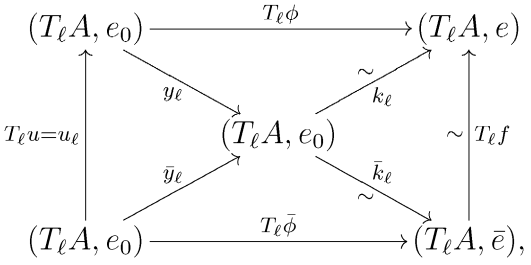
$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & (A, \lambda_0) & \xrightarrow{\phi} & (A, \lambda) & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle u} & & \uparrow{\scriptstyle f} & & \\ 0 & \longrightarrow & \bar{K} & \longrightarrow & (A, \lambda_0) & \xrightarrow{\bar{\phi}} & (A, \bar{\lambda}) & \longrightarrow & 0, \end{array}$$

where we use some isomorphism $A/\bar{K} \cong A$ to define the isogeny $\bar{\phi}$ and the principal polarization $\bar{\lambda}$. We apply the snake lemma and get an exact sequence

$$0 \to \ker g \to \ker u \to \ker f \to \operatorname{coker} g = 0 \to \operatorname{coker} u = 0 \to \operatorname{coker} f \to 0.$$

But the map $\ker g \to \ker u$ is the sum of the isomorphisms $\ker g_\ell \cong \ker u_\ell$, so $\ker u \to \ker f$ is the zero map; therefore $\ker f = 0$. Clearly $\operatorname{coker} f = 0$, so f is an isomorphism.

We check that this isomorphism preserves level N structures. We have a diagram



where we know that the outer square commutes, and that the triangles situated over, to the left, and under the central $(T_\ell A, e_0)$ commute. Therefore the triangle to the right of the central $(T_\ell A, e_0)$ also commutes, i.e. $k_\ell = T_\ell f \circ \bar{k}_\ell$. The level N structures on (A, λ) and $(A, \bar{\lambda})$ are defined in such a way that the inner squares in the following

diagram commute:

$$\begin{array}{ccccc}
 & & \overset{f}{\overset{\sim}{\frown}} & & \\
(A[\ell^n], e) & \xrightarrow[\sim]{k_\ell^{-1}} & (A[\ell^n], e_0) & \xrightarrow[\sim]{\bar{k}_\ell} & (A[\ell^n], \bar{e}) \\
\alpha\downarrow\sim & & \alpha_0\downarrow\sim & & \bar{\alpha}\downarrow\sim \\
((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \mathrm{std}) & = & ((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \mathrm{std}) & = & ((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \mathrm{std}),
\end{array}$$

therefore the outer rectangle also commutes, i.e. f preserves the level N structures.

The same argument with reversed arrows shows that f preserves differentials.

Now suppose $\bar{x} = x\ell$, $\ell \neq p$ (the case $\ell = p$ is analogous, even easier). If $\ell' \nmid \ell p$, then $\bar{x}_{\ell'} = x_{\ell'}\ell$ and $\bar{y}_{\ell'} = y_{\ell'}\ell$. Multiplication by ℓ is an isomorphism of $(T_{\ell'}A, e_0)$, so it induces an isomorphism $\bar{K}_{\ell'} \cong K_{\ell'}$ by applying the same argument as before on the diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & K_{\ell'} & \longrightarrow & (A[\ell'^k], e_0) & \xrightarrow{y_{\ell'}} & (A[\ell'^k], e_0) & \longrightarrow & C_{\ell'} & \longrightarrow & 0 \\
 & & g_{\ell'}\uparrow\sim & & \ell\uparrow\sim & & \| & & v_{\ell'}\uparrow\sim & & \\
0 & \longrightarrow & \bar{K}_{\ell'} & \longrightarrow & (A[\ell'^k], e_0) & \xrightarrow{\bar{y}_{\ell'}} & (A[\ell'^k], e_0) & \longrightarrow & \bar{C}_{\ell'} & \longrightarrow & 0.
\end{array}$$

Something similar occurs at p. If $\ell' = \ell$, we get $\bar{x}_\ell = x_\ell\ell$ and $\bar{y}_\ell = y_\ell$ so $\bar{K}_\ell = K_\ell$. We have an isomorphism $\bar{K} \cong K$ so $(A, \bar{\lambda}) \cong (A, \lambda)$. We need to check that this isomorphism is compatible with the level structures and the differentials. Let $\ell' \nmid \ell p$, then we have a diagram

$$\begin{array}{ccccc}
 & & \overset{\ell}{\overset{\sim}{\frown}} & & \\
(T_{\ell'}A, e) & \xleftarrow{k_{\ell'}} & (T_{\ell'}A, e_0) & \xrightarrow{\bar{k}_{\ell'}} & (T_{\ell'}A, \bar{e}) \\
\alpha\downarrow & & \alpha_0\downarrow & & \bar{\alpha}\downarrow \\
((\mathbb{Z}/\ell'^n\mathbb{Z})^{2g}, \mathrm{std}) & = & ((\mathbb{Z}/\ell'^n\mathbb{Z})^{2g}, \mathrm{std}) & = & ((\mathbb{Z}/\ell'^n\mathbb{Z})^{2g}, \mathrm{std}).
\end{array}$$

Since the top "triangle" commutes, we see that the level structures commute with the isomorphism. The same thing happens at p. When $\ell' = \ell$, then $\bar{K}_\ell = K_\ell$ so we get the same diagram as above, except that the top isomorphism is actually the identity map.

It remains to check the local choices. The group C_ℓ (therefore K_ℓ) depends on the chosen isomorphism $(T_\ell A, e_0) \cong (\mathbb{Z}_\ell^{2g}, \mathrm{std})$, and this can change y_ℓ by right multiplication by an element of $U_\ell(N)$. Suppose we have another such candidate

$\bar{y}_\ell = u_\ell y_\ell$, then we would get a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (T_\ell A, e_0) & \xrightarrow{y_\ell} & (T_\ell A, e_0) & \longrightarrow & C_\ell & \longrightarrow & 0 \\ & & \| & & \uparrow{\scriptstyle u_\ell}\wr & & \uparrow{\scriptstyle v_\ell}\wr & & \\ 0 & \longrightarrow & (T_\ell A, e_0) & \xrightarrow{\bar{y}_\ell} & (T_\ell A, e_0) & \longrightarrow & \bar{C}_\ell & \longrightarrow & 0, \end{array}$$

from which we conclude as before that $\bar{K}_\ell \cong K_\ell$ and $(A, \bar{\lambda}) \cong (A, \lambda)$. For the level N structure, we have the diagram

$$\begin{array}{ccccc} & & \overset{\alpha}{\frown} & & \\ (A[\ell^n], e) & \xrightarrow{k_\ell^{-1}} & (A[\ell^n], e_0) & \xrightarrow{\alpha_0} & ((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \mathrm{std}) \\ \downarrow\wr & & \| & & \| \\ (A[\ell^n], \bar{e}) & \xrightarrow{(\bar{k}_\ell)^{-1}} & (A[\ell^n], e_0) & \xrightarrow{\alpha_0} & ((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \mathrm{std}) \\ & & \underset{\bar{\alpha}}{\smile} & & \end{array}$$

and a similar argument holds for the η and $\bar{\eta}$. □

Lemma 19. *The map γ is bijective with inverse δ.*

Proof. Suppose we started with $[x] \in \Omega$ and got $[(A, \lambda_0) \xrightarrow{\phi} (A, \lambda), \alpha, \eta]$. For $\ell \neq p$ we get the exact sequence

$$0 \to (T_\ell A, e_0) \xrightarrow{T_\ell \phi} (T_\ell A, e) \to \operatorname{coker} T_\ell \phi \to 0.$$

We see from diagram (3.1) that $y_\ell = k_\ell^{-1} \circ T_\ell \phi$, where k_ℓ is an isomorphism that restricts to $\alpha^{-1} \circ \alpha_0$. Therefore $[y_\ell]$ is exactly the local element that is obtained in the computation of $\gamma([\phi, \alpha, \eta])$. The same thing happens at p, so indeed $\gamma \circ \delta = 1$.

Conversely, suppose we start with a triple $((A, \lambda_0) \xrightarrow{\phi} (A, \lambda), \alpha, \eta)$. We get local elements x_ℓ forming an adèle x. We have $\ker \phi = \prod_\ell \operatorname{coker} x_\ell$. Now when we apply δ we already have $x_\ell \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ so $y_\ell = x_\ell$ and $K = \oplus \operatorname{coker} x_\ell = \ker \phi$. We get an isogeny $(A, \lambda_0) \to (A, \bar{\lambda})$ which has the same kernel as ϕ, therefore $(A, \bar{\lambda}) \cong (A, \lambda)$. It is clear from the construction of δ that the level N structure and the invariant differential will stay the same. □

We have just proved

Theorem 20. *There is a canonical bijection $\tilde{\Sigma}^0 \to \Omega$.*

3.2. Compatibilities

We now turn to the proof of the following result:

Theorem 21. *The canonical bijection $\gamma : \tilde{\Sigma}^0(N) \to \Omega(N)$ is compatible with the action of the Hecke algebra, with the action of $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$, and with the operation of raising the level.*

3.2.1. Hecke action

In this section ℓ will denote a fixed prime not dividing pN. We have given the definition of the Hecke operators in Section 2.2.2; we start this section by making the definition more explicit.

If $HgH \in \mathscr{H}_\ell$, we denote by $\det(HgH)$ the ℓ-part of the determinant of any representative of HgH. The action of $\mathscr{H}_\ell$ on $\tilde{\Sigma}^0$ is defined as follows. If $\det(HgH) > 1$, let C be a subgroup of A of type HgH and let $[(A, \lambda_0) \xrightarrow{\phi} (A, \lambda), \alpha, \eta] \in \tilde{\Sigma}^0$. The abelian variety A/C is also superspecial, so it can be identified with A. We denote by ψ_C the composition $A \to A/C \cong A$, and we denote by λ_C the principal polarization induced on the image A. We set

$$T_{HgH}([(A, \lambda_0) \xrightarrow{\phi} (A, \lambda), \alpha, \eta]) \coloneqq \sum_{C \text{ of type } HgH} [(A, \lambda_0) \xrightarrow{\phi} (A, \lambda) \xrightarrow{\psi_C} (A, \lambda_C), \alpha_C, \eta_C],$$

where $\eta_C \coloneqq M({\psi_C}')^{-1}(\eta)$, and α_C is defined by the diagram:

$$\begin{array}{ccc} (A[N], e) & \xrightarrow[\sim]{\psi_C} & (A[N], e_C) \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha_C} \\ ((\mathbb{Z}/N\mathbb{Z})^{2g}, \mathrm{std}) & = & ((\mathbb{Z}/N\mathbb{Z})^{2g}, \mathrm{std}). \end{array} \tag{5}$$

Note that these definitions make sense because $(\deg \psi_C, pN) = 1$.

Now suppose $\det(HgH) < 1$. Given C a subgroup of A of type $Hg^{-1}H$, let ψ_C be the composition $A \to A/C \cong A$ and let $\hat{\psi}_C : A \to A$ be the dual isogeny to ψ_C. Given a principal polarization λ on A, there is a principal polarization λ_C on A such that the following diagram commutes:

$$\begin{array}{ccc} A & \xleftarrow{\hat{\psi}_C} & A \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\lambda_C} \\ A^t & \xrightarrow{(\hat{\psi}_C)^t} & A^t. \end{array}$$

The action is defined by

$$T_{HgH}([(A,\lambda_0)\xrightarrow{\phi}(A,\lambda),\alpha,\eta]) \coloneqq \sum_{C \text{ of type } Hg^{-1}H} [(A,\lambda_0)\xrightarrow{\phi}(A,\lambda)\xleftarrow{\hat{\psi}_C}(A,\lambda_C),\lambda_C,\alpha_C,\eta_C],$$

where $\eta_C = M(\hat{\psi}_C{}')(\eta)$, and α_C is defined by the diagram

$$\begin{array}{ccc} (A[N],e) & \xleftarrow[\sim]{\hat{\psi}_C} & (A[N],e_C) \\ \alpha\downarrow & & \downarrow\alpha_C \\ ((\mathbb{Z}/N\mathbb{Z})^{2g},\mathrm{std}) & = & ((\mathbb{Z}/N\mathbb{Z})^{2g},\mathrm{std}). \end{array} \tag{6}$$

The algebra $\mathscr{H}_\ell$ acts on $H\backslash G$ as follows: let $HgH = \coprod_i Hg_i$, let $Hx \in H\backslash G$ and choose a representative $x \in Hx$. Then there exist representatives $g_i \in Hg_i$ such that $T_{HgH}(Hx) = \sum_i Hg_i x$. The algebra $\mathscr{H}_\ell$ acts on Ω by acting on the component Hx_I of $[x] \in \Omega$.

Lemma 22. *The bijection $\gamma : \tilde{\Sigma}^0 \to \Omega$ is compatible with the action of the local Hecke algebra $\mathscr{H}_\ell$, i.e. for all $HgH \in \mathscr{H}_\ell$ and $[\phi,\alpha,\eta]$ we have*

$$\gamma(T_{HgH}([\phi,\alpha,\eta])) = T_{HgH}(\gamma([\phi,\alpha,\eta])).$$

Proof. Let $HgH \in \mathscr{H}_\ell$, let $[(A,\lambda_0)\xrightarrow{\phi}(A,\lambda),\alpha,\eta] \in \Sigma^0$ and let $[x] \coloneqq \gamma([\phi,\alpha,\eta])$.

Suppose at first that $\det(HgH) > 1$ and let C be a subgroup of A of type HgH. Let $[x_C] \coloneqq \gamma([\psi_C \circ \phi, \alpha_C, \eta_C])$. If $(\ell', p\ell) = 1$, we have a diagram

$$\begin{array}{ccccc} (T_{\ell'}A,e_0) & \xrightarrow{T_{\ell'}\phi} & (T_{\ell'}A,e) & \xrightarrow[\sim]{T_{\ell'}\psi_C} & (T_{\ell'}A,e_C). \\ x_{\ell'}\downarrow & \overset{k_{\ell'}}{\nearrow}_{\sim} & & & \\ (T_{\ell'}A,e_0) & & & & \end{array}$$

Since $(T_{\ell'}\psi_C)\circ k_{\ell'} : (T_{\ell'}A,e_0) \to (T_{\ell'}A,e_C)$ is a symplectic isomorphism restricting to $\alpha_C^{-1}\circ\alpha_0$ (see diagram 5), we get that $[x_{C,\ell'}] = [x_{\ell'}]$.

A similar argument, based on the following diagram, shows that $[x_{C,p}] = [x_p]$:

$$\begin{array}{ccccc} (M,e_C) & \xrightarrow[\sim]{M(\psi'_C)} & (M,e) & \xrightarrow{M(\phi')} & (M,e_0) \\ & & & \overset{k_p}{\searrow}_{\sim} & \uparrow x_p \\ & & & & (M,e_0). \end{array}$$

We now figure out what happens at ℓ. Fix $x_\ell \in Hx_\ell$, then the symplectic isomorphism $k_\ell : (T_\ell A, e_0) \to (T_\ell A, e)$ is fixed and allows us to identify these two symplectic $\mathbb{Z}_\ell$-modules. Choose a symplectic isomorphism $k_C : (T_\ell A, e) \to (T_\ell A, e_C)$ and set $y_C \coloneqq k_C^{-1} \circ T_\ell \psi_C$. Via the identification k_ℓ, y_C induces a map $z_C : (T_\ell A, e_0) \to (T_\ell A, e_0)$. We have a diagram

$$\begin{array}{ccccc}
(T_\ell A, e_0) & \xrightarrow{T_\ell \phi} & (T_\ell A, e) & \xrightarrow{T_\ell \psi_C} & (T_\ell A, e_C). \\
\downarrow{\scriptstyle x_\ell} & \overset{\sim}{\nearrow}{\scriptstyle k_\ell} & \downarrow{\scriptstyle y_C} & \overset{\sim}{\nearrow}{\scriptstyle k_C} & \\
(T_\ell A, e_0) & & (T_\ell A, e) & & \\
\downarrow{\scriptstyle z_C} & \overset{\sim}{\nearrow}{\scriptstyle k_\ell} & & & \\
(T_\ell A, e_0) & & & &
\end{array}$$

Since $k_C \circ k_\ell$ is a symplectic isomorphism $(T_\ell A, e_0) \to (T_\ell A, e_C)$ and $z_C \circ x_\ell$ satisfies all the properties $x_{C,\ell}$ should, we conclude that $Hx_{C,\ell} = Hz_C x_\ell$. The assumption that C is of type HgH implies that $Hz_C \subset HgH$.

It remains to show that the map $C \mapsto Hz_C$ gives a bijection between the set of subgroups C of A of type HgH and the set of right cosets Hz contained in HgH. We start by constructing an inverse map. Let $Hz \subset HgH$ and pick a representative z. This corresponds to a map $z : (T_\ell A, e_0) \to (T_\ell A, e_0)$, and hence induces via k_ℓ a map $y : (T_\ell A, e) \to (T_\ell A, e)$. We use the same construction as in the definition of the inverse map δ in Section 3.1 to get a subgroup C of A which is canonically isomorphic to the cokernel of y. This C will be of type HgH because $Hz \subset HgH$. The proof of the bijectivity of $C \mapsto z_C$ is now the same as the proof of Lemma 19.

It remains to deal with the case $\det(HgH) < 1$. This works essentially the same, except that various arrows are reversed. We illustrate the point by indicating how to obtain the equivalent of the map $C \mapsto Hz_C$ in this setting. Let C be a subgroup of A of type $Hg^{-1}H$. This defines a new element of $\tilde{\Sigma}^0$ which we denote by $[\hat{\psi}_C^{-1} \circ \phi, \alpha_C, \eta_C]$ (by a slight abuse of notation since $\hat{\psi}_C$ is not invertible as an isogeny). Let $[x_C] \coloneqq \gamma([\hat{\psi}_C^{-1} \circ \phi, \alpha_C, \eta_C])$. If $(\ell', p\ell) = 1$, we have a diagram

$$\begin{array}{ccccc}
(T_{\ell'} A, e_0) & \xrightarrow{T_{\ell'} \phi} & (T_{\ell'} A, e) & \xleftarrow[\sim]{T_{\ell'} \hat{\psi}_C} & (T_{\ell'} A, e_C). \\
\downarrow{\scriptstyle x_{\ell'}} & \overset{\sim}{\nearrow}{\scriptstyle k_{\ell'}} & & & \\
(T_{\ell'} A, e_0) & & & &
\end{array}$$

Since $(T_{\ell'} \hat{\psi}_C)^{-1} \circ k_{\ell'} : (T_{\ell'} A, e_0) \to (T_{\ell'} A, e_C)$ is a symplectic isomorphism restricting to $\alpha_C^{-1} \circ \alpha_0$ (see diagram 6), we get that $[x_{C,\ell'}] = [x_{\ell'}]$. The situation at p is similar and we have $[x_{C,p}] = [x_p]$.

What about ℓ? As before, we fix $x_\ell \in Hx_\ell$ and with it the symplectic isomorphism $k_\ell : (T_\ell A, e_0) \to (T_\ell A, e)$. Choose a symplectic isomorphism $k_C : (T_\ell A, e) \to (T_\ell A, e_C)$

and set $y_C \coloneqq T_\ell\hat{\psi}_C \circ k_C$. Via the identification k_ℓ, y_C induces a map $z_C : (T_\ell A, e_0) \to (T_\ell A, e_0)$. We have a diagram

$$\begin{array}{ccccc}
(T_\ell A, e_0) & \xrightarrow{T_\ell\phi} & (T_\ell A, e) & \xleftarrow{T_\ell\hat{\psi}_C} & (T_\ell A, e_C). \\
\downarrow{\scriptstyle x_\ell} & \overset{\sim}{\nearrow}{\scriptstyle k_\ell} & \uparrow{\scriptstyle y_C} & \overset{\sim}{\nearrow}{\scriptstyle k_C} & \\
(T_\ell A, e_0) & & (T_\ell A, e) & & \\
\uparrow{\scriptstyle z_C} & \overset{\sim}{\nearrow}{\scriptstyle k_\ell} & & & \\
(T_\ell A, e_0) & & & &
\end{array}$$

It is now clear that $z_C \circ x_{C,\ell} = x_\ell$. z is only defined up to right multiplication by elements of H (because of the choice of k_C), so we get the formula $Hx_{C,\ell} = Hz_C^{-1}x_\ell$. The assumption that C is of type $Hg^{-1}H$ guarantees that $Hz_C^{-1} \subset HgH$. The rest of the proof proceeds similarly to the case $\det(HgH) > 1$. □

3.2.2. Action of $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$

Within this section we will write G to denote $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$. The group G acts on $\tilde{\Sigma}^0$ by $g \cdot [\phi, \lambda, \alpha, \eta] \coloneqq [\phi, \lambda, g \circ \alpha, \eta]$.

The action on Ω is more delicate. It is easy to see that since $U_\ell = \mathrm{Aut}(T_\ell A, e_0)$, we have $U_\ell(N)\backslash U_\ell = \mathrm{Aut}(A[\ell^n], e_0)$, where $\ell^n || N$. Our fixed symplectic isomorphism $\alpha_0 : (A[N], e_0) \to ((\mathbb{Z}/N\mathbb{Z})^{2g}, \mathrm{std})$ identifies G with $\mathrm{Aut}(A[N], e_0)$ via $g \mapsto \alpha_0^{-1} \circ g \circ \alpha_0$. Therefore we get an identification

$$G \xrightarrow{\sim} \prod_\ell U_\ell(N)\backslash U_\ell$$

$$g \mapsto \prod_\ell U_\ell(N)(\alpha_0^{-1} \circ g \circ \alpha_0),$$

where the product is finite since the terms with $\ell \nmid N$ are 1. The action of G on Ω is then given by

$$g \cdot \left[\prod_\ell U_\ell(N)x_\ell\right] \coloneqq \left[\prod_\ell U_\ell(N)(\alpha_0^{-1} \circ g \circ \alpha)x_\ell\right].$$

Lemma 23. *The bijection* $\gamma : \tilde{\Sigma}^0 \to \Omega$ *is compatible with the action of the group* $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$.

Proof. Let $[\prod U_\ell(N)x_\ell] \coloneqq \gamma([\phi, \lambda, \alpha, \eta])$ and

$$\left[\prod U_\ell(N)x'_\ell\right] \coloneqq \gamma(g \cdot [\phi, \lambda, \alpha, \eta]) = \gamma([\phi, \lambda, g \circ \alpha, \eta]).$$

Pick some $\ell \neq p$ and set $H \coloneqq U_\ell(N)$; we claim that $Hx'_\ell = H(\alpha_0^{-1} \circ g \circ \alpha)x_\ell$. Recall that $x_\ell = k_\ell^{-1} \circ T_\ell \phi$, where $k_\ell : (T_\ell A, e_0) \to (T_\ell A, e)$ is some symplectic isomorphism extending $\alpha^{-1} \circ \alpha_0$. Therefore $k_\ell{}' \coloneqq k_\ell \circ (\alpha_0^{-1} \circ g \circ \alpha_0)$ is a symplectic isomorphism extending $\alpha^{-1} \circ g \circ \alpha_0$ and is thus precisely what we need in order to define $x_\ell{}' = (k'_\ell)^{-1} \circ T_\ell \phi$. By the definition of k'_ℓ we have

$$x'_\ell = (\alpha_0^{-1} \circ g^{-1} \circ \alpha) \circ k_\ell^{-1} \circ T_\ell \phi = (\alpha_0^{-1} \circ g^{-1} \circ \alpha) \circ x_\ell,$$

which is what we wanted to show. □

3.2.3. Raising the level

Suppose $N' = dN$ for some positive integer d. A level N' structure

$$\alpha' : (A[N'], e) \to ((\mathbb{Z}/N'\mathbb{Z})^{2g}, \mathrm{std})$$

on the principally polarized abelian variety (A, λ) induces a level N structure on (A, λ) in the following way. Multiplication by d on $A[N']$ gives a surjection $d : A[N'] \to A[N]$, and there is a natural surjection $\pi : (\mathbb{Z}/N'\mathbb{Z})^{2g} \to (\mathbb{Z}/N\mathbb{Z})^{2g}$ given by reduction mod N. We want to define a map $\alpha : A[N] \to (\mathbb{Z}/N\mathbb{Z})^{2g}$ that completes the following square:

$$\begin{array}{ccc} A[N'] & \xrightarrow[\sim]{\alpha'} & (\mathbb{Z}/N'\mathbb{Z})^{2g} \\ {\scriptstyle d}\big\downarrow & & \big\downarrow{\scriptstyle \pi} \\ A[N] & \dashrightarrow^{\alpha} & (\mathbb{Z}/N\mathbb{Z})^{2g} \end{array}$$

This is straightforward: let $P \in A[N]$ and take some preimage Q of it in $A[N']$. Set $\alpha(P) \coloneqq \pi(\alpha'(Q))$. This is easily seen to be well-defined and a bijection. Since both surjections d and π respect the symplectic structure, α is a symplectic isomorphism. We conclude that $[\phi, \lambda, \alpha', \eta] \mapsto [\phi, \lambda, \alpha, \eta]$ gives a map $\tilde{\Sigma}^0(N') \to \tilde{\Sigma}^0(N)$.

There is a similar map on the Ω's. We only need to consider primes $\ell | N'$. Here we have $U_\ell(N') \subset U_\ell(N)$ so we get maps $U_\ell(N') \backslash G_\ell \to U_\ell(N) \backslash G_\ell$, which can be put together to form $\Omega(N') \to \Omega(N)$.

We want to show that the bijection γ commutes with these maps. This is clear at primes $\ell \nmid N'$, so suppose ℓ is a prime divisor of N'; say $\ell^m || N$ and $\ell^n || N'$. Choose elements $[\phi, \lambda, \alpha', \eta] \in \tilde{\Sigma}^0(N')$, $[x'] \coloneqq \gamma([\phi, \lambda, \alpha', \eta])$ and $[x] \coloneqq \gamma([\phi, \lambda, \alpha, \eta])$. By definition, we have $x'_\ell = (k'_\ell)^{-1} \circ \phi$ where $k'_\ell : (T_\ell A, e_0) \to (T_\ell A, e)$ is a symplectic isomorphism restricting to

$$\begin{array}{ccc} (A[\ell^n], e_0) & \xrightarrow[\sim]{k'_\ell} & (A[\ell^n], e) \\ {\scriptstyle \alpha'_0}\big\downarrow{\scriptstyle \sim} & & {\scriptstyle \alpha'}\big\downarrow{\scriptstyle \sim} \\ ((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \mathrm{std}) & = & ((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \mathrm{std}). \end{array}$$

This defines the local component $U_\ell(N')x'_\ell$. We can restrict k'_ℓ even further to the ℓ^m-torsion, and then by the definition of α we have

$$\begin{array}{ccc} (A[\ell^m], e_0) & \xrightarrow[\sim]{k'_\ell} & (A[\ell^m], e) \\ {\scriptstyle \alpha'_0}\downarrow{\scriptstyle \sim} & & {\scriptstyle \alpha}\downarrow{\scriptstyle \sim} \\ ((\mathbb{Z}/\ell^m\mathbb{Z})^{2g}, \mathrm{std}) & = & ((\mathbb{Z}/\ell^m\mathbb{Z})^{2g}, \mathrm{std}). \end{array}$$

But this means that $k_\ell{}'$ plays the role of the k_ℓ in the definition of x_ℓ, so $U_\ell(N)x'_\ell = U_\ell(N)x_\ell$. This is precisely what the map $\Omega(N') \to \Omega(N)$ looks like at ℓ, so we are done.

4. Restriction to the superspecial locus

Let V be an $\bar{\mathbb{F}}_p$-vector space and let $\rho : \mathrm{GU}_g(\mathbb{F}_{p^2}) \to \mathrm{GL}(V)$ be a representation. A *superspecial modular form* of weight ρ and level N is a function $f : \Sigma \to V$ satisfying

$$f([A, \lambda, \alpha, M\eta]) = \rho(M)^{-1} f([A, \lambda, \alpha, \eta]), \quad \text{for all } M \in \mathrm{GU}_g(\mathbb{F}_{p^2}).$$

The space of all such forms will be denoted S_ρ. If τ is a subrepresentation of ρ, then $S_\tau \subset S_\rho$. If ρ and τ are representations, then $S_{\rho\otimes\tau} = S_\rho \otimes S_\tau$.

Let $\mathscr{I}$ denote the ideal sheaf of $i : \Sigma \hookrightarrow X$, i.e. the kernel in:

$$0 \to \mathscr{I} \to \mathscr{O}_X \to i_*\mathscr{O}_\Sigma \to 0.$$

The sheaf $\mathscr{I}$ is coherent [10, Proposition II.5.9]. Given one of our sheaves $\mathbb{E}_\rho$, we obtain after tensoring and taking cohomology

$$0 \to \mathrm{H}^0(X, \mathscr{I} \otimes \mathbb{E}_\rho) \to \mathrm{H}^0(X, \mathbb{E}_\rho) \to \mathrm{H}^0(X, i_*\mathscr{O}_\Sigma \otimes \mathbb{E}_\rho) = \mathrm{H}^0(\Sigma, i^*\mathbb{E}_\rho).$$

We rewrite the part that interests us in a more familiar notation:

$$0 \to \mathrm{H}^0(X, \mathscr{I} \otimes \mathbb{E}_\rho) \to M_\rho(N) \xrightarrow{r} S_{\mathrm{Res}\,\rho},$$

where Res restricts representations on GL_g to the finite subgroup $\mathrm{GU}_g(\mathbb{F}_{p^2})$.

Let $\omega := \Lambda^g\mathbb{E} = \mathbb{E}_{\det}$; it is an ample invertible sheaf [4, Theorem V.2.5].

Proposition 24. *For $n \gg 0$, r is a surjective map $M_{\rho\otimes\det^n}(N) \to S_{\mathrm{Res}(\rho\otimes\det^n)}$.*

Proof. Let k be such that ω^k is very ample. This defines an open immersion $j : X \hookrightarrow \mathbb{P}^N$, such that $j_*\mathscr{O}(1) = \omega^k$. By Hartshorne [10, Exercise II.5.15] there exists a locally free sheaf $\mathbb{E}'_\rho$ on $\mathbb{P}^N$ such that $\mathbb{E}'_\rho|_{j(X)} = \mathbb{E}_\rho$. Let $f = j \circ i$, then we have an exact

sequence of sheaves on $\mathbb{P}^N$:

$$0 \to \mathscr{I}_{\Sigma \subset \mathbb{P}^N} \otimes \mathbb{E}'_\rho \otimes \mathscr{O}(1)^m \to \mathbb{E}'_\rho \otimes \mathscr{O}(1)^m \to f_* \mathscr{O}_\Sigma \otimes \mathbb{E}'_\rho \otimes \mathscr{O}(1)^m \to 0.$$

By Hartshorne [10, Theorem III.5.2], we know that for $m \gg 0$ the map

$$\mathrm{H}^0(\mathbb{P}^N, \mathbb{E}'_\rho \otimes \mathscr{O}(1)^m) \to \mathrm{H}^0(\mathbb{P}^N, f_* \mathscr{O}_\Sigma \otimes \mathbb{E}'_\rho \otimes \mathscr{O}(1)^m)$$

is surjective. We get a commutative diagram

$$\begin{array}{ccccc}
\mathrm{H}^0\left(\mathbb{P}^N, \mathbb{E}'_\rho \otimes \mathscr{O}(m)\right) & \twoheadrightarrow & \mathrm{H}^0\left(\mathbb{P}^N, f_* \mathscr{O}_\Sigma \otimes \mathbb{E}'_\rho \otimes \mathscr{O}(m)\right) & = & \mathrm{H}^0\left(\Sigma, (\mathbb{E}'_\rho \otimes \mathscr{O}(m))|_\Sigma\right) \\
\downarrow \text{restriction to } X & & \downarrow \text{restriction to } X & & \downarrow \\
\mathrm{H}^0\left(X, \mathbb{E}_\rho \otimes \omega^{km}\right) & \longrightarrow & \mathrm{H}^0\left(X, i_* \mathscr{O}_\Sigma \otimes \mathbb{E}_\rho \otimes \omega^{km}\right) & = & \mathrm{H}^0\left(\Sigma, (\mathbb{E}_\rho \otimes \omega^{km})|_\Sigma\right).
\end{array}$$

The rightmost vertical map is an isomorphism, hence the middle vertical map is also an isomorphism and therefore

$$\mathrm{H}^0(X, \mathbb{E}_\rho \otimes \omega^{km}) \to \mathrm{H}^0(X, i_* \mathscr{O}_\Sigma \otimes \mathbb{E}_\rho \otimes \omega^{km})$$

is a surjection. We have proved the proposition for large enough n which are congruent to 0 modulo k. In order to do the same for all large enough n congruent to a modulo k (for $0 < a < k$), we use the above argument replacing $\mathbb{E}_\rho$ by $\mathbb{E}_\rho \otimes \omega^a$. Since there are only finitely many such a, the proposition is proved. □

4.1. Lifting weights

If H is a subgroup of a group G, we say that a representation ρ of H *lifts* to G if there exists a representation $\bar{\rho}$ of G such that $\rho = \mathrm{Res}\, \bar{\rho}$. It is clear that if ρ lifts to $\bar{\rho}$ and τ lifts to $\bar{\tau}$, then $\rho \oplus \tau$ lifts to $\bar{\rho} \oplus \bar{\tau}$.

Let q be some power of p. The following is a direct consequence of Steinberg [24, Theorems 6.1 and 7.4]:

Proposition 25. *Every irreducible representation of* $\mathrm{SL}_g(\mathbb{F}_q)$ *lifts to a unique irreducible rational representation of* $\mathrm{SL}_g(\bar{\mathbb{F}}_p)$.

We now extend this to

Proposition 26. *Every irreducible representation of* $\mathrm{GL}_g(\mathbb{F}_q)$ *lifts to an irreducible rational representation of* $\mathrm{GL}_g(\bar{\mathbb{F}}_p)$.

Proof. It suffices to prove that every irreducible representation lifts to a completely reducible one. Let $\rho : \mathrm{GL}_g(\mathbb{F}_q) \to \mathrm{GL}(V)$ be irreducible.

Via the canonical embeddings $\mathrm{SL}_g(\mathbb{F}_q) \subset \mathrm{GL}_g(\mathbb{F}_q)$ and $\mathbb{G}_m(\mathbb{F}_q) \subset \mathrm{GL}_g(\mathbb{F}_q)$, ρ induces representations $\rho_s : \mathrm{SL}_g(\mathbb{F}_q) \to \mathrm{GL}(V)$ and $\rho_m : \mathbb{G}_m(\mathbb{F}_q) \to \mathrm{GL}(V)$, such that

$\operatorname{Im}\rho_s$ commutes with $\operatorname{Im}\rho_m$. Since $\mathrm{GL}_g(\mathbb{F}_q) = \mathrm{SL}_g(\mathbb{F}_q)\cdot\mathbb{G}_m(\mathbb{F}_q)$ and $\mathrm{SL}_g(\mathbb{F}_q)\cap\mathbb{G}_m(\mathbb{F}_q) = \boldsymbol{\mu}_g(\mathbb{F}_q)$, we also have that $\rho_s(\zeta) = \rho_m(\zeta)$ for all $\zeta\in\boldsymbol{\mu}_g(\mathbb{F}_q)$.

Any representation of $\mathbb{G}_m(\mathbb{F}_q)$ is of the form

$$\mathbb{G}_m(\mathbb{F}_q)\to\mathrm{GL}(V)$$

$$\lambda\mapsto\begin{pmatrix}\lambda^{a_1} & & \\ & \ddots & \\ & & \lambda^{a_n}\end{pmatrix}$$

with $a_i\in\mathbb{Z}/(q-1)\mathbb{Z}$. We claim that in our case $\mathbb{G}_m(\mathbb{F}_q)$ acts by scalars on V. Suppose this is false, then there exists $\lambda\in\mathbb{G}_m(\mathbb{F}_q)$ such that at least two of the diagonal entries of $\rho_m(\lambda)$ are distinct. By changing the basis of V we can assume $\rho_m(\lambda)$ is in Jordan canonical form. Let $A\in\mathrm{SL}_g(\mathbb{F}_{p^2})$, then the fact that $\rho_s(A)$ commutes with $\rho_m(\lambda)$ forces A to have the same shape as $\rho_m(\lambda)$ (i.e. it is block-diagonal with blocks of the same dimensions as $\rho_m(\lambda)$). Since this holds for all $A\in\mathrm{SL}_g(\mathbb{F}_q)$, we conclude that as an $\mathrm{SL}_g(\mathbb{F}_q)$-module, V has a direct sum decomposition $V = V_1\oplus\cdots\oplus V_j$ corresponding to the shape of $\rho_m(\lambda)$ (in the chosen basis for V, V_1 is the span of the first k vectors, where k is the size of the first Jordan block of $\rho_m(\lambda)$, etc.). But this means that V_1 is a proper subspace of V which invariant under both $\mathrm{SL}_g(\mathbb{F}_q)$ and $\mathbb{G}_m(\mathbb{F}_q)$, contradicting the hypothesis that V is an irreducible representation of $\mathrm{GL}_g(\mathbb{F}_q)$. So $\mathbb{G}_m(\mathbb{F}_q)$ acts by scalars on V, say $\rho_m(\lambda)v = \lambda^a v$ for some $a\in\mathbb{Z}/(q-1)\mathbb{Z}$.

From this it is clear that ρ_m is completely reducible and that any choice of $\bar{a}\in\mathbb{Z}$ with $\bar{a}\equiv a\pmod{q-1}$ yields a completely reducible lift $\bar{\rho}_m : \mathbb{G}_m(\bar{\mathbb{F}}_p)\to\mathrm{GL}(V)$ given simply by $\lambda\mapsto\lambda^{\bar{a}}$. Note that $\bar{\rho}_m$ is a rational representation. Later on we will need to choose a lift of a to $\bar{a}\in\mathbb{Z}$ that suits us better.

It is also pretty clear that ρ_s is irreducible: if W is an irreducible $\mathrm{SL}_g(\mathbb{F}_q)$-submodule, then W is also $\mathbb{G}_m(\mathbb{F}_q)$-invariant so it is $\mathrm{GL}_g(\mathbb{F}_q)$-invariant, hence either $W = 0$ or $W = V$.

By Proposition 25, ρ_s lifts to an irreducible rational $\bar{\rho}_s : \mathrm{SL}_g(\bar{\mathbb{F}}_p)\to\mathrm{GL}(V)$. Since $\mathbb{G}_m$ acts by scalars, $\operatorname{Im}\bar{\rho}_m$ commutes with $\operatorname{Im}\bar{\rho}_s$. We claim that the maps $\bar{\rho}_m$ and $\bar{\rho}_s$ agree on $\boldsymbol{\mu}_g(\bar{\mathbb{F}}_p) = \mathrm{SL}_g(\bar{\mathbb{F}}_p)\cap\mathbb{G}_m(\bar{\mathbb{F}}_p)$. Assuming this is true, we can construct a rational representation

$$\bar{\rho} : \mathrm{GL}_g(\bar{\mathbb{F}}_p)\to\mathrm{GL}(V)$$

$$M\mapsto\bar{\rho}_m(\det M)\cdot\bar{\rho}_s((\det M)^{-1}M).$$

Since the restriction of $\bar{\rho}$ to $\mathrm{SL}_g(\bar{\mathbb{F}}_p)$ is $\bar{\rho}_s$ and in particular irreducible, we conclude that $\bar{\rho}$ is irreducible.

It remains to prove that $\bar{\rho}_m$ and $\bar{\rho}_s$ agree on the gth roots of unity. It suffices to do this for a primitive gth root ζ. Write $g = p^s g'$ with $(p, g') = 1$. We have $(\zeta^{g'})^{p^s} = \zeta^g = 1$, so $\zeta^{g'} = 1$ since the only p^sth root of unity in characteristic p is 1. Therefore ζ is a g'th root of unity, so without loss of generality we may assume that $(p, g) = 1$.

Consider the linear transformation $\bar{\rho}_s(\zeta)$. It is diagonalizable if and only if its minimal polynomial has distinct roots. But the transformation satisfies $X^g - 1 = 0$, which has distinct roots, and hence the minimal polynomial will also have distinct roots. So we can choose a basis for V such that $\bar{\rho}_s(\zeta)$ is diagonal. If it has at least two distinct diagonal entries, we can apply the same argument as before to conclude that since it commutes with all of $\bar{\rho}_s(\mathrm{SL}_g(\bar{\mathbb{F}}_p))$ the representation $\bar{\rho}_s$ is reducible, which is a contradiction. So $\bar{\rho}_s(\zeta) = \zeta^b$, for some $b \in \mathbb{Z}/g\mathbb{Z}$. We want to show that $\bar{\rho}_m(\zeta) = \bar{\rho}_s(\zeta)$, i.e. that we can choose $\bar{a} \in \mathbb{Z}$ such that $\bar{a} \equiv b \pmod{g}$. Let $d \coloneqq (g, q-1)$ and write $g = dm$, $q - 1 = dn$. We have $(\zeta^m)^d = \zeta^g = 1$ so $(\zeta^m)^{q-1} = (\zeta^{md})^n = 1$ so $\zeta^m \in \mathbb{F}_q$. Therefore $\zeta^m \in \boldsymbol{\mu}_g(\mathbb{F}_q)$ and hence $(\zeta^b)^m = \bar{\rho}_s(\zeta^m) = \bar{\rho}_m(\zeta^m) = (\zeta^m)^{\bar{a}}$. This implies that $m\bar{a} \equiv mb \pmod{g}$, i.e. $\bar{a} \equiv b \pmod{d}$. Since $d = (g, q-1)$ and $d|(\bar{a} - b)$ there exist integers u, v such that $\bar{a} - b = ug + v(q-1)$ and therefore

$$(\bar{a} - v(q-1)) \equiv b \pmod{g},$$

which is what we wanted. □

Note that in contrast with Proposition 25 the lift of ρ to $\mathrm{GL}_g(\bar{\mathbb{F}}_p)$ is not unique. Fix some lift $\bar{\rho}$, then any lift can be written in the form $\det^m \otimes \bar{\rho}$, where m is a common multiple of g and $q - 1$.

Corollary 27. *Given an irreducible representation $\tau : \mathrm{GU}_g(\mathbb{F}_{p^2}) \to \mathrm{GL}(W)$, there exists an irreducible rational representation $\bar{\rho} : \mathrm{GL}_g(\bar{\mathbb{F}}_p) \to \mathrm{GL}(V)$ such that $\tau \subset \mathrm{Res}\,\bar{\rho}$.*

Proof. Consider the induced representation from $\mathrm{GU}_g(\mathbb{F}_{p^2})$ to $\mathrm{GL}_g(\mathbb{F}_{p^2})$. This has an irreducible subrepresentation $\rho : \mathrm{GL}_g(\mathbb{F}_{p^2}) \to \mathrm{GL}(V)$ with the property that $\tau \subset \mathrm{Res}\,\rho$. The result now follows from the previous proposition. □

4.2. Proof of the main result

We have come to the main result of the paper. Recall the notation $U_\ell(N) \coloneqq \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)(N)$ for $\ell \neq p$, $U_p \coloneqq \ker(\mathrm{GU}_g(\mathcal{O}_p) \to \mathrm{GU}_g(\mathbb{F}_{p^2}))$ and

$$U \coloneqq U_p \times \prod_{\ell \neq p} U_\ell(N).$$

Theorem 28. *Fix a dimension $g > 1$, a level $N \geqslant 3$ and a prime p not dividing N. The systems of Hecke eigenvalues coming from Siegel modular forms $(\mathrm{mod}\, p)$ of dimension g, level N and any weight ρ, are the same as the systems of Hecke eigenvalues coming from algebraic modular forms $(\mathrm{mod}\, p)$ of level U and any weight ρ_Σ on the group $\mathrm{GU}_g(B)$.*

Proof. Let f be a Siegel modular form of weight $\rho : \mathrm{GL}_g \to \mathrm{GL}_m$ which is a Hecke eigenform. If $r(f) = 0$, then $f \in \mathrm{H}^0(X, \mathscr{I} \otimes \mathbb{E}_\rho)$. The quotient map of $\mathscr{O}_X$-modules $\mathscr{I} \to \mathscr{I}/\mathscr{I}^2$ induces (after tensoring with $\mathbb{E}_\rho$ and taking global sections) a map

$$\mathrm{H}^0(X, \mathscr{I} \otimes \mathbb{E}_\rho) \to \mathrm{H}^0(X, \mathscr{I}/\mathscr{I}^2 \otimes \mathbb{E}_\rho), \text{ which we denote by } f \mapsto \bar{f}.$$

Consider $\bar{f} \in \mathrm{H}^0(X, \mathscr{I}/\mathscr{I}^2 \otimes \mathbb{E}_\rho)$. We have an exact sequence

$$0 \to \mathscr{I} \otimes \mathscr{I}/\mathscr{I}^2 \otimes \mathbb{E}_\rho \to \mathscr{I}/\mathscr{I}^2 \otimes \mathbb{E}_\rho \to i_* \mathscr{O}_\Sigma \otimes \mathscr{I}/\mathscr{I}^2 \otimes \mathbb{E}_\rho \to 0$$

which gives us a long exact sequence that starts with

$$0 \to \mathrm{H}^0(X, \mathscr{I}^2/\mathscr{I}^3 \otimes \mathbb{E}_\rho) \to \mathrm{H}^0(X, \mathscr{I}/\mathscr{I}^2 \otimes \mathbb{E}_\rho) \xrightarrow{r_1} \mathrm{H}^0(\Sigma, i^*(\mathscr{I}/\mathscr{I}^2 \otimes \mathbb{E}_\rho)).$$

If $r_1(\bar{f}) = 0$ then $\bar{f} \in \mathrm{H}^0(X, \mathscr{I}^2/\mathscr{I}^3 \otimes \mathbb{E}_\rho)$ and we can similarly consider $r_2(\bar{f})$, $r_3(\bar{f})$, etc. There exists some n such that $r_n(\bar{f}) \neq 0$. Let $f_S := r_n(\bar{f}) \in \mathrm{H}^0(\Sigma, i^*(\mathscr{I}^n/\mathscr{I}^{n+1} \otimes \mathbb{E}_\rho))$. Note that $\mathscr{I}^n/\mathscr{I}^{n+1} = \mathrm{Sym}^n(\mathscr{I}/\mathscr{I}^2)$ and that $i^*(\mathscr{I}/\mathscr{I}^2) = i^*(\Omega^1_X)$. Recall from Section 2.2.3 the Kodaira–Spencer isomorphism $\Omega^1_X \cong \mathbb{E}_{\mathrm{Sym}^2 \mathrm{std}}$. We conclude that $f_S \in S_{\mathrm{Res}((\mathrm{Sym}^{2n} \mathrm{std}) \otimes \rho)}$. So our process associates to a Siegel modular form f of weight ρ a superspecial modular form f_S of weight $\mathrm{Res}((\mathrm{Sym}^{2n}\mathrm{std}) \otimes \rho)$ for some integer n depending on f. Moreover, since the restrictions r_i and the Kodaira–Spencer isomorphism are Hecke maps, we conclude that f_S is a Hecke eigenform with the same eigenvalues as f.

Now let f_S be a superspecial Siegel modular form of weight $\rho_S : \mathrm{GU}_g(\mathbb{F}_{p^2}) \to \mathrm{GL}_m(\bar{\mathbb{F}}_p)$. By applying Corollary 27 we get a rational representation $\bar{\rho} : \mathrm{GL}_g \to \mathrm{GL}_m$ such that $\rho_S \subset \mathrm{Res}\, \bar{\rho}$. By functoriality we get $S_{\rho_S} \subset S_{\mathrm{Res}\, \bar{\rho}}$. We know that the map $r : M_{\bar{\rho} \otimes \det^n}(N) \to S_{\mathrm{Res}(\bar{\rho} \otimes \det^n)}$ is surjective for $n \gg 0$, and therefore there exists an integer k such that

$$r : M_{\bar{\rho} \otimes \det^{k(p^2-1)}}(N) \to S_{\mathrm{Res}(\bar{\rho} \otimes \det^{k(p^2-1)})} = S_{\mathrm{Res}\, \bar{\rho}} \supset S_{\rho_S}$$

is surjective. Since this map is also Hecke-invariant, we conclude from Ash and Stevens [2, Proposition 1.2.2] that any system of Hecke eigenvalues that occurs in S_{ρ_S} also occurs in $M_{\bar{\rho} \otimes \det^{k(p^2-1)}}$.

So far we showed that the systems of Hecke eigenvalues given by Siegel modular forms (mod p) of all weights are the same as the systems of Hecke eigenvalues given by superspecial modular forms S_{ρ_S} of all weights. By Theorem 21 we know that S_{ρ_S} is isomorphic as a Hecke module to the space of algebraic modular forms (mod p) of weight ρ_S, and we are done. □

4.3. Agreement with the definition of Gross

In this section we will write $G := \mathrm{GU}_g(\mathbb{F}_{p^2})$.

Recall from Section 2.1.3 that Gross defines algebraic modular forms $(\mathrm{mod}\, p)$ as follows: let $\rho : G \to \mathrm{GL}(V)$ be an irreducible representation where V is a finite-dimensional vector space *over* $\mathbb{F}_p$, then set

$$M(\rho) := \{f : \Omega \to V \mid f(\lambda x) = \rho(\lambda)^{-1} f(x) \text{ for all } \lambda \in G\}.$$

For comparison, our spaces of modular forms on Ω are defined as

$$M(\tau) := \{f : \Omega \to W \mid f(\lambda x) = \rho(\lambda)^{-1} f(x) \text{ for all } \lambda \in G\},$$

where $\tau : G \to \mathrm{GL}(W)$ is an irreducible representation and W is a finite-dimensional vector space *over* $\bar{\mathbb{F}}_p$.

The purpose of this section is to show that the spaces $M(\rho)$ and $M(\tau)$ for varying ρ and τ give the same systems of Hecke eigenvalues.

First suppose that $(a_T : T)$ is a system of Hecke eigenvalues coming from $M(\rho)$. Then there exists $f \in M(\rho) \otimes \bar{\mathbb{F}}_p$ such that $T(f) = a_T f$ for all T. Let $\rho \otimes \bar{\mathbb{F}}_p$ denote the composition $G \xrightarrow{\rho} \mathrm{GL}(V) \hookrightarrow \mathrm{GL}(V \otimes \bar{\mathbb{F}}_p)$. The map

$$M(\rho) \otimes \bar{\mathbb{F}}_p \to M(\rho \otimes \bar{\mathbb{F}}_p)$$

$$m \otimes \alpha \mapsto \alpha m$$

is an isomorphism compatible with the action of the Hecke operators, so the image of f in $M(\rho \otimes \bar{\mathbb{F}}_p)$ is an eigenform with the same eigenvalues as f. Therefore the system (a_T) also comes from $M(\rho \otimes \bar{\mathbb{F}}_p)$.

Conversely, suppose that $(a_T : T)$ is a system of Hecke eigenvalues coming from $M(\tau)$ for some $\tau : G \to \mathrm{GL}(W)$, W a finite-dimensional $\bar{\mathbb{F}}_p$-vector space. Then there exists $f \in M(\tau)$ such that $T(f) = a_T f$ for all T. Since G is a finite group there exist $q = p^a$, a finite-dimensional $\mathbb{F}_q$-vector space W' and a representation $\tau' : G \to \mathrm{GL}(W')$ such that $\tau' \otimes \bar{\mathbb{F}}_p = \tau$. Similarly, Ω is a finite set and f is a map $\Omega \to W$ so by enlarging q if necessary, there exists $f' \in M(\tau')$ such that f is the image of $f' \otimes 1$ under the isomorphism $M(\tau') \otimes \bar{\mathbb{F}}_p \cong M(\tau)$. Clearly $T(f') = a_T f'$ for all T; in particular $a_T \in \mathbb{F}_q$ for all T.

We now use the following

Proposition 29. *Suppose L/K is a finite Galois extension with Galois group G and V is a finite-dimensional vector space over L. Let $\mathscr{T}$ be a collection of commuting diagonalizable linear operators on V and let V_K be the space V viewed as a vector space over K. If a $\mathscr{T}$-eigenvector v has system of eigenvalues $\{a_T : T \in \mathscr{T}\}$, then for every $\sigma \in G$ there exists an eigenvector $v_\sigma \in V_K$ with system of eigenvalues $\{\sigma(a_T) : T \in \mathscr{T}\}$.*

Let us first see how this concludes our argument. We apply the proposition to the finite Galois extension $\mathbb{F}_q/\mathbb{F}_p$, the vector space $M(\tau')$, the Hecke operators T, the eigenvector f' and the identity Galois element $\sigma = 1$. We conclude that if we consider $M(\tau')$ as a vector space over $\mathbb{F}_p$, there exists an eigenvector f'' with the same system of eigenvalues as f'. This is precisely what we needed to show.

Proof of Proposition 29. The isomorphism φ of the next lemma induces an isomorphism of L-vector spaces

$$\begin{aligned} \varphi : L \otimes_K V &\to \bigoplus_{\sigma \in G} Ve_\sigma \\ \alpha \otimes w &\mapsto \sum_{\sigma \in G} \sigma(\alpha) w e_\sigma. \end{aligned}$$

Let $v_\sigma \coloneqq \varphi^{-1}(ve_{\sigma^{-1}})$. We have

$$Tv_\sigma = \varphi^{-1}((Tv)e_{\sigma^{-1}}) = \varphi^{-1}((a_T v)e_{\sigma^{-1}}) = \sigma(a_T)\varphi^{-1}(ve_{\sigma^{-1}}) = \sigma(a_T)v_\sigma,$$

so v_σ is an eigenvector of T with eigenvalue $\sigma(a_T)$, and this holds for all $T \in \mathscr{T}$. □

Lemma 30. *Suppose L/K is a finite Galois extension with Galois group G. The map*

$$\varphi : L \otimes_K L \to \bigoplus_{\sigma \in G} Le_\sigma$$

defined by $\alpha \otimes \beta \mapsto \sum_{\sigma \in G} \sigma(\alpha)\beta e_\sigma$ is an isomorphism of L-algebras.

Proof. It is pretty clear that φ is an L-algebra homomorphism. Since the dimensions of the domain and of the range are equal (and equal to $[L : K]$), it suffices to prove that φ is injective.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of L as a K-vector space. Then $\{\alpha_i \otimes \alpha_j : 1 \leqslant i, j \leqslant n\}$ is a basis of $L \otimes_K L$ as a K-vector space. Suppose $\varphi(\sum c_{ij}\alpha_i \otimes \alpha_j) = 0$. If we write $G = \{\sigma_1, \ldots, \sigma_n\}$, then we have

$$\sum_{i,j} c_{ij}\sigma_k(\alpha_i)\alpha_j = 0 \quad \text{for all } k. \tag{7}$$

Let A be the $n \times n$ matrix whose (i,j)th entry is $\sigma_i(\alpha_j)$, and let c be the column vector whose ith entry is $\sum_j c_{ij}\alpha_j$. Then system (7) can be written as $Ac = 0$. But it is an easy consequence of independence of characters [13, Corollary VI.5.4] that $A \in \mathrm{GL}_n(L)$, therefore we must have $c = 0$, i.e.

$$\sum_j c_{ij}\alpha_j = 0 \quad \text{for all } i.$$

Since the α_j are linearly independent we conclude that $c_{ij} = 0$ for all i and j, hence φ is injective. □

Acknowledgments

The results of this paper were obtained while the author was a doctoral student at the Massachusetts Institute of Technology, and partially funded by NSERC, FCAR and MIT. He thanks B. Gross for suggesting the problem, A.J. de Jong for his invaluable supervision, and R. Beheshti, M. Lieblich, F. Oort, D. Vogan for patiently and repeatedly answering his questions.

References

[1] A.N. Andrianov, V.G. Zhuravlëv, Modular Forms and Hecke Operators, American Mathematical Society, Providence, RI, 1995 (translated from the 1990 Russian original by Neal Koblitz).
[2] A. Ash, G. Stevens, Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues, J. Reine Angew. Math. 365 (1986) 192–220.
[3] C.-L. Chai, Siegel moduli schemes and their compactifications over $\mathbb{C}$, in: G. Cornell, J.H. Silverman (Eds.), Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 231–251.
[4] G. Faltings, C.-L. Chai, Degeneration of Abelian Varieties, Springer, Berlin, 1990 with an appendix by David Mumford.
[5] J.-M. Fontaine, Groupes p-divisibles sur les corps locaux, Société Mathématique de France, Paris, 1997, Astérisque, No. 47–48.
[6] A. Ghitza, Siegel modular forms (mod p) and algebraic modular forms, Ph.D. Thesis, MIT, 2003, arXiv:math.NT/0306224.
[7] B.H. Gross, Modular Galois representations, unpublished, January 1996.
[8] B.H. Gross, Modular forms (mod p) and Galois representations, Internat. Math. Res. Notices (16) (1998) 865–875.
[9] B.H. Gross, Algebraic modular forms, Israel J. Math. 113 (1999) 61–93.
[10] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics, Vol. 52, Springer, New York, 1977.
[11] N. Jochnowitz, Congruences between systems of eigenvalues of modular forms, Trans. Amer. Math. Soc. 270 (1) (1982a) 269–285.
[12] N. Jochnowitz, A study of the local components of the Hecke algebra mod ℓ, Trans. Amer. Math. Soc. 270 (1) (1982b) 253–267.
[13] S. Lang, Algebra, 3rd Edition, Addison-Wesley, Reading, MA, 1993.
[14] K.-Z. Li, F. Oort, Moduli of Supersingular Abelian varieties, Lecture Notes in Mathematics, Vol. 1680, Springer, Berlin, 1998.
[15] J.S. Milne, Abelian varieties, in: G. Cornell, J.H. Silverman (Eds.), Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.
[16] L. Moret-Bailly, Familles de courbes et de variétés abéliennes sur $\mathbb{P}^1$, I et II, in: Séminaire sur les Pinceaux de Courbes de Genre au Moins Deux, Société Mathématique de France, Paris, 1981, pp. 109–140.
[17] P. Norman, An algorithm for computing local moduli of abelian varieties, Ann. Math. (2) 101 (1975) 499–509.
[18] T. Oda, The first de Rham cohomology group and Dieudonné modules, Ann. Sci. École Norm. Sup. (4) 2 (1969) 63–135.
[19] F. Oort, Commutative Group Schemes, Lecture Notes in Mathematics, Vol. 15, Springer, Berlin, 1966.
[20] F. Oort, Which abelian surfaces are products of elliptic curves?, Math. Ann. 214 (1975) 35–47.
[21] J.-P. Serre, Two letters on quaternions and modular forms (mod p), Israel J. Math. 95 (1996) 281–299 with introduction, appendix and references by R. Livné.

[22] G. Shimura, Arithmetic of alternating forms and quaternion hermitian forms, J. Math. Soc. Japan 15 (1963) 33–65.
[23] T. Shioda, Supersingular $K3$ surfaces, in: Algebraic Geometry (Proceedings of the Summer Meeting, University of Copenhagen, Copenhagen, 1978), Springer, Berlin, 1979, pp. 564–591.
[24] R. Steinberg, Representations of algebraic groups, Nagoya Math. J. 22 (1963) 33–56.
[25] M.-F. Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Mathematics, Vol. 800, Springer, Berlin, 1980.