SIEGEL MODULAR FORMS (MOD $p$) AND ALGEBRAIC MODULAR FORMS

ALEXANDRU GHITZA

Abstract. In his letter [Ser96], J.-P. 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 $\Lambda_B^*/B^* \to \overline{\mathbb{F}}_p$, where $B$ is the endomorphism algebra of a supersingular elliptic curve. After giving a detailed exposition of Serre’s result, we prove 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 $GU_g(B)$, as defined in [Gro99] and [Gro98]. The correspondence is obtained by restricting to the superspecial locus of the moduli space of abelian varieties.

Contents

1. Introduction
2. Elliptic modular forms
   2.1. The geometric theory of modular forms (mod $p$)
   2.2. Main result and reductions
   2.3. Preliminary results
   2.4. Construction of the bijection
   2.5. Compatibilities
3. Siegel modular forms
   3.1. The geometric theory of Siegel modular forms
   3.2. Superspecial abelian varieties
   3.3. Construction of the bijection
   3.4. Compatibilities
   3.5. Restriction to the superspecial locus
4. References

1. INTRODUCTION

The study of arithmetic properties of modular forms goes back to Ramanujan, who observed that the coefficients $\tau(n)$ of the modular form

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n)q^n$$

satisfy interesting congruence relations modulo various primes. After these congruence relations had been proved by classical methods, Swinnerton-Dyer used results of Serre and Deligne in order to conduct a systematic study of the problem. His main tool is the description of the algebra of modular forms mod $p$ (see [SD73], [SD76]).
Consider a modular form $f$ of weight $k$ and level $N$

$$f = \sum_{n=0}^{\infty} a_n q^n$$

whose coefficients $a_n$ are rational and $p$-integral (that is, $p$ does not divide the denominator of $a_n$). Write $\tilde{f}$ for the reduction of $f$ modulo $p$, i.e. the element of $\mathbb{F}_p[[q]]$ obtained by reducing each coefficient of $f$ modulo $p$. We denote the set of all such series $M_k(N)$. Set $M(N) = \sum_{k \in \mathbb{Z}} M_k(N)$, known as the algebra of level $N$ modular forms (mod $p$). For $\ell$ prime to $pN$, one defines the Hecke operator $T_\ell$ by

$$T_\ell f = \sum_{n=0}^{\infty} a_{\ell n} q^n + \ell^{k-1} \sum_{n=0}^{\infty} a_n q^{\ell n}.$$

An eigenform is an element $f$ of $M_k(N)$ which is a simultaneous eigenvector for all $T_\ell$, $\ell \nmid pN$. Given an eigenform, one obtains a system of eigenvalues $(b_\ell)_{\ell \nmid pN}$ defined simply by $T_\ell f = b_\ell f$.

A considerable amount of effort has gone into the study of this Hecke action on modular forms. One of the approaches, due to Serre and inspired by the philosophy of the Langlands program, is to interpret these modular forms in terms of ad`eles on quaternion algebras. More precisely, let $B$ be the quaternion algebra ramified at $p$ and $\infty$ and let $\mathbb{A}_B^\times$ denote the group of ad`eles on $B$. Serre proved the following

**Theorem 1.1** ([Ser96]). The systems of eigenvalues $(b_\ell)_{\ell \nmid pN}$ given by the Hecke operators on modular forms (mod $p$) of any level $N$ are the same as those obtained from locally constant functions $f : \mathbb{A}_B^\times / B^\times \to \mathbb{F}_p$.

Given an eigenform with eigenvalues $(b_\ell)$, Deligne shows in [Del71] (see also [Gro90]) how to construct a mod $p$ Galois representation of degree 2

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F}_p)$$

such that $\rho(\text{Frob}_\ell)$ has trace $b_\ell$ and determinant $\ell^{k-1}$. Serre shows therefore that the systems of traces of Frobenii for a modular representation are the same as the eigenvalues of locally constant functions $\mathbb{A}_B^\times / B^\times \to \mathbb{F}_p$. We remark that he was lead to this result by working on his famous conjectures, which basically say that any Galois representation of degree 2 that satisfies certain properties comes from a modular form in the way we mentioned (see [Ser87]).

Inspired by this work, Gross has introduced ([Gro99]) the notion of algebraic modular forms (mod $p$) on certain reductive algebraic groups $G$ over $\mathbb{Q}$. The hope is to establish a relation between these forms and higher-dimensional Galois representations

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \hat{G}(\mathbb{F}_p),$$

where $\hat{G}$ is the $L$-group of $G$ (see [Gro98] for a precise statement). Serre’s result gives one direction of this relation in the case $G = B^\times$, $\hat{G} = \text{GL}_2$, while the opposite direction is the object of the Serre conjectures.

The aim of this thesis is to generalize Serre’s work to the case $G = GU_g(B) = \text{the group of unitary similitudes of the quaternionic hermitian space } B^g$, for $g > 1$. We start by giving a detailed and explicit treatment of Serre’s theorem in § 2. After recalling some basic facts about modular forms, we reduce Theorem 1.1 to the existence of a Hecke-invariant bijection between a finite subset of the modular curve $X(N)$ and a finite double coset space. The reduction is based on restricting modular forms to the supersingular locus, and on the use of the Hasse invariant to prove that this restriction is compatible with the Hecke action. The construction of the bijection of finite sets is explicit but somewhat lengthy and takes the remainder of the section.
We attack the generalization to higher dimensions in §3. After recalling the definition of Siegel modular forms, we briefly discuss properties of superspecial abelian varieties and of the algebraic group $GU_g(B)$. The main result is the following.

**Theorem 1.2.** Fix a dimension $g > 1$, a level $N \geq 3$ and a prime $p$ not dividing $N$. The systems of Hecke eigenvalues coming from Siegel modular forms $(\text{mod } p)$ of dimension $g$, level $N$ and any weight $\rho$, are the same as the systems of Hecke eigenvalues coming from algebraic modular forms $(\text{mod } p)$ of level $N$ and any weight $\rho$ on the group $GU_g(B)$.

The proof consists of two main steps: first we show that the restriction to the locus of superspecial principally polarized abelian varieties preserves the systems of eigenvalues, and that systems of eigenvalues occurring on the superspecial locus can be lifted to the entire moduli space; we then construct a Hecke bijection between the superspecial locus and a double coset space built from $GU_g(B)$.

### 2. Elliptic modular forms

We give a detailed exposition of Serre’s letter to Tate (see [Ser96]) linking elliptic modular forms (mod $p$) to quaternion algebras.

#### 2.1. The geometric theory of modular forms (mod $p$)

We review some of the definitions and results from Chapter 1 of [Kat73]. The reader unfamiliar with the geometric definition of modular forms is encouraged to consult Katz’ article for details.

An elliptic curve over a scheme $S$ is a proper smooth morphism $\pi : E \to S$, whose geometric fibers are connected curves of genus one, together with a section $0 : S \to E$:

$$
\pi \quad \text{encapsulated by:} \quad \omega_{E/S} := \pi_* (\Omega^1_{E/S}).
$$

We define $\omega_{E/S} := \pi_* (\Omega^1_{E/S})$. This is an invertible sheaf on $S$; by Serre duality it is canonically dual to $R^1 \pi_*(O_E)$.

For each integer $N \geq 1$, $E[N] := \ker([N] : E \to E)$ is a finite flat commutative group scheme of rank $N^2$ over $S$. It is étale over $S$ if and only if $S$ is a scheme over $\mathbb{Z}[\frac{1}{N}]$. In this case, we define a level $N$ structure on $E$ to be an isomorphism

$$
\alpha : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2_S.
$$

If such an isomorphism exists and $S$ is connected, then the set of all level $N$ structures is principal homogeneous under $\text{Aut}((\mathbb{Z}/N\mathbb{Z})^2_S) = \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

For $N \geq 3$, the functor “isomorphism classes of elliptic curves with level $N$ structure” is representable by a scheme $Y(N)$ which is an affine smooth curve over $\mathbb{Z}[\frac{1}{N}]$, finite and flat of degree equal to $\#(\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\})$ over the affine $j$-line $\mathbb{Z}[\frac{1}{N},j]$, and étale over the open set of the affine $j$-line where $j$ and $j - 1728$ are invertible. The normalization of the projective $j$-line $P^1_{\mathbb{Z}[\frac{1}{N}]}$ in $Y(N)$ is a proper and smooth curve $X(N)$ over $\mathbb{Z}[\frac{1}{N}]$, the global sections of whose structure sheaf are $\mathbb{Z}[\frac{1}{N},\zeta_N]$. Let $(\mathcal{E}/Y(N),\alpha)$ be the universal elliptic curve with level $N$ structure. There is a unique invertible sheaf $\omega$ on $X(N)$ whose restriction to $Y(N)$ is $\omega_{\mathcal{E}/Y(N)}$ and whose sections over the completion $\mathbb{Z}[\frac{1}{N},\zeta_N][[[g]]]$ at each cusp are precisely the $\mathbb{Z}[\frac{1}{N},\zeta_N][[[g]]]$ multiples of the canonical differential of the Tate curve. The Kodaira-Spencer isomorphism

$$
(\omega_{\mathcal{E}/Y(N)})^2 \cong \Omega^1_{Y(N)/\mathbb{Z}[\frac{1}{N}]}
$$
extends to an isomorphism
\[ \omega^2 \cong \Omega^1_{X(N)/\mathbb{Z}[1/p]}(\log(X(N) - Y(N))). \]

A modular form \((mod \ p)\) of level \(N\) and weight \(k\) is a global section of \(\omega^k\) on \(X(N) \otimes \overline{\mathbb{F}}_p\) or equivalently a global section of the quasi-coherent sheaf \(\omega^k \otimes \overline{\mathbb{F}}_p\) on \(X(N)\).

An important fact in the mod \(p\) theory is the existence of a modular form \(A\) of level 1 and weight \(p - 1\), called the Hasse invariant. For its properties, see §IV.4 in [Har77], §2.0 and §2.1 in [Kat73].

2.2. Main result and reductions. Fix a prime \(p\) and an integer \(N \geq 3\) prime to \(p\). Set \(X := X(N) \otimes \overline{\mathbb{F}}_p\).

We work with Katz’ definition of modular forms \((mod \ p)\) of level \(N\) and weight \(k\):
\[ M_k(N) = H^0(X, \omega^k). \]

Multiplication by the Hasse invariant \(A\) gives a natural Hecke embedding
\[ M_{k-(p-1)}(N) \hookrightarrow M_k(N) \]
and we’re interested in the structure of the quotient \(W_k(N) = M_k(N)/M_{k-(p-1)}(N)\) as a module over the Hecke operators \(T_\ell\), \(\ell \not\mid pN\). On the level of sheaves, we define \(S_k\) by the following
\[ 0 \to \omega^{k-(p-1)} \times A \to \omega^k \to S_k \to 0. \]

The Hasse invariant \(A\) vanishes to order 1 when evaluated on the supersingular elliptic curves (and does not vanish anywhere else), so \(S_k\) is 0 over the ordinary locus and one-dimensional over the supersingular points.

We take global sections and get the exact sequence
\[ 0 \to W_k(N) \to S_k(N) \to H^1(X, \omega^{k-(p-1)}) \to H^1(X, \omega^k) \to 0. \]

Actually by Theorem 1.7.1 in [Kat73], \(H^1(X, \omega^{k-(p-1)}) = 0\) if \(k \geq p + 1\), so \(W_k(N) = S_k(N)\) when \(k \geq p + 1\).

An \(\mathbb{F}_p\)-structure on an elliptic curve \(E/\overline{\mathbb{F}}_p\) is an elliptic curve \(E'/\mathbb{F}_p\) such that \(E\) is isomorphic to \(E' \otimes \overline{\mathbb{F}}_p\).

**Lemma 2.1.** 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.** It is well-known that \(E\) is supersingular if and only if \([-p] : E \to E\) is purely inseparable (see for instance Theorem V.3.1 of [Sil86]). Multiplication by \(-p\) is an isogeny of degree \(p^2\), so by Corollary II.2.12 of [Sil86] there is a commutative triangle
\[ \begin{array}{ccc}
E & \xrightarrow{[-p]} & E \\
\downarrow \scriptscriptstyle{\text{Fr}^2} & & \downarrow \sim \\
E^{(p^2)} & & \\
\end{array} \]
where \(E^{(p^2)}\) is obtained by raising to the power \(p^2\) the coefficients of a Weierstrass equation for \(E\) and \(\text{Fr}^2 : E \to E^{(p^2)}\) is the morphism \([x : y : z] \mapsto [x^{p^2} : y^{p^2} : z^{p^2}]\). Since \(E \cong E^{(p^2)}\) we have \(j(E) = j(E^{(p^2)}) = j(E)^{p^2}\), i.e. \(j(E) \in \mathbb{F}_p^2\). Therefore there exists a supersingular elliptic curve \(E''/\mathbb{F}_p^2\) such that \(j(E'') = j(E)\). In other words, \(E\) has an \(\mathbb{F}_p^2\)-structure.
The curve $E''$ is supersingular so the morphism $[-p]: E' \to E''$ is purely inseparable. As before we have a commutative diagram

$$
\begin{array}{ccc}
E' & \xrightarrow{[-p]} & E'' \\
\downarrow{\pi'} & & \downarrow{\lambda} \\
E' & \xrightarrow{\sim} & E'',
\end{array}
$$

where $\pi'': E'' \to E''$ is the geometric Frobenius $[x : y : z] \mapsto [x^{p^2} : y^{p^2} : z^{p^2}]$, and $\lambda \in \text{Aut}(E'')$. Therefore

$$
\pi'' = \lambda^{-1} \circ [-p] = [-p] \circ \lambda^{-1}.
$$

As usual, we write $G_{F_{p^2}}$ to denote $\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{p^2})$. Let $\sigma \in G_{F_{p^2}}$ be the Frobenius element, defined by $x \mapsto x^{p^2}$; it is a topological generator of $G_{F_{p^2}}$. Consider the continuous 1-cocycle $\xi: G_{F_{p^2}} \to \text{Aut}(E'')$ defined by $\sigma \mapsto \lambda^{-1}$. Since $\lambda^{-1}$ is a morphism defined over $\mathbb{F}_{p^2}$, $\sigma$ acts trivially on $\lambda^{-1}$ and $\xi$ is a group homomorphism. Using a combination of Theorem X.2.2 and Proposition X.5.3 in [Sil86], we know that given $\xi \in H^1(G_{F_{p^2}}, \text{Aut}(E''))$ one can construct an elliptic curve $E'/\mathbb{F}_{p^2}$ and an isomorphism $\phi: E' \otimes \overline{\mathbb{F}}_p \to E'' \otimes \overline{\mathbb{F}}_p$ satisfying

$$
\xi(\tau) = \phi^\tau \circ \phi^{-1}, \quad \text{for all } \tau \in G_{F_{p^2}}.
$$

We recall that the action of $G_{F_{p^2}}$ on $\overline{\mathbb{F}}_p$-morphisms is given by

$$
\phi^\tau(P) = \left(\phi \left(P^{\tau^{-1}}\right)\right)^\tau.
$$

We’ll now work with quasi-isogenies so that we can make sense of things like $(\pi')^{-1}$. If we work on points the previous relation can be written

$$
\phi^\sigma(P) = \pi'' \circ \phi \circ (\pi')^{-1}(P).
$$

Therefore

$$
\lambda^{-1}(P) = \xi(\sigma)(P) = \pi'' \circ \phi \circ (\pi')^{-1} \circ \phi^{-1}(P).
$$

Now

$$
\pi''(P) = [-p] \circ \lambda^{-1}(P) = [-p] \circ \pi'' \circ \phi \circ (\pi')^{-1} \circ \phi^{-1}(P) \Rightarrow \pi'(P) = [-p](P),
$$

where we’ve made extensive use of the fact that $[-p]$ commutes with everything. We conclude that $\pi' = [-p]$ as maps $E'(\overline{\mathbb{F}}_p) \to E'(\overline{\mathbb{F}}_p)$, from which it follows that they are equal as morphisms.

It remains to prove the functoriality. Suppose we have a morphism $f: E_1 \to E_2$ of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Let $E'_1$, $E'_2$ be the respective canonical $\mathbb{F}_{p^2}$-structures, then $f$ induces a morphism $f': E'_1 \otimes \overline{\mathbb{F}}_p \to E'_2 \otimes \overline{\mathbb{F}}_p$. On points, we have as before

$$
(f')^\sigma(P) = \pi'_2 \circ f' \circ (\pi'_1)^{-1}(P) = [-p] \circ f' \circ [-p]^{-1}(P) = f'(P).
$$

This equality holds on points, so it also holds as morphisms. Since $f'$ is fixed by the generator of $G_{F_{p^2}}$, it is fixed by the whole group therefore it is defined over $\mathbb{F}_{p^2}$.

Since $E$ has a canonical $\mathbb{F}_{p^2}$-structure, so does its cotangent space $\omega(E)$. Therefore the vector space $\omega^{p^2-1}(E)$ has a canonical $\mathbb{F}_{p^2}$-basis and we can identify $\omega^k(E)$ with $\omega^{k+p^2-1}(E)$.

Let $\Sigma(N)$ denote the finite set of $\mathbb{F}_{p^2}$-isomorphism classes of triples $(E, \alpha, \eta)$, where $E$ is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$, $\alpha: E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ is a level $N$ structure and $\eta \neq 0$ is an invariant differential defined over $\mathbb{F}_{p^2}$. To save brackets, we’ll write the isomorphism class of the triple $(E, \alpha, \eta)$ as $[E, \alpha, \eta]$. 

6 On the other hand, fix a supersingular elliptic curve $E_0$ over $\mathbf{F}_p$ and let $\mathcal{O} = \text{End}(E_0)$, $B = \text{End}^0(E_0) = \mathcal{O} \otimes \mathbb{Q}$. For any prime $\ell \neq p$ let $\mathcal{O}_{\ell}^\times(N)$ denote those elements of $\mathcal{O}_{\ell}^\times$ which are congruent to 1 modulo $\ell^n$, where $\ell^n \parallel N$. Let $\mathcal{O}_{\ell}^\times(1)$ be the kernel of the map $\mathcal{O}_{\ell}^\times \rightarrow \mathbf{F}_p^\times$ given by reduction modulo the uniformizer $\pi$ of $\mathcal{O}_{\ell}$. Finally let

$$U := B_{\ell}^\times \times \mathcal{O}_{\ell}^\times(1) \times \prod_{\ell \neq p} \mathcal{O}_{\ell}^\times(N)$$

and

$$\Omega(N) := U \backslash A_{B}^\times / B^\times.$$

For $\ell \nmid pN$ we have Hecke operators $T_\ell$ acting on both $\Sigma(N)$ and $\Omega(N)$ (see §2.5.1 for the definition). The main technical result of this section is

**Theorem 2.2.** There exists a bijection $\Sigma(N) \cong \Omega(N)$ which is compatible with
- the action of the Hecke operators $T_\ell$, $\ell \nmid pN$,
- the action of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$,
- raising the level $N$.

We now return to the topic of modular forms. We can identify $S_k(N)$ with the functions $f : \Sigma(N) \rightarrow \mathbf{F}_p$ such that

$$f([E, \alpha, \lambda\eta]) = \lambda^{-k} f([E, \alpha, \eta]) \quad \forall \lambda \in \mathbf{F}_p^\times.$$

The modular forms $M_k(\Omega(N))$ of weight $k$ on $\Omega(N)$ are functions $f : \Omega(N) \rightarrow \mathbf{F}_p$ such that

$$f(\lambda[x]) = \lambda^{-k} f([x]) \quad \forall \lambda \in \mathcal{O}_p^\times / \mathcal{O}_p^\times(1) = \mathbf{F}_p^\times.$$

The Hecke operators on $\Sigma(N)$, respectively $\Omega(N)$, induce Hecke operators acting on the corresponding modular forms. It follows immediately from Theorem 2.2 that there is a bijection

$$S_k(N) \cong M_k(\Omega(N))$$

which is compatible with the action of the Hecke operators.

**Lemma 2.3.** As $k$ varies, $S_k(N)$ is periodic of period $p^2 - 1$.

*Proof.* By Lemma 2.1 we know that any supersingular curve $E$ over $\mathbf{F}_p$ has a canonical $\mathbf{F}_{p^2}$-structure. Therefore the cotangent space $\omega(E)$ has a canonical $\mathbf{F}_{p^2}$-structure and $\omega^{p^2-1}(E)$ has a canonical $\mathbf{F}_{p^2}$-basis. Hence for any $k$ we can identify $\omega^k(E)$ with $\omega^{k+p^2-1}(E)$, and $S_k(N)$ with $S_{k+p^2-1}(N)$. \(\square\)

**Lemma 2.4.** Every sequence $(a_{\ell})$ occurring as a system of eigenvalues of the Hecke operators acting on some $M_k(N)$ also occurs in some $S_{k'}(N)$, and conversely.

*Proof.* Suppose $(a_{\ell})$ is given by $f \in M_k(N)$, i.e. $T_\ell f = a_{\ell} f$ for all $\ell \nmid pN$. Factor $f = A^m g$, where $m$ is a nonnegative integer and $A$ does not divide $g$. Let $k' = k - m(p - 1)$, then $g$ has weight $k'$. Since multiplication by $A$ is a Hecke map we conclude that $g$ is a Hecke eigenform with eigenvalues $a_{\ell}$.

Conversely, if $(a_{\ell})$ is given by $g \in S_k(N)$ we may assume by Lemma 2.3 that $k \geq p + 1$, in which case the restriction map

$$M_k(N) \rightarrow S_k(N)$$

is surjective. We now use Proposition 1.2.2 of [AS86] to conclude that $(a_{\ell})$ is given by some $f \in M_k(N)$. \(\square\)
Let \( k \) vary. We conclude that there is a bijection between the systems of eigenvalues coming from

\[ M_\ast(N) := \bigoplus_k M_k(N) \]

and those coming from

\[ M_\ast(\Omega(N)) := \bigoplus_{k \mod (p^2-1)} M_k(\Omega(N)). \]

If we let \( N \) vary, we get

\[ \bigoplus_N M_\ast(N) = \left\{ \text{functions } \bigcup_N \Omega(N) \to \mathbb{F}_p \right\}. \]

The right hand side is the space of \( \mathcal{O}_p^\times(1) \)-invariant locally constant functions from \( \mathbb{A}_B^\times/B^\times \) to \( \mathbb{F}_p \). The following lemma is the last step of the proof of Theorem 1.1:

**Lemma 2.5.** Let \( G \) be a pro-p-group with a continuous action on an \( \mathbb{F}_p \)-vector space \( V \), and let \( T_\ell \) be endomorphisms of \( V \) that commute with the action of \( G \). Let \( (a_\ell) \) be a system of eigenvalues of the \( T_\ell \) given by a common eigenvector \( v \in V \). Then we can choose \( v \) in such a way that it is \( G \)-invariant.

**Proof.** We are given a continuous representation

\[ \rho : G \to \text{GL}(V), \]

where \( G = \varprojlim G_j \) has the profinite topology and \( \text{GL}(V) \) has the discrete topology. The kernel of \( \rho \) is the inverse image of the open set \( \{1\} \) so it is open, but a basis of open neighborhoods of the identity in \( G \) is given by the kernels of the maps \( G \to G_j \). Therefore \( \rho \) factors as in the following diagram:

\[
\begin{array}{ccc}
G & \xrightarrow{\rho} & \text{GL}(V) \\
\downarrow \pi & & \downarrow \rho \\
\bar{G}, & & \\
\end{array}
\]

where \( \bar{G} \) is a finite group. Define

\[ w := \sum_{g \in \bar{G}} \bar{\rho}(g)v. \]

We have

\[ T_\ell w = \sum_{g \in \bar{G}} T_\ell \bar{\rho}(g)v = \sum_{g \in \bar{G}} \bar{\rho}(g)T_\ell v = \sum_{g \in \bar{G}} \bar{\rho}(g)a_\ell v = a_\ell \sum_{g \in \bar{G}} \bar{\rho}(g)v = a_\ell w, \]

so \( w \) is a common eigenvector of the \( T_\ell \), with the same eigenvalues as \( v \). Finally for \( h \in G \) we have

\[ \rho(h)w = \bar{\rho}(\pi(h))w = \sum_{g \in \bar{G}} \bar{\rho}(\pi(h))\bar{\rho}(g)v = \sum_{g \in \bar{G}} \bar{\rho}(\pi(h)g)v = \sum_{g' \in \bar{G}} \bar{\rho}(g')v = w, \]

so \( w \) is \( G \)-invariant. \( \square \)

2.3. Preliminary results.
2.3.1. $p$-divisible groups and Dieudonné modules. We start by recalling the basic terminology and results of contravariant Dieudonné theory, following [Fon77].

A $p$-divisible group of height $h$ is a system
$$G_0 \xrightarrow{i_0} G_1 \xrightarrow{i_1} \ldots \xrightarrow{i_n} G_n \xrightarrow{i_n} \ldots,$$
where for all $n$, $G_n$ is a finite commutative group scheme of rank $p^n$, $i_n$ is a group homomorphism and the following sequence is exact:
$$0 \rightarrow G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{p^n} G_{n+1}.$$
This definition was tailored specifically so that $A[p^n] = (A[p^n])$ is a $p$-divisible group of height $2\dim A$.

If $G = (G_n, i_n)$ and $H = (H_n, j_n)$ are $p$-divisible groups, a homomorphism $f : G \rightarrow H$ is a system of group scheme homomorphisms $f_n : G_n \rightarrow H_n$ such that the following diagram commutes for all $n \geq 1$:

$$
\begin{array}{ccc}
G_n & \xrightarrow{i_n} & G_{n+1} \\
\downarrow{f_n} & & \downarrow{j_{n+1}} \\
H_n & \xrightarrow{j_n} & H_{n+1}.
\end{array}
$$

Let $k$ be a perfect field of characteristic $p > 0$. Let $W := W(k)$ be the ring of infinite Witt vectors over $k$, i.e. the ring of integers of the absolutely unramified complete extension $L$ of $\mathbb{Q}_p$ with residue field $k$. Let $\sigma : W \rightarrow W$ be the automorphism induced by the Frobenius $x \mapsto x^p$ of $k$. Let $\mathcal{A} := W[F, V]$, where the Frobenius $F$ and the Verschiebung $V$ are variables satisfying
$$FV = VF = p, \quad F\lambda = \sigma(\lambda)F, \quad V\lambda = \sigma^{-1}(\lambda)V \quad \forall \lambda \in W.$$ Let $W_n$ denote the $n$-th Witt group scheme. If $G$ is a commutative $k$-group scheme, we define its Dieudonné module by
$$M(G) := \lim_{\rightarrow} \Hom_{k^{gp}}(G, W_n) \oplus (W(\bar{k}) \otimes_{\mathbb{Z}} \Hom_{k^{gp}}(G_{\bar{k}}, (\mathbb{G}_m)_{\bar{k}}))^\Gal(\bar{k}/k).$$

**Theorem 2.6** (Dieudonné-Cartier-Barsotti-Oda). The functor $M$ gives an anti-equivalence from the category of finite commutative $k$-group schemes of $p$-power rank to the category of left $\mathcal{A}$-modules of finite $W$-length, taking a group of rank $p^n$ to a module of length $n$. It is compatible with perfect base extension, i.e. if $K/k$ is perfect then
$$M(G_K) \cong W(K) \otimes_W M(G).$$

The proof of this is on page 69 of [Dem72]. The main ingredient is to be found in §V.1.4 of [DG70].

**Theorem 2.7** (Oda). If $G = (G_n)$ is a $p$-divisible group of height $h$, $M(G) := \lim_{\rightarrow} M(G_n)$ is a left $\mathcal{A}$-module which is $W$-free of rank $h$. This gives an equivalence of these two categories which is compatible with perfect base extension.

One can define the dual of a Dieudonné module $M$ by setting $M^* := \Hom_W(M, W)$ and
$$(F^*u)(m) := \sigma(u(Vm)), \quad (V^*u)(m) := \sigma^{-1}(u(Fm))$$
for all $u \in M^*$, $m \in M$.

**Lemma 2.8.** If $W$ is a local ring with residue field $k$, then any $W$-module of length 1 is isomorphic to $k$. If $W$ is a DVR with uniformizer $\pi$, then any $W$-module of length $n$ is isomorphic to one of the form
$$\bigoplus_{i=1}^l W/(\pi^{e_i}W), \quad e_i > 0, \sum e_i = n.$$
Proof. Let $M$ be a $W$-module of length 1. Let $x \in M$ nonzero and consider $Wx$. This is a $W$-module and $0 \subseteq Wx \subset M$ so because $M$ has length 1 we have $Wx = M$. From this we conclude that the $W$-module homomorphism $W \to M$ given by $w \to wx$ is surjective with kernel $\operatorname{Ann} M = \{w \in W : wM = 0\}$, so $M \cong W/\operatorname{Ann} M$. Since $\pi W$ is the unique maximal ideal of $W$ we have a canonical surjective homomorphism of $W$-modules

$$\phi : W/\operatorname{Ann} M \to W/\pi W \cong k.$$ 

But $M$ has length 1 so $\ker \phi$ is either 0 or $M$. The latter is impossible since $\phi$ is surjective, so $M \cong k$.

We now prove the second assertion by induction on the length $n$. The base case $n = 1$ is what we just proved above. Now suppose the assertion is true for all $W$-modules of length strictly less than $n$ and let $M$ be a $W$-module of length $n$. We have two possibilities:

- Suppose $M = Wx$. Then as before $M \cong W/\operatorname{Ann} M$. But $\operatorname{Ann} M$ is a proper ideal of $W$, hence $\operatorname{Ann} M = \pi^i W$ for some $i$, since $W$ is a DVR. The quotient $W/\pi^i W$ has length $i$, on the other hand $M$ has length $n$ so $i = n$ and $M \cong W/\pi^n W$.

- Suppose $M$ is not generated by a single element; say $\{x_1, \ldots, x_j\}$ is a minimal set of generators for $M$. I claim that $M$ is actually the direct sum of the $Wx_i$. Suppose $Wx_1 \cap Wx_2 \neq 0$. Then there exist nonzero $w_1, w_2 \in W$ such that $w_1 x_1 = w_2 x_2$. But $W$ is a DVR, so $w_1 = u_1 \pi^{n_1}, w_2 = u_2 \pi^{n_2}$ where $u_1, u_2 \in W^\times$ and $n_1, n_2 \in \mathbb{N}$. Suppose without loss of generality that $n_2 \geq n_1$. Then $x_1 = u_1^{-1} u_2 \pi^{n_2-n_1} x_2$, so $Wx_1 \subset Wx_2$, contradicting the minimality of the chosen set of generators. So

$$M = Wx_1 + Wx_2 + \ldots Wx_j$$

and we can apply the induction hypothesis to each of the $Wx_i$ since they have length smaller than $n$.

Let $E'$ be a supersingular elliptic curve over $\mathbb{F}_{p^2}$, whose Frobenius satisfies $\pi_{E'} = -p$. The goal of this section is to describe the structure of the Dieudonné module of the $p$-divisible group $E'[p^\infty]$, and to identify its endomorphism ring. The idea is to understand $M(E'[p])$ first, and then lift it to get $M(E'[p^2])$, and so on all the way to $M(E'[p^\infty])$.

Within this section we'll use $k$ to denote the field $\mathbb{F}_{p^2}$. If $\tau$ is an automorphism of $k$, $T : k \to k$ is a $\tau$-linear operator and $A$ is the matrix of $T$ with respect to some basis, we shall write

$$T = A\tau.$$ 

This helps eliminate the confusion that arises when composing several such operators.

The structure of $M(E'[p])$. We're looking for a left $A$-module of $W$-length 2 which is killed by $p$ and such that

$$F^2 = -p\sigma^2 = 0.$$ 

By Lemma 2.8, we have that $M \cong (W/pW)^2 = k^2$. Alternatively, we know that

$$M(E'[p^n]) = M(E'[p^\infty])/(p^n)$$

and $M(E'[p^\infty])$ is free of rank 2 because $E'[p^\infty]$ has height 2. Therefore $M(E'[p^n]) \cong W_n^2$.

It remains to find the semi-linear operators $F$ and $V$. A priori there are several cases according to the $k$-dimension of $\ker F$. But the following result, applied with $X = Y = E'$, $f = f^t = \text{multiplication by } p$ says that $E'[p]$ is self-dual:

**Theorem 2.9** (See Theorem III.19.1 in [Oor66]). Let $f : X \to Y$ be an isogeny of abelian varieties with kernel $K$, and let $\bar{K}$ be the kernel of the dual isogeny $f^t : Y^t \to X^t$. Then there is a canonical isomorphism between the dual $K^t$ of $K$ and $\bar{K}$.
Therefore $M = M(E'[p])$ is self-dual, which in particular means that the kernels of $F$ and $V$ have the same dimension. First we rule out the case $\dim \ker F = \dim \ker V = 0$: $F$ cannot be bijective because $F^2 = 0$.

We also rule out the case $\dim \ker F = \dim \ker V = 0$, i.e. $F = V = 0$. This can be done in two different ways:

- If $F = 0$, then the Frobenius of $M(E'[p^2])$ can be expressed as $pA$ for some $A \in M_2(k)$, and its square will be $p^2A^2 = 0 \neq -p$, contradiction.
- If $F = V = 0$, then $M = M(\alpha_p) \oplus M(\alpha_p)$, where $M(\alpha_p) = (k, F = 0, V = 0)$ is the Dieudonné module of the finite group scheme $\alpha_p$. So we want to show that $E'[p]$ is not isomorphic to $\alpha_p^2$. The dimension of the tangent space to $E'[p]$ at the origin is the same as the dimension of the tangent space to $E'$ at the origin, which is 1 since $E'$ is a smooth curve. The dimension of the tangent space to $\alpha_p^2$ at the origin is twice the dimension of the tangent space to $\alpha_p$ at the origin, i.e. $2 \times 1 = 2$. Therefore we get a contradiction.

The only remaining possibility is $\dim \ker F = 1$. Say $\ker F = km_1$ and pick $m_2 \in M$ such that \{m_1, m_2\} is a basis of $M$, then $F = (\begin{smallmatrix} 0 & a_1 \\ 1 & 0 \end{smallmatrix}) \sigma$. We impose $F^2 = 0$:

$$F^2 = (\begin{smallmatrix} 0 & a_1a_2^p \\ 0 & a_2^{p+1} \end{smallmatrix}) \sigma^2 = 0 \Rightarrow a_2 = 0.$$  

We can also change the basis in such a way that $a_1$ becomes 1: let $m'_1 = m_1$, $m'_2 = a_1^{-1/p}m_2$ (can take $p$-th roots because $\mathbb{F}_{p^2}$ is perfect). With respect to the basis \{m'_1, m'_2\} we have

$$F = (\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}) \sigma.$$  

The Verschiebung is given a priori by some matrix

$$V = (\begin{smallmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{smallmatrix}) \sigma^{-1}.$$  

We impose $FV = VF = 0$:

$$FV = (\begin{smallmatrix} b_{11}b_{21} & b_{12}b_{22} \\ 0 & 0 \end{smallmatrix}) = 0 \Rightarrow b_{21} = b_{22} = 0,$$

$$VF = (\begin{smallmatrix} 0 & b_{11} \\ 0 & 0 \end{smallmatrix}) = 0 \Rightarrow b_{11} = 0.$$  

Therefore the matrix of $V$ is of the form

$$V = (\begin{smallmatrix} 0 & \lambda \\ 0 & 0 \end{smallmatrix}) \sigma^{-1},$$  

where $\lambda \neq 0$ since $\dim \ker V = 1$. Any change of basis that fixes the matrix of $F$ also fixes the matrix of $V$, so it looks like we’re stuck with the parameter $\lambda$. But we can find the actual value of $\lambda$ by investigating $M_2 = M(E'[p^2])$.

The structure of $M(E'[p^2])$. We use Nakayama’s lemma to lift the basis of $k^2$ to a basis of $W^2$. With respect to this basis the operators $F$ and $V$ look like

$$F = (\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}) \sigma + pA \sigma, \quad V = (\begin{smallmatrix} 0 & \lambda \\ 0 & 0 \end{smallmatrix}) \sigma^{-1} + pB \sigma^{-1}.$$  

We impose the conditions $F^2 = -pA^2$, $FV = VF = p$:

$$F^2 = p(\begin{smallmatrix} a_{11} & a_{12}+a_{22} \\ 0 & a_{22} \end{smallmatrix}) \sigma^2 = -pA^2 \Rightarrow a_{21} = -1, a_{11} = -a_{22}^p,$$

$$FV = p(\begin{smallmatrix} b_{11} & b_{12} - \lambda^p a_{22} \\ 0 & -\lambda^p \end{smallmatrix}) = p \Rightarrow b_{21} = 1, \lambda = -1, a_{22} = -b_{22},$$

$$VF = p(\begin{smallmatrix} 1 & b_{11}/\lambda + b_{11} \\ 0 & 1 \end{smallmatrix}) = p \Rightarrow b_{22} = -b_{11}^p.$$  

This implies that $F$ and $V$ are of the form

$$F = (\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}) \sigma + p(\begin{smallmatrix} -b_{11} & a_{12} \\ -1 & b_{11}^{p-1} \end{smallmatrix}) \sigma, \quad V = (\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}) \sigma^{-1} + p(\begin{smallmatrix} b_{11} & b_{12} \\ 1 & -b_{11}^{p-1} \end{smallmatrix}) \sigma^{-1}.$$
In particular,

\[ M(E'[p]) = (k^2, F = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \sigma, V = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \sigma^{-1}). \]

We're only a few matrix multiplications away from having the structure of \( M(E'[p^2]) \), so we might as well do it. We want to change the basis of \( W_2^2 \) in such a way that the matrices for \( F \) and \( V \) look nicer. To keep this simple, we will change the basis by a matrix of the form

\[ I + pC, \quad \text{where} \quad C = \begin{pmatrix} c_{21} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \in M_2(k). \]

The new matrix for the Frobenius will be

\[ \left( I - p \left( \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \right) \right) \left( \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + p \left( \begin{pmatrix} b_{11} & a_{12} \\ -1 & b_{11} \end{pmatrix} \right) \right) \sigma (I + p \left( \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \right)) = \left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \sigma + p \left( \begin{pmatrix} b_{11} & a_{12} - c_{11} + c_{22} \\ -1 & b_{11} - c_{22} \end{pmatrix} \right) \sigma \right). \]

So we can set \( c_{21} = b_{11}^p, c_{11} = c_{22}^p + a_{12} \) and get a very simple expression for \( F \). What about \( V \)? The new matrix for it is

\[ \left( I - p \left( \begin{pmatrix} a_{12} + c_{22}^p \\ b_{11} \end{pmatrix} \right) \right) \left( \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} + p \left( \begin{pmatrix} b_{11} & b_{12} \\ 1 & b_{11} \end{pmatrix} \right) \right) \sigma^{-1} (I + p \left( \begin{pmatrix} a_{12} + c_{22}^p \\ b_{11} \end{pmatrix} \right) \sigma^{-1} = \left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \sigma^{-1} + p \left( \begin{pmatrix} 0 & a_{12} + b_{12} \\ 0 & 0 \end{pmatrix} \sigma^{-1} \right). \]

All we can say so far is that there exists a basis of \( W_2^2 \) with respect to which

\[ F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \sigma + p \left( \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \sigma, V = \left( \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \sigma^{-1} + p \left( \begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix} \sigma^{-1}, \right. \]

where \( \lambda \in \mathbb{F}_p \). It turns out that we can pin down \( \lambda \), once again by going a step higher. Lift this basis to one of \( W_3^2 \); we have

\[ F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \sigma + p \left( \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \sigma + p^2 A \sigma, V = \left( \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} + p \left( \begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix} \sigma^{-1} + p^2 B \sigma^{-1}, \right. \]

We impose the conditions \( F^2 = -p \sigma^2, FV = p \):

\[ F^2 = p \left( \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \sigma + p^2 \left( \begin{pmatrix} a_{21}^p & a_{22}^p + a_{11} \\ a_{21}^p & a_{22}^p \end{pmatrix} \right) \sigma^2 = -p \sigma^2 \Rightarrow a_{21} = 0, a_{11} = -a_{22}^p, \]

\[ FV = p \left( \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} + p \left( \begin{pmatrix} b_{21}^p & b_{22}^p + a_{22}^p \\ 0 & 0 \end{pmatrix} \lambda^p \right) \right) = p \Rightarrow b_{21} = 0, a_{22} = -b_{22}, \lambda = 0. \]

Therefore

\[ M(E'[p^2]) = (W_2^2, F = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix} \sigma, V = \left( \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \sigma^{-1}). \]

Proposition 2.10. For any integer \( n \geq 2 \) we have

\[ M(E'[p^n]) = (W_2^n, F = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix} \sigma, V = \left( \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \sigma^{-1}). \]

Proof. We proceed by induction on \( n \), the base case \( n = 2 \) having been done above. Suppose the statement is true for \( n \geq 2 \). Use Nakayama’s lemma to lift the basis of \( W_n^2 \) to one of \( W_{n+1}^2 \). With respect to the latter we have

\[ F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \sigma + p \left( \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \sigma + p^n A \sigma, V = \left( \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \sigma^{-1} + p \left( \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \sigma^{-1} + p^n B \sigma^{-1}. \right. \]
We impose the conditions $F^2 = -p$, $FV = V^F GHTZA$

\[
F^2 = -p\sigma^2 + p^n \begin{pmatrix} a_{21}^p & a_{22}^p + a_{11}^p \\ 0 & 0 \end{pmatrix} \sigma^2 = -p\sigma^2 \Rightarrow a_{21} = 0, a_{11} = -a_{22}^p,
\]

\[
FV = p + p^n \begin{pmatrix} b_{21}^p & b_{22}^p + b_{11}^p \\ 0 & 0 \end{pmatrix} = p \Rightarrow a_{22} = -b_{22}, a_{11} = b_{22}^p, b_{21} = 0,
\]

\[
VF = p + p^n \begin{pmatrix} 0 & b_{12}^p + b_{11}^p \\ 0 & 0 \end{pmatrix} = p \Rightarrow b_{22} = -b_{11}^p,
\]

and conclude that

\[
A = \begin{pmatrix} -b_{11} & a_{12} \\ 0 & b_{11}^p \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} \\ 0 & -b_{11}^p \end{pmatrix}.
\]

We'll apply a change of basis with matrix $I + p^nC$. The new matrix of the Frobenius is

\[
(I - p^n \begin{pmatrix} c_{11} & c_{12} \\ b_{11} & b_{12} \end{pmatrix}) \left( \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + p \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + p^n \begin{pmatrix} -b_{11} & a_{12} \\ -b_{11}^p & b_{11}^p \end{pmatrix} \right) \sigma \left( I + p^n \begin{pmatrix} c_{11} & c_{12} \\ b_{11} & b_{12} \end{pmatrix} \right) = (0 0) \sigma + p (0 0) \sigma + p^n (0 0) \sigma - 1 + p^n (0 0) \sigma^{-1},
\]

where $\lambda \in \mathbb{F}_p^2$. We want to show that $\lambda = 0$; for this we need to go to $M(E'[p^{n+2}])$. Lift the new basis of $W_n^2$ to $W_{n+2}^2$. Our operators are of the form

\[
F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \sigma + p \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \sigma + p^{n+1} A \sigma,
\]

\[
V = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \sigma^{-1} + p \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \sigma^{-1} + p^n \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \sigma^{-1} + p^{n+1} B \sigma^{-1}.
\]

We impose the conditions $F^2 = -p\sigma^2$ and $FV = p:

\[
F^2 = -p\sigma^2 + p^{n+1} \begin{pmatrix} a_{21}^p & a_{22}^p + a_{11}^p \\ 0 & 0 \end{pmatrix} \sigma^2 = -p\sigma^2 \Rightarrow a_{21} = 0, a_{11} = -a_{22},
\]

\[
VF = p + p^{n+1} \begin{pmatrix} b_{21}^p & b_{22}^p + b_{11}^p \\ 0 & 0 \end{pmatrix} = p \Rightarrow b_{21} = 0, a_{22} = -b_{22}, \lambda = 0.
\]

This concludes the proof of the proposition. \(\square\)

A direct consequence of this is that

\[
M(E'[p^{\infty}]) = (W, F = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix} \sigma, V = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \sigma^{-1}).
\]

The endomorphism ring of $M(E'[p^{\infty}])$.

**Corollary 2.11.** Let $M = M(E'[p^{\infty}])$. Then $\text{End}(M) = \mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$, where $\mathcal{O} = \text{End}(E')$. Moreover, $\mathcal{O}_p^\times(1)$ can be identified with the group of automorphisms of $M$ which lift the identity map on $M/FM$.

**Proof.** Let $g \in \text{End}(M)$; 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

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

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

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 doesn't give anything new. Therefore

\[
\text{End}(M) = \left\{ \begin{pmatrix} x & y \\ -yp & x \end{pmatrix} : x, y \in \mathbb{W}(\mathbb{F}_p^2) \right\} = \left\{ \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} + F \begin{pmatrix} 0 & 0 \\ 0 & y \end{pmatrix} : x, y \in \mathbb{W}(\mathbb{F}_p^2) \right\}.
\]
But $W(F_{p^2})$ is the ring of integers of the unique unramified quadratic extension $L$ of $Q_p$. Let $\pi$ be a solution of $X^2 + p = 0$ in $L$. The map $\sigma : x \mapsto x^p$ is the unique nontrivial automorphism of $L$. It is now easy to see that the map

$$\varphi : \text{End}(M) \to B_p = \{L,-p\} = B \otimes Q_p$$

$$(\varphi_0 \ 0 \ 0) + F\left(\begin{array}{c} 0 \ 0 \ 0 \\ 0 \ y \ y' \end{array}\right) \mapsto x + \pi y$$

is an injective ring homomorphism. It identifies $\text{End}(M)$ with $O_p = \{x + \pi y : x, y \in O_L\}$, the unique maximal order of $B_p$.

It remains to prove the last statement. Let $g = \left(\begin{array}{c} x \ y' \\ -y \ x' \end{array}\right) \in \text{End}(M)^\times = O_p^\times$. Note that

$$M/FM = \left\{\left(\begin{array}{c} 1 \ 0 \\ 0 \ \lambda \end{array}\right) + FM : \lambda \in F_{p^2}\right\}.$$ 

Let $\bar{x}$ be the reduction of $x$ modulo $\pi$, 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 $\pi$, i.e. with $O_p^\times(1)$.

**Corollary 2.12.** Let $E_1$, $E_2$ be two supersingular elliptic curves over $F_{p^2}$ and let $E'_1$, $E'_2$ denote their canonical $F_{p^2}$-structures. Put $M_1 = M(E'_1[p^\infty])$, $M_2 = M(E'_2[p^\infty])$. Then $M_1 \cong M_2$ and any isomorphism $M_1/FM_1 \cong M_2/FM_2$ lifts to an isomorphism $M_1 \cong M_2$.

**Proof.** We already proved the first part by describing the structure of $M = M(E'[p^\infty])$ for such curves. As for the second part, it suffices to show that any automorphism of $M/FM$ lifts to an automorphism of $M$. From the description of $M/FM$ in the proof of the previous corollary we know that the automorphisms are given by multiplication by some $\lambda \in F_{p^2}^\times$. But then the matrix

$$\left(\begin{array}{cc} \lambda^p & 0 \\ 0 & \lambda \end{array}\right)$$

represents an automorphism of $M$ which restricts to multiplication by $\lambda$ on $M/FM$, which is what we wanted to show.

**2.3.2. Local study of isogenies.**

**Lemma 2.13.** Let $\phi : A \to B$ be an isogeny of abelian varieties. For any prime $\ell$ and any $n \geq \text{ord}_\ell \deg \phi$, there exists a canonical isomorphism between the kernel and the cokernel of the restriction of $\phi$ to the $\ell^n$-torsion.

**Proof.** First suppose $\ell \neq p$. Let $\ell^k \| \deg \phi$ and $d := \ell^{-k} \deg \phi$. For any $n > 0$ let $K_{\ell,n}$ and $C_{\ell,n}$ denote the kernel and the cokernel of the restriction of $\phi$ to $A[\ell^n]$:

$$0 \to K_{\ell,n} \to A[\ell^n] \xrightarrow{\phi} B[\ell^n] \to C_{\ell,n} \to 0.$$ 

This is an exact sequence of finite groups so

$$1 = \frac{\#(K_{\ell,n}) \cdot \#(B[\ell^n])}{\#(A[\ell^n]) \cdot \#(C_{\ell,n})},$$

but $\#(A[\ell^n]) = \ell^{2gn} = \#(B[\ell^n])$ (where $g = \text{dim } A = \text{dim } B$) so $\#(K_{\ell,n}) = \#(C_{\ell,n})$.

Since $(d,\ell) = 1$, multiplication by $d$ is an injective endomorphism of $A[\ell^n]$. But by the order counting that we did above the cokernel is also trivial, so $d$ gives an automorphism of $A[\ell^n]$. Therefore it makes sense to define a map $f : B[\ell^n] \to A[\ell^n]$ as the composition:

$$B[\ell^n] \xrightarrow{\phi^\vee} A[\ell^n] \xrightarrow{\ell^{n-k}} A[\ell^n] \xrightarrow{d^{-1}} A[\ell^n].$$
Note that
\[
\phi \circ f = \phi \circ (d^{-1} \ell^{n-k} \phi(\ell^n)) = (\text{deg } \phi) d^{-1} \ell^{n-k} = \ell^n
\]
and $\ell^n : B[\ell^n] \to B[\ell^n]$ is just the zero map, so we actually have $f : B[\ell^n] \to \ker \phi = K_{\ell,n}$. Next we see that
\[
f \circ \phi = (d^{-1} \ell^{n-k} \phi(\ell^n)) \circ \phi = d^{-1} \ell^{n-k} (\text{deg } \phi) = \ell^n,
\]
so $f$ factors as
\[
A[\ell^n] \xrightarrow{\phi} B[\ell^n] \xrightarrow{f} C_{\ell,n} \xrightarrow{0}.
\]
To save letters we'll denote this map $C_{\ell,n} \to K_{\ell,n}$ by $f$. Now we define $g : K_{\ell,n} \to C_{\ell,n}$ such that $g$ is the inverse of $f$. Let $a \in K_{\ell,n}$ and pick $a' \in A$ such that $\ell^n a' = a$. Note that $\ell^n \phi(a') = \phi(\ell^n a') = \phi(a) = 0$ since $a \in \ker \phi$. So $\phi(a') \in B[\ell^n]$; let $g(a)$ be the image of $\phi(a')$ in $C_{\ell,n}$. This is easily seen to be well-defined: if $a'' \in A$ is such that $\ell^n a'' = a$, then $\ell^n (a'' - a') = a - a = 0$ so $a'' - a' \in A[\ell^n]$ and we get
\[
\phi(a'') = \phi(a' + (a'' - a')) = \phi(a') + \phi(a'' - a'),
\]
and $\phi(a'' - a')$ gets mapped to 0 in $C_{\ell,n}$. It is clear that $f$ and $g$ are inverses:
\[
f(g(a)) = f(\phi(\ell^n a)) = d^{-1} \ell^{n-k} \phi(\ell^n a) = d^{-1} \ell^{n-k} (\text{deg } \phi) \ell^n a = a,
\]
and similarly $g(f(b)) = b$.

When $\ell = p$ we have an exact sequence of finite commutative group schemes
\[
0 \to K_{p,n} \to A[p^n] \xrightarrow{\phi} B[p^n] \to C_{p,n} \to 0,
\]
where the map $\phi$ is obtained by the usual argument from
\[
\begin{array}{cccccc}
0 & \longrightarrow & A[p^n] & \xrightarrow{\phi} & A & \xrightarrow{p^n} & A & \xrightarrow{0} \\
& & \downarrow & & \downarrow & & \downarrow & \\
0 & \longrightarrow & B[p^n] & \xrightarrow{\phi} & B & \xrightarrow{p^n} & B & \xrightarrow{0}.
\end{array}
\]
Applying the Dieudonné functor $M$ we get an exact sequence of left $A$-modules of finite length
\[
0 \to M(C_{p,n}) \to M(B[p^n]) \xrightarrow{M(\phi)} M(A[p^n]) \to M(K_{p,n}) \to 0.
\]
A trivial modification of the proof given above for $\ell \neq p$ will do the trick. The advantage of working with the Dieudonné modules instead of the group schemes is that for the construction of the inverse we need to work with actual elements, and they are not available in group-scheme-land.

**Proposition 2.14.** Let $\phi : A \to B$ be an isogeny of abelian varieties. For any prime $\ell \neq p$, $\phi$ induces an injective $\mathbb{Z}_\ell$-linear map $T_\ell \phi : T_\ell A \to T_\ell B$ whose cokernel is canonically isomorphic to $(\ker \phi)_\ell$.

When $\ell = p$, $\phi$ induces an injective $\mathbb{W}$-linear map $M(\phi) : M(B[p^\infty]) \to M(A[p^\infty])$ whose cokernel is canonically isomorphic to $M((\ker \phi)_p)$.

**Proof.** We start with $\ell \neq p$. Let $(a_n) \in T_\ell A$, i.e. $a_n \in A[\ell^n]$ and $a_{n-1} = \ell a_n$ for all $n$. Set $T_\ell \phi((a_n)) := (\phi(a_n))$. We have $\ell^n \phi(a_n) = \phi(\ell^n a_n) = \phi(0) = 0$ and $\phi(a_{n-1}) = \phi(\ell a_n) = \ell \phi(a_n)$ so indeed $(\phi(a_n)) \in T_\ell B$.

Suppose $T_\ell \phi((a_n)) = 0$, i.e. $\phi(a_n) = 0$ for all $n$. But $\phi$ is an isogeny so its kernel is finite, therefore the sequence $(a_n)$ has an infinite constant subsequence. Fix an integer $N > 0$, then there exist $n > m > N$ such that $a_n = a_m$. But $a_n = \ell^{n-m} a_m$, so we get $(\ell^{n-m} - 1)a_m = 0$, therefore
In particular $a_j = 0$ for all $j \leq N$. This works for arbitrarily large $N$ so $(a_n) = 0$ and $T_{\ell}\phi$ is injective.

By Lemma 2.13 we know that if $n \geq \ord_{\ell} \deg \phi$, the kernel $K_{\ell,n}$ of the restriction of $\phi$ to $A[\ell^n]$ is isomorphic to the cokernel $C_{\ell,n}$ of the same map. But for $n \geq \ord_{\ell} \deg \phi$ we have $K_{\ell,n} = (\ker \phi)_{\ell}$, so in particular $C_{\ell,n}$ stabilizes. Therefore for $n \geq \ord_{\ell} \deg \phi$ we have

$$\coker T_{\ell}\phi = C_{\ell,n} \to K_{\ell,n} = (\ker \phi)_{\ell},$$

which is what we wanted to show.

Now suppose $\ell = p$. The map $M(\phi) : M(A[p\infty]) \to M(B[p\infty])$ is simply

$$\cdots \xrightarrow{p} M(B[p^3]) \xrightarrow{p} M(B[p^2]) \xrightarrow{p} M(B[p]) \xrightarrow{M(\phi)} M(A[p^3]) \xrightarrow{p} M(A[p^2]) \xrightarrow{p} M(A[p]).$$

To show that $M(\phi)$ is injective, first note that $K_{p,n}$ is a subgroup scheme of $\ker \phi$ for all $n$. Since $\phi$ is an isogeny, $\ker \phi$ is a finite group scheme so the $K_{p,n}$ stabilize to $(\ker \phi)_p$. Applying the Dieudonné functor gives that the cokernel of $M(\phi)$ is isomorphic to $M((\ker \phi)_p)$.

Suppose $M(\phi)((a_n)) = 0$, then $a_n \in M(C_{p,n})$ for all $n$. But the $M(C_{p,n})$ stabilize so there exists $n_0$ such that $a_n \in M(B[p^{n_0}]) \cong W_{n_0}^2$ for all $n$. Since $p^{n_0} = 0$ in $W_{n_0}^2$ we get that $a_n = p^n a_0 = 0$ for all $n \geq n_0$. Therefore $(a_n) = 0$ and $M(\phi)$ is injective.

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

**Lemma 2.15.** Let $E$ be a supersingular elliptic curve over $\mathbb{F}_p$. Then a non-zero invariant differential on $E$ defined over $\mathbb{F}_{p^2}$ is equivalent to a choice of nonzero 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 $\mathbb{F}_{p^2}$ can easily be identified with the differentials of $E'$, i.e. with the cotangent space $\omega(E')$. Consider the exact sequence

$$0 \to E'[p] \to E' \xrightarrow{p} E' \to 0.$$

The contravariant functor $\omega$ is exact so we get an exact sequence

$$0 \to \omega(E') \xrightarrow{p} \omega(E') \to \omega(E'[p]) \to 0.$$

But $E'$ is supersingular so $p$ is purely inseparable, i.e. it induces the zero map on (co)tangent spaces. We conclude that $\omega(E') \cong \omega(E'[p])$. By Proposition III.4.3 in [Fon77], $\omega(E'[p])$ is isomorphic to $M/FM$, so $\omega(E') \cong M/FM$ and a choice of nonzero invariant differential of $E$ defined over $\mathbb{F}_{p^2}$ amounts to a choice of nonzero element in $M/FM$.}

### 2.4. Construction of the bijection

Fix a supersingular elliptic curve $E_0$ over $\mathbb{F}_p$ and let $O = \End(E_0)$, $B = \End^0(E_0) = \mathcal{O} \otimes \mathbb{Q}$, $M_0 = M(E_0'[p\infty])$, where $E_0'$ is the canonical $\mathbb{F}_{p^2}$-structure given by Lemma 2.1. We know that $B$ is isomorphic to the unique quaternion algebra ramified at $p$ and $\infty$. Also fix a level $N$ structure $\alpha_0 : E_0[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ and a nonzero invariant differential $\eta_0 \in M_0/FM_0$ defined over $\mathbb{F}_{p^2}$.

We consider triples of the form $(E_1, \alpha_1, \eta_1)$, where $E_1$ is a supersingular elliptic curve over $\mathbb{F}_p$, $\alpha_1 : E_1[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ is a full level $N$ structure and $0 \neq \eta_1 \in M_1/FM_1$ is a nonzero invariant differential form on $E_1$ defined over $\mathbb{F}_{p^2}$.

Recall from §2.2 that we defined $\Sigma(N)$ to be the finite set of $\mathbb{F}_p$-isomorphism classes of triples $(E_1, \alpha_1, \eta_1)$ as above. By Honda-Tate theory ([Tat68]) any two supersingular elliptic curves are
Isogenous; also any curve isogenous to a supersingular one is supersingular. Therefore after the choice of \((E_0, \alpha_0, \eta_0)\) the set \(\Sigma(N)\) can be identified with the set \(\Sigma^0(N)\) of triples \(\left(\phi_1 : E_0 \to E_1, \alpha_1 : E_1[\mathbb{N}] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2, 0 \neq \eta_1 \in M_1/FM_1\right)\),

where \(\phi_1 : E_0 \to E_1\) is an isogeny. Two such triples \((\phi_1, \alpha_1, \eta_1)\) and \((\phi_2, \alpha_2, \eta_2)\) are considered the same if there exists an isomorphism \(f : E_1 \to E_2\) such that \(M(f')(\eta_2) = \eta_1\) and the following diagram commutes:

\[
\begin{array}{ccc}
E_1[\mathbb{N}] & \xrightarrow{f} & E_2[\mathbb{N}] \\
\alpha_1 \downarrow \sim & & \alpha_2 \downarrow \sim \\
(\mathbb{Z}/N\mathbb{Z})^2 & \sim & (\mathbb{Z}/N\mathbb{Z})^2.
\end{array}
\]

For any prime \(\ell \neq p\) let \(\mathcal{O}_p^\times(N)\) denote those elements of \(\mathcal{O}_p^\times\) which are congruent to \(1\) modulo \(\ell^n\), where \(\ell^n||N\). Let \(\mathcal{O}_p^\times(1)\) be the kernel of the map \(\mathcal{O}_p^\times \to \mathbb{F}_p^\times\) given by reduction modulo the uniformizer \(\pi\) of \(\mathcal{O}_p\). Finally let

\[
U = B_\infty^\times \times \mathcal{O}_p^\times(1) \times \prod_{\ell \neq p} \mathcal{O}_\ell^\times(N)
\]

and

\[
\Omega(N) = U(1, N)\bs A_\mathbb{F}_p^\times/B_\mathbb{F}_p^\times.
\]

Since the level \(N\) is fixed throughout this section, we’ll drop the reference to \(N\) and write simply \(\Sigma, \Sigma^0\) and \(\Omega\) for our finite sets. The purpose of the section is to exhibit a canonical bijection between \(\Sigma^0\) and \(\Omega\).

Let \([\phi_1, \alpha_1, \eta_1] \in \Sigma^0\) and pick a representative \((\phi_1, \alpha_1, \eta_1)\) of this isomorphism class.

By [Tat66] we know that \(\text{End}(T_\ell E_0) = \mathcal{O}_\ell := \mathcal{O} \otimes \mathbb{Z}_\ell\). Choose a \(\mathbb{Z}_\ell\)-linear isomorphism \(k_{\ell,1} : T_\ell E_0 \xrightarrow{\sim} T_\ell E_1\) whose restriction gives a commutative diagram

\[
\begin{array}{ccc}
E_0[\ell^n] & \xrightarrow{k_{\ell,1}} & E_1[\ell^n] \\
\alpha_0 \downarrow \sim & & \alpha_1 \downarrow \sim \\
(\mathbb{Z}/\ell^n\mathbb{Z})^2 & \sim & (\mathbb{Z}/\ell^n\mathbb{Z})^2.
\end{array}
\]

Set \(x_\ell := k_{\ell,1}^{-1} \circ T_\ell \phi_1\), then \(x_\ell \in \text{End}(T_\ell E_0) = \mathcal{O}_\ell\). Note that \(x_\ell\) is not necessarily invertible in \(\mathcal{O}_\ell\) but it is nonzero, so \(x_\ell \in B_\mathbb{E}\). If \(\ell \nmid N \cdot \deg \phi_1\) then \(T_\ell \phi_1\) is actually an isomorphism extending \(\alpha_1^{-1} \circ \alpha_0\), so we can take \(x_\ell = 1\) in this case.

How does this depend on the choice of \(k_{\ell,1}\)? Let \(k_{\ell,1} : T_\ell E_0 \to T_\ell E_1\) be an isomorphism extending \(\alpha_1^{-1} \circ \alpha_0 : E_0[\ell^n] \to E_1[\ell^n]\). Let \(u = (k_{\ell,1})^{-1} \circ k_{\ell,1} \in \text{End}(T_\ell E_0)^{\times} = \mathcal{O}_\ell^\times\). Observe that \(u\) restricts to the identity on \(E_0[\ell^n] = (T_\ell E_0)/\ell^n(T_\ell E_0)\), so actually \(u \in \mathcal{O}_p^\times(N)\). Conversely, if \(u \in \mathcal{O}_\ell^\times(N)\), then \(k_{\ell,1} \circ u^{-1} : T_\ell E_0 \to T_\ell E_1\) is an isomorphism extending \(\alpha_1^{-1} \circ \alpha_0\). Therefore an isogeny \(\phi_1 : E_0 \to E_1\) defines for each prime \(\ell \neq p\) an element \([x_\ell] \in \mathcal{O}_\ell^\times(N)\bs B_\mathbb{E}\). Moreover, \([x_\ell]\) = 1 for all but finitely many \(\ell\).

We need to carry out the same program at the prime \(p\). The isogeny \(\phi_1 : E_0 \to E_1\) induces an injective \(\mathcal{W}\)-linear map \(M(\phi_1') : M_1 \to M_0\) (note the contravariance!), whose cokernel is isomorphic to \((\ker \phi_1')_p\). By Corollary 2.12 there exists an isomorphism of Dieudonné modules \(k_{p,1} : M_1 \xrightarrow{\sim} M_0\) such that the induced isomorphism \(M_1/FM_1 \to M_0/FM_0\) maps \(\eta_1\) to \(\eta_0\); by Corollary 2.11 \(k_{p,1}\) is
well-defined up to multiplication by $\mathcal{O}_p(1)$. Set $x_p := M(\phi_1) \circ k_{p,1}^{-1} \in \text{End}(M_0) = \mathcal{O}_p$, then we get $[x_p] \in \mathcal{O}_p^\times(1) \backslash B_p^\times$:

$$
\begin{array}{ccc}
M_1 & \xrightarrow{M(\phi_1)} & M_0 \\
\downarrow{\sim} & & \downarrow{x_p} \\
M_0 & & M_0.
\end{array}
$$

So far, our construction associates to a triple $(\phi_1, \alpha_1, \eta_1)$ an element $[x] \in U(1,N) \backslash \mathbb{A}_B^X$. This depends on the choice of isogeny $E_0 \to E_1$:

**Lemma 2.16.** Any isogeny $\tilde{\phi}_1 : E_0 \to E_1$ is of the form $\tilde{\phi}_1 = \phi_1 \circ u$, where

$$
u \in (\text{End}(E_0) \otimes \mathbb{Q})^\times = B^X.
$$

**Proof.** We treat $\phi_1, \tilde{\phi}_1$ as quasi-isogenies, i.e. elements of $\text{Hom}(E_0, E_1) \otimes \mathbb{Q}$. Let $n = \text{deg} \phi_1$, then we have that as quasi-isogenies:

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

We can therefore write $\phi_1^{-1} = \tilde{\phi}_1 \otimes \frac{1}{n}$ and we’ve shown that any isogeny has an inverse quasi-isogeny – actually a trivial modification of the argument shows that any quasi-isogeny is invertible. Now all we need to do is to set

$$
u = \phi_1^{-1} \circ \tilde{\phi}_1 \in (\text{End}(E_0) \otimes \mathbb{Q})^\times = B^X.
$$

Therefore we cannot hope to get anything better than a map $\Sigma^0 \to U \backslash \mathbb{A}_B^X / B^X$. We now show that this map is well-defined, i.e. that it only depends on the isomorphism class $[\phi_1, \alpha_1, \eta_1]$. Let $f : E_1 \to E_2$ be an isomorphism such that the diagrams (1) commute. By Lemma 2.16 it does not matter which isogeny $\phi_2 : E_0 \to E_2$ we work with, so we might as well take $\phi_2 = f \circ \phi_1$. We get the following diagrams

$$
\begin{array}{ccc}
t_\ell f & & t_\ell E_0 \\
\downarrow{\sim} & \uparrow{\sim} & \downarrow{\sim} \\
t_\ell E_1 & \xrightarrow{t_\ell f} & t_\ell E_0 \\
\end{array}
$$

where $k_{\ell,2} := t_\ell f \circ k_{\ell,1}$. It is now clear that we end up with the same $x_\ell \in \mathcal{O}_\ell^\times(N) \backslash B_\ell^X$ as the one obtained from $E_1$. The exact same thing happens at the prime $p$.

We obtain a map

$$
\gamma : \Sigma^0 \to \Omega.
$$

We need to construct an inverse. Let $[x] \in \Omega$ and choose a representative $x = (x_\ell) \in \mathbb{A}_B^X$. Let $\ell \neq p$. We have $x_\ell \in B_\ell^X = \text{End}(V_\ell E_0)^\times$, i.e. $x_\ell : V_\ell E_0 \to V_\ell E_0$ is a linear isomorphism. But $V_\ell E_0 = T_\ell E_0 \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ and $\mathbb{Q}_\ell = \mathbb{Z}_\ell[\frac{1}{\ell}]$. Choose an isomorphism $T_\ell E_0 \cong \mathbb{Z}_\ell^2$ extending $\alpha_0 : E_0[\ell^n] \to (\mathbb{Z}/\ell^n\mathbb{Z})^2$. This gives us a matrix $A_\ell \in \text{GL}_2(\mathbb{Q}_\ell)$ which represents $x_\ell$. Let $n_\ell \in \mathbb{Z}$ be the smallest integer such that $\ell^{n_\ell} A_\ell$ has coefficients in $\mathbb{Z}_\ell$. Via our isomorphism this corresponds to an endomorphism $y_\ell \in \text{End}(T_\ell E_0)$ which is injective with finite cokernel $C_\ell$. Let $\ell^k$ be the order of $C_\ell$. Let $K_\ell$ be the kernel of the map induced by $y_\ell$ on $E_0[\ell^k]$:

$$
0 \to K_\ell \to E_0[\ell^k] \xrightarrow{y_\ell} E_0[\ell^k] \to C_\ell \to 0.
$$
For \( \ell = p \) we have \( x_p \in B^*_p = (\text{End}(M_0) \otimes \mathbb{Q}^p)^A \). Write \( x_p = a + \pi b \), where \( a, b \in L_p \) and \( \pi^2 = -p \). We have

\[
a = \sum_i a_i \otimes \frac{1}{p^i},
\]

\[
b = \sum_j b_j \otimes \frac{1}{p^j},
\]

with \( a_i, b_j \in \text{End}(M_0) \). 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 \( y_p = a' + \pi b' \in \text{End}(M_0) \). This \( y_p \) is an endomorphism of the Dieudonné module \( M_0 \) which induces an automorphism of \( M_0 \otimes \mathbb{Q}_p \), 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

\[
M(E_0[p^k]) \to M(E_0[p^k]) \to C_p \to 0.
\]

Then \( C_p \) is the Dieudonné module of a subgroup scheme \( K_p \) of \( E_0 \) of rank \( p^k \).

Since \( x \in \mathbb{A}^n \), \( n_\ell = 0 \) for all but finitely many \( \ell \). Therefore it makes sense to set \( q := \prod \ell^{n_\ell} \in \mathbb{Q}^\times \) and \( y := x_q \); the \( \ell \)-th component of \( y \) is precisely the \( y_\ell \) above, and clearly \( [x] = [y] \). Now set \( K := \bigoplus K_\ell \), then \( K \) is a finite subgroup of \( E_0 \). So to the given \( (x_\ell) \in \mathbb{A}^n \) we can associate the quotient isogeny \( \phi : E_0 \to E_0/K \). For \( \ell \neq p \), our construction gives for any positive integer \( m \)

\[
\begin{array}{ccccccccc}
0 & \to & \ker & \to & E_0[\ell^m] & \to & (E_0/K)[\ell^m] & \to & 0 \\
& & \parallel & & \parallel & & \parallel & & \\
0 & \to & \ker & \to & E_0[\ell^m] & \to & E_0[\ell^m] & \to & 0
\end{array}
\]

Due to the structure of \( \ell^m \)-torsion, it is not hard to see that one can construct an isomorphism (actually, there exist many of them) \( E_0[\ell^m] \cong (E_0/K)[\ell^m] \) which makes the above diagram commute. On the level of Tate modules, we get

\[
\begin{array}{ccccccccc}
0 & \to & T_\ell E_0 & \to & T_\ell(E_0/K) & \to & 0 \\
& & \parallel & & \parallel & & \\
0 & \to & T_\ell E_0 & \to & y\ell E_0 & \to & T_\ell E_0
\end{array}
\]

In particular, we can set \( \alpha := \alpha_0 \circ k_\ell^{-1} \), then the isomorphisms \( \alpha : (E_0/K)[\ell^m] \cong (\mathbb{Z}/\ell^m\mathbb{Z})^2 \) for \( \ell | N \) piece together to give a level \( N \) structure on \( E_0/K \).

Let \( M := M((E_0/K)[p^\infty]) \). For \( \ell = p \) we have similarly

\[
\begin{array}{ccccccccc}
0 & \to & M & \to & M_0 & \to & \text{coker } M(\phi) & \to & 0 \\
& & \parallel & & \parallel & & \parallel & & \\
0 & \to & M_0 & \to & M_0 & \to & C_p & \to & 0
\end{array}
\]

and \( \eta := k_p^{-1}(\eta_0) \in M/FM \) gives a nonzero invariant differential on \( E_0/K \).

The next result tells us that we have indeed constructed a map

\[
\delta : \Omega \to \Sigma^0.
\]

**Proposition 2.17.** \( \delta \) is well-defined.
Proof. First suppose that $\bar{x} = xu$, where $u \in \text{End}(E_0)$ is not divisible by any rational prime. Let $\ell \neq p$, then $\bar{x}_\ell = x_\ell u$, so $\bar{y}_\ell = y_\ell u$:

\[
\begin{array}{cccccc}
0 & \rightarrow & T_\ell E_0 & \overset{g_\ell}{\rightarrow} & T_\ell E_0 & \rightarrow & C_\ell & \rightarrow & 0 \\
& & \downarrow{u} & & \downarrow{v_\ell} & & \downarrow{v_\ell} & & \\
0 & \rightarrow & T_\ell E_0 & \overset{g_\ell}{\rightarrow} & T_\ell E_0 & \rightarrow & \tilde{C}_\ell & \rightarrow & 0.
\end{array}
\]

The snake lemma gives

$$\text{coker } v_\ell = 0, \quad \ker v_\ell \cong \text{coker } u.$$  

Let $\ell^k$ be the order of $\tilde{C}_\ell$, then we can restrict the above diagram to the $\ell^k$-torsion and get

\[
\begin{array}{cccccc}
0 & \rightarrow & K_\ell & \overset{g_\ell}{\rightarrow} & E_0[\ell^k] & \overset{y_\ell}{\rightarrow} & E_0[\ell^k] & \rightarrow & C_\ell & \rightarrow & 0 \\
& & \downarrow{u_\ell} & & \downarrow{v_\ell} & & \downarrow{v_\ell} & & \\
0 & \rightarrow & K_\ell & \overset{g_\ell}{\rightarrow} & E_0[\ell^k] & \overset{y_\ell}{\rightarrow} & E_0[\ell^k] & \rightarrow & \tilde{C}_\ell & \rightarrow & 0,
\end{array}
\]

where $u_\ell$ is the restriction of $u$ to $E_0[\ell^k]$ and $g_\ell$ is the restriction of $u$ to $K_\ell$. Note that $\text{coker}(u_\ell : T_\ell E_0 \rightarrow T_\ell E_0) = \text{coker}(u : E_0[\ell^k] \rightarrow E_0[\ell^k])$. Since there’s no snake lemma for diagrams of long exact sequences, we split the above diagram in two:

\[
\begin{array}{cccccc}
0 & \rightarrow & K_\ell & \overset{g_\ell}{\rightarrow} & E_0[\ell^k] & \overset{y_\ell}{\rightarrow} & E_0[\ell^k]/\ker y_\ell & \rightarrow & 0 \\
& & \downarrow{u_\ell} & & \downarrow{h_\ell} & & \downarrow{h_\ell} & & \downarrow{v_\ell} \\
0 & \rightarrow & K_\ell & \overset{g_\ell}{\rightarrow} & E_0[\ell^k] & \overset{y_\ell}{\rightarrow} & E_0[\ell^k]/\ker \bar{y}_\ell & \rightarrow & 0 \\
& & \downarrow{h_\ell} & & \downarrow{h_\ell} & & \downarrow{h_\ell} & & \downarrow{v_\ell} \\
0 & \rightarrow & \text{Im } y_\ell & \overset{C_\ell}{\rightarrow} & E_0[\ell^k] & \overset{C_\ell}{\rightarrow} & C_\ell & \rightarrow & 0
\end{array}
\]

where I have taken the liberty of using the same label $h_\ell$ for two maps which are canonically isomorphic. We first apply the snake lemma to the diagram on the right and get

$$\ker h_\ell = 0, \quad \text{coker } h_\ell \cong \text{ker } v_\ell.$$  

Using this information together with the snake lemma in the diagram on the left gives

$$\ker g_\ell \cong \ker u_\ell, \quad 0 \rightarrow \text{coker } g_\ell \rightarrow \text{coker } u_\ell \rightarrow \text{coker } h_\ell \rightarrow 0.$$  

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

Let $g = \bigoplus g_\ell : \bar{K} \rightarrow K$ and let $f : E_0/\bar{K} \rightarrow E_0/K$ be defined by the diagram

\[
\begin{array}{cccccc}
0 & \rightarrow & K & \overset{\phi}{\rightarrow} & E_0 & \overset{\phi}{\rightarrow} & E_0/K & \rightarrow & 0 \\
& & \downarrow{g} & & \downarrow{u} & & \downarrow{f} & & \\
0 & \rightarrow & K & \overset{\phi}{\rightarrow} & E_0 & \overset{\phi}{\rightarrow} & E_0/\bar{K} & \rightarrow & 0.
\end{array}
\]

We apply the snake lemma and get an exact sequence

$$0 \rightarrow \ker g \rightarrow \ker u \rightarrow \ker f \rightarrow \text{coker } g = 0 \rightarrow \text{coker } u = 0 \rightarrow \text{coker } f = 0.$$  

But the map $\ker g \rightarrow \ker u$ is the sum of the isomorphisms $\ker g_\ell \cong \ker u_\ell$, so $\ker u \rightarrow \ker f$ is the zero map; therefore $\ker f = 0$. Clearly $\text{coker } f = 0$, so $f$ is an isomorphism.
We check that this isomorphism preserves level $N$ structures. We have a diagram

\[
\begin{array}{c}
\begin{tikzcd}
T_k E_0 & T_k(E_0/K) \\
T_{\ell u} T_k E_0 & T_{\ell f} E_0 \\
T_k E_0 & T_k(E_0/K)
\end{tikzcd}
\end{array}
\]

where we know that the outer square commutes, and that the triangles situated over, to the left, and under the central $T_k E_0$ commute. Therefore the triangle to the right of the central $T_k E_0$ also commutes, i.e. $k_\ell = T_k f \circ k_\ell$. The level $N$ structures on $E_0/K$ and $E_0/K$ are defined in such a way that the inner squares in the following diagram commute:

\[
\begin{array}{c}
\begin{tikzcd}
(E_0/K)[\ell^n] & (E_0/K)[\ell^n] \\
E_0 & (E_0/K)[\ell^n]
\end{tikzcd}
\end{array}
\]

\[
\begin{array}{c}
\begin{tikzcd}
E_0 & (E_0/K)[\ell^n] \\
\ell & \ell
\end{tikzcd}
\end{array}
\]

\[
\begin{array}{c}
\begin{tikzcd}
(\mathbb{Z}/\ell^n\mathbb{Z})^2 & (\mathbb{Z}/\ell^n\mathbb{Z})^2 \\
\theta & \theta
\end{tikzcd}
\end{array}
\]

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 $\tilde{x} = x\ell$, $\ell \neq p$ (the case $\ell = p$ is analogous, even easier). If $\ell' \not\mid \ell p$, then $\tilde{x} = x\ell'$ and $\tilde{y}_\ell = y_\ell \ell$. Multiplication by $\ell$ is an isomorphism of $T_\ell E_0$, so it induces an isomorphism $\bar{K}_{\ell'} \cong K_{\ell'}$ by applying the same argument as before on the diagram:

\[
\begin{array}{c}
\begin{tikzcd}
0 & K_{\ell'} & E_0[\ell^k] & E_0[\ell^k] & C_{\ell'} & 0 \\
& y_{\ell'} & E_0[\ell^k] & E_0[\ell^k] & C_{\ell'} & 0
\end{tikzcd}
\end{array}
\]

Something similar occurs at $p$. If $\ell' = \ell$, we get $\tilde{x}_\ell = x_\ell \ell$ and $\tilde{y}_\ell = y_\ell \ell$ so $\bar{K}_{\ell} = K_{\ell}$. We have an isomorphism $\bar{K} \cong K$ so $E_0/K \cong E_0/K$. We need to check that this isomorphism is compatible with the level structures and the differentials. Let $\ell' \not\mid \ell p$, then we have a diagram

\[
\begin{array}{c}
\begin{tikzcd}
\begin{tikzcd}
T_{\ell'}(E_0/K) & T_{\ell'} E_0 & T_{\ell'}(E_0/K) \\
& k_{\ell'} & k_{\ell'}
\end{tikzcd}
\end{array}
\end{array}
\]

\[
\begin{array}{c}
\begin{tikzcd}
(\mathbb{Z}/\ell^n\mathbb{Z})^2 & (\mathbb{Z}/\ell^n\mathbb{Z})^2 & (\mathbb{Z}/\ell^n\mathbb{Z})^2
\end{tikzcd}
\end{array}
\]

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 $K_{\ell} = K_{\ell}$ 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. $C_{\ell}$ (therefore $K_{\ell}$) depends on the chosen isomorphism $T_{\ell} E_0 \cong \mathbb{Z}_2^2$, and this can change $y_\ell$ by multiplication by an element of $O_\ell^\times(N)$. Suppose we have
another such candidate $\tilde{y}_\ell = u_\ell y_\ell$, then we would get a commutative diagram

\[
\begin{array}{ccccccc}
0 & \longrightarrow & T_\ell E_0 & \xrightarrow{y_\ell} & T_\ell E_0 & \longrightarrow & C_\ell & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow u_\ell & & \downarrow v_\ell & & \sim & & \sim \\
0 & \longrightarrow & T_\ell E_0 & \xrightarrow{\tilde{y}_\ell} & T_\ell E_0 & \longrightarrow & C_\ell & \longrightarrow & 0, \\
\end{array}
\]

from which we conclude as before that $K_\ell \cong K_\ell$ and $E_0/K \cong E_0/K$. For the level $N$ structure, we have the diagram

\[
\begin{array}{ccc}
(E_0/K)[\ell^n] & \xrightarrow{k_\ell^{-1}} & E_0[\ell^n] & \xrightarrow{\alpha_0} & (\mathbb{Z}/\ell^n\mathbb{Z})^2 \\
\downarrow \sim & & \downarrow & & \downarrow \\
(E_0/K)[\ell^n] & \xrightarrow{(k_\ell)^{-1}} & E_0[\ell^n] & \xrightarrow{\tilde{\alpha}_0} & (\mathbb{Z}/\ell^n\mathbb{Z})^2
\end{array}
\]

and a similar argument holds for the $\eta$ and $\tilde{\eta}$.

\begin{proof}
Suppose we started with $[x] \in \Omega$ and got $[\phi : E_0 \rightarrow E_0/K, \alpha, \eta]$. For $\ell \neq p$ we get the exact sequence (of $\mathbb{Z}_\ell$-modules)

\[0 \rightarrow T_\ell E_0 \xrightarrow{T_\ell \phi} T_\ell(E_0/K) \rightarrow \text{coker } T_\ell \phi \rightarrow 0.\]

We see from diagram (2.4) that $y_\ell = k_\ell^{-1} \circ T_\ell \phi$, where $k_\ell$ is an isomorphism that restricts to $\alpha^{-1} \circ \alpha_0$. Therefore $[y_\ell]$ is exactly the local element that’s 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 $(\phi : E_0 \rightarrow E, \alpha, \eta)$. We get local elements $x_\ell$ forming an adèles $x$. We have $\ker \phi = \prod_\ell \text{coker } x_\ell$. Now when we apply $\delta$ we already have $x_\ell \in \mathcal{O}_\ell$ so $y_\ell = x_\ell$ and $K = \prod_\ell \text{coker } x_\ell = \ker \phi$. We get an isogeny $E_0 \rightarrow E_0/K$ which has the same kernel as $\phi$, therefore $E = E_0/K$. It is clear from the construction of $\delta$ that the level $N$ structure and the invariant differential will stay the same.

We have just proved

**Theorem 2.19.** There is a canonical bijection $\Sigma^0 \rightarrow \Omega$.

Before moving on we record the following consequence of our arguments.

**Corollary 2.20.** Every class $[\phi, \alpha, \eta] \in \Sigma^0$ has a representative satisfying $p \nmid \deg \phi$.

**Proof.** Let $[x] = \gamma([\phi, \alpha, \eta])$. Let $\tilde{x}$ be a representative of $[x]$. Let $B = \{L, \pi\}$ be a description of our quaternion algebra, then $\pi$ is a uniformizer of $B_p$. Therefore $\tilde{x}_p = u\pi^k$, with $k \in \mathbb{Z}$, $u \in \mathcal{O}_p^\times$. But then $\tilde{x}_p\pi^{-k} \in \mathcal{O}_p^\times$. Since $\pi \in \mathcal{O}_p^\times(1)$, we can use the representative $x = \tilde{x}\pi^{-k}$ for computing $\delta$, in which case $C_p = 1$ so the degree of the resulting isogeny is prime to $p$.

**Remark 2.21.** We note here that one can say more: the isogeny $\phi : E_0 \rightarrow E$ can be chosen to have square-free degree. This is not easy to show.

2.5. **Compatibilities.** It remains to prove the following result:

**Theorem 2.22.** The canonical bijection $\gamma : \Sigma^0(N) \rightarrow \Omega(N)$ is compatible with the action of the Hecke algebra, with the action of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$, and with the operation of raising the level.
5.1. Hecke action. In this section \( \ell \) will denote a fixed prime not dividing \( pN \). For generalities on Hecke algebras, see §3.1.2 in [AZ95].

If \( H_1, H_2 \) are subgroups of a group \( G \), we say that \( H_1 \) is commensurable with \( H_2 \) (write \( H_1 \sim H_2 \)) if \( H_1 \cap H_2 \) has finite index in both \( H_1 \) and \( H_2 \). If \( H \) is a subgroup of \( G \), we define its commensurator by

\[
\text{Comm}(H) := \{ g \in G : g^{-1} H g \sim H \}.
\]

Finally, we say that \((G,H)\) is a Hecke pair if \( \text{Comm}(H) = G \). For example, one can find in §3.2.1 of [AZ95] a proof of the fact that \((\text{GL}_2(\mathbb{Q}_\ell), \text{GL}_2(\mathbb{Z}_\ell))\) is a Hecke pair.

If \((G,H)\) is a Hecke pair then any double coset \( HgH \) has a finite decomposition into left cosets. Since the map \( H \backslash G \to G/H \) given by \( gH \mapsto Hg^{-1} \) is a bijection, we also know that \( HgH \) has a finite decomposition into the same number of right cosets, i.e. we can write

\[
HgH = \bigcup_{j=1}^{s} x_j g H = \bigcup_{j=1}^{s} H g y_j,
\]

where \( x_j, y_j \in H \) for all \( j \).

The Hecke algebra of the Hecke pair \((G,H)\) is by definition \( \mathcal{H}(G,H) := \mathbb{Z}[H \backslash G / H] \), with the multiplication described above. From now on we set \( G = \text{GL}_2(\mathbb{Q}_\ell), H = \text{GL}_2(\mathbb{Z}_\ell) \) and \( \mathcal{H}_\ell = \mathcal{H}(\text{GL}_2(\mathbb{Q}_\ell), \text{GL}_2(\mathbb{Z}_\ell)) \). We call \( \mathcal{H}_\ell \) the local Hecke algebra at \( \ell \).

Take an isogeny \( \phi : E_1 \to E_2 \) whose degree is a power of \( \ell \). It induces an injective \( \mathbb{Z}_\ell \)-linear map \( T_{\ell \phi} : T_{\ell E_1} \to T_{\ell E_2} \) which gives an element \( g \in G = \text{GL}_2(\mathbb{Q}_\ell) \). Since \( g \) is defined only up to changes of bases for \( T_{\ell E_1} \) and \( T_{\ell E_2} \), \( \phi \) actually defines a double coset \( HgH \), where \( H = \text{GL}_2(\mathbb{Z}_\ell) \). In this situation we say that \( \phi \) is of type \( HgH \). We say that a finite subgroup \( C \) of an elliptic curve \( E \) is of type \( HgH \) if the quotient isogeny \( E \to E/C \) is of type \( HgH \).

If \( HgH \in \mathcal{H}_\ell \), we denote by \( \det(HgH) \) the \( \ell \)-part of the determinant of any representative of \( HgH \). The action of \( \mathcal{H}_\ell \) on \( \Sigma^0 \) is defined as follows. If \( \det(HgH) > 1 \), set

\[
T_{HgH}(\phi : E_0 \to E, \alpha, \eta) := \sum_{C \subset E \text{ of type } HgH} [E_0 \xrightarrow{\phi} E \xrightarrow{\psi_C} E/C, \alpha_C, \eta_C],
\]

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

\[
\begin{array}{c}
E[N] \xrightarrow{\psi_C} (E/C)[N] \\
\alpha \downarrow \quad \alpha_C \downarrow \\
(\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\eta} (\mathbb{Z}/N\mathbb{Z})^2.
\end{array}
\]

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

Now suppose \( \det(HgH) < 1 \). Given a finite subgroup \( C \) of \( E \) of type \( Hg^{-1}H \), let \( \hat{\psi}_C : (E/C) \to E \) be the dual isogeny to the quotient \( \psi_C : E \to E/C \). The action is defined by

\[
T_{HgH}(\phi : E_0 \to E, \alpha, \eta) := \sum_{C \subset E \text{ of type } Hg^{-1}H} [E_0 \xrightarrow{\phi} E \xleftarrow{\hat{\psi}_C} E/C, \alpha_C, \eta_C],
\]

where \( \eta_C = M(\psi_C')(\eta) \), and \( \alpha_C \) is defined by the diagram

\[
\begin{array}{c}
E[N] \xrightarrow{\hat{\psi}_C} (E/C)[N] \\
\alpha \downarrow \quad \alpha_C \downarrow \\
(\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\eta} (\mathbb{Z}/N\mathbb{Z})^2.
\end{array}
\]
The algebra $\mathcal{H}_\ell$ acts on $H \backslash G$ as follows: let $HgH = \bigcap_i Hg_i$, let $Hx \in H \backslash G$ and choose a representative $x \in Hx$. Then there exist representatives $g_i \in Hg_i$ such that

$$T_{HgH}(Hx) = \sum Hg_i x.$$ 

The algebra $\mathcal{H}_\ell$ acts on $\Omega$ by acting on the component $Hz \ell$ of $[x] \in \Omega$.

**Lemma 2.23.** The bijection $\gamma : \Sigma^0 \to \Omega$ is compatible with the action of the local Hecke algebra $\mathcal{H}_\ell$, i.e. for all $HgH \in \mathcal{H}_\ell$ and $[\phi, \alpha, \eta]$ we have

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

**Proof.** Let $HgH \in \mathcal{H}_\ell$, let $[\phi : E_0 \to E, \alpha, \eta] \in \Sigma^0$ and let $[x] = \gamma([\phi, \alpha, \eta])$.

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

$$T_{\ell'}E_0 \xrightarrow{T_{\ell'}\phi} T_{\ell'}E \xrightarrow{T_{\ell'}\psi_C} T_{\ell'}(E/C).$$

Since $(T_{\ell'}\psi_C) \circ k_{\ell'} : T_{\ell'}E_0 \to T_{\ell'}(E/C)$ is an isomorphism restricting to $\alpha_C^{-1} \circ \alpha_0$ (see diagram (2)), we get that $[x_{C,\ell'}] = [x_{\ell'}]$.

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

$$M_C \xrightarrow{M(\psi_C)} M \xrightarrow{M(\phi')} M_0 \xrightarrow{k_p} M_0.$$ 

Let’s figure out what happens at $\ell$. Fix $x_\ell \in Hx_\ell$, then the isomorphism $k_\ell : T_\ell E_0 \to T_\ell E$ is fixed and allows us to identify these two $\mathbb{Z}_\ell$-modules. Choose a $\mathbb{Z}_\ell$-linear isomorphism $k_C : T_\ell E \to T_\ell(E/C)$ and set $y_C = k_C^{-1} \circ T_\ell \psi_C$. Via the identification $k_\ell$, $y_C$ induces a map $z_C : T_\ell E_0 \to T_\ell E_0$. We have a diagram

$$T_\ell E_0 \xrightarrow{T_\ell \phi} T_\ell E \xrightarrow{T_\ell \psi_C} T_\ell(E/C).$$

Since $k_C \circ k_\ell$ is an isomorphism $T_\ell E_0 \to T_\ell(E/C)$ 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 $E$ of type $HgH$ and the set of right cosets $H_C$ contained in $HgH$. We start by constructing an inverse map. Let $Hz \subset HgH$ and pick a representative $z$. This corresponds to a map $z : T_\ell E_0 \to T_\ell E_0$, and hence induces via $k_\ell$ a map $y : T_\ell E \to T_\ell E$. We use the same construction as in the definition of the map $\delta$ in §2.4 (pages 17 and following) to get a subgroup $C$ of $E$ which is canonically isomorphic to the cokernel of $y$. $C$ 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 2.18.
24 It remains to deal with the case \( \det(HgH) \neq 1 \). 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 \( C \to Hz_C \) in this setting. Let \( C \) be a subgroup of \( E \) of type \( Hg^{-1}H \). This defines a new element of \( \Sigma^0 \) which we denote by \( \psi^{-1}_C \circ \phi, \alpha_C, \eta_C \) (by a slight abuse of notation since \( \psi_C \) is not invertible as an isogeny). Let \( \gamma(x_C) := \gamma(\psi^{-1}_C \circ \phi, \alpha_C, \eta_C) \). If \( (\ell', p\ell) = 1 \), we have a diagram:

\[
\begin{array}{c}
T_{\ell'} E_0 \xrightarrow{T_{\ell'} \phi} T_{\ell'} E \xleftarrow{T_{\ell'} \psi_C} T_{\ell'} (E/C).
\end{array}
\]

Since \( (T_{\ell'} \psi_C)^{-1} \circ k_{\ell'} : T_{\ell'} E_0 \to T_{\ell'} (E/C) \) is an isomorphism restricting to \( \alpha_C^{-1} \circ \alpha_0 \) (see diagram (3)), we get that \( [x_{C,\ell'}] = [x_{C}] \). The situation at \( p \) is similar and we have \([x_{C,p}] = [x_{p}]\).

What about \( \ell \)? As before, we fix \( x_\ell \in Hx_\ell \) and with it the isomorphism \( k_{\ell} : T_{\ell} E_0 \to T_{\ell} E \). Choose an isomorphism \( k_C : T_{\ell} E \to T_{\ell} (E/C) \) and set \( y_C := T_{\ell} \psi_C \circ k_C \). Via the identification \( k_{\ell} \), \( y_C \) induces a map \( z_C : T_{\ell} E_0 \to T_{\ell} E_0 \). We have a diagram:

\[
\begin{array}{c}
T_{\ell} E_0 \xrightarrow{T_{\ell} \phi} T_{\ell} E \xleftarrow{T_{\ell} \psi_C} T_{\ell} (E/C).
\end{array}
\]

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 \( \det(HgH) > 1 \). \( \square \)

2.5.2. Action of \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \). Within this section we’ll write \( G \) to denote \( \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \). The group \( G \) acts on \( \Sigma^0 \) as follows:

\[
g \cdot [\phi, \alpha, \eta] := [\phi, g \circ \alpha, \eta].
\]

The action on \( \Omega \) is more delicate. It is easy to see that since \( \mathcal{O}_\ell = \text{End}(T_{\ell} E_0) \), we have \( \mathcal{O}_\ell^\times \mathcal{O}_\ell \mathcal{O}_\ell = \text{Aut}(E_0[\ell^n]) \), where \( \ell^n \parallel N \). Our fixed isomorphism \( \alpha_0 : E_0[N] \to (\mathbb{Z}/N\mathbb{Z})^2 \) identifies \( G \) with \( \text{Aut}(E_0[N]) \) via \( g \mapsto \alpha_0^{-1} \circ g \circ \alpha_0 \). Therefore we get an identification:

\[
G \sim \prod_{\ell} \mathcal{O}_\ell^\times \mathcal{O}_\ell \mathcal{O}_\ell \mathcal{O}_\ell,
\]

\[
g \mapsto \prod_{\ell} \mathcal{O}_\ell^\times \mathcal{O}_\ell (\alpha_0^{-1} \circ g \circ \alpha_0),
\]

where the product is finite since the terms with \( \ell \parallel N \) are 1. The action of \( G \) on \( \Omega \) is then given by

\[
g \cdot \left( \prod_{\ell} \mathcal{O}_\ell^\times (N) x_{\ell} \right) := \left( \prod_{\ell} \mathcal{O}_\ell^\times (N)(\alpha_0^{-1} \circ g \circ \alpha) x_{\ell} \right).
\]

Lemma 2.24. The bijection \( \gamma : \Sigma^0 \to \Omega \) is compatible with the action of \( G = \text{GL}_2(\mathbb{Z}/N\mathbb{Z}) \).
Proof. Let \( \prod O^\times_\ell(N)x_\ell := \gamma((\phi, \alpha, \eta)/\ell) \) and \( \prod [O^\times_\ell(N)/\ell]_\ell := \gamma(g \cdot [\phi, \alpha, \eta]) = \gamma([\phi, g \circ \alpha, \eta]). \) Pick some \( \ell \neq p \) and set \( H := O^\times_\ell(N); \) 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 \( k_\ell : T_\ell E_0 \rightarrow T_\ell E \) is some isomorphism extending \( \alpha^{-1} \circ \alpha_0. \) Therefore \( k_\ell' := k_\ell \circ (\alpha_0^{-1} \circ g \circ \alpha_0) \) is an isomorphism extending \( \alpha^{-1} \circ g \circ \alpha_0 \) and hence precisely what we need in order to define \( x_\ell' = (k_\ell')^{-1} \circ T_\ell \phi. \) By the definition of \( k_\ell' \) 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. \( \square \)

2.5.3. Raising the level. Suppose \( N' = dN \) for some positive integer \( d. \) A level \( N' \) structure \( \alpha' : E[N'] \rightarrow (\mathbb{Z}/N'\mathbb{Z})^2 \) on an elliptic curve \( E \) induces a level \( N \) structure on \( E \) in the following way. Multiplication by \( d \) on \( E[N'] \) gives a surjection \( d : E[N'] \rightarrow E[N], \) and there is a natural surjection \( \pi : (\mathbb{Z}/N'\mathbb{Z})^2 \rightarrow (\mathbb{Z}/N\mathbb{Z})^2 \) given by reduction mod \( N. \) We want to define an isomorphism \( \alpha : E[N] \rightarrow (\mathbb{Z}/N\mathbb{Z})^2 \) that completes the following square
\[
\begin{array}{ccc}
E[N'] & \overset{\alpha'}{\sim} & (\mathbb{Z}/N'\mathbb{Z})^2 \\
d \downarrow & & \downarrow \pi \\
E[N] & \overset{\alpha}{\sim} & (\mathbb{Z}/N\mathbb{Z})^2.
\end{array}
\]
This is straightforward: let \( P \in E[N] \) and take some preimage \( Q \) of it in \( E[N']. \) Set \( \alpha(P) := \pi(\alpha'(Q)). \) This is easily seen to be well-defined and a bijection. We conclude that \([\phi, \alpha', \eta] \rightarrow [\phi, \alpha, \eta] \) gives a map
\[
\Sigma^0(N') \rightarrow \Sigma^0(N).
\]
There is a similar map on the \( \Omega \)'s. We only need to consider primes \( \ell | N'. \) Here we have \( O^\times_\ell(N') \subset O^\times_\ell(N) \) so we get maps \( \Sigma^0(N') \backslash B_\ell \rightarrow \Sigma^0(N) \backslash B_\ell, \) which can be put together to form \( \Omega(N') \rightarrow \Omega(N). \)

We want to show that the bijection \( \gamma \) commutes with these maps. This is clear at primes \( \ell \nmid N', \) so suppose \( \ell \) is a prime divisor of \( N' \); say \( \ell^m | N \) and \( \ell^n || N. \) Let \([\phi, \alpha', \eta] \in \Sigma^0(N'), [x'] = \gamma([\phi, \alpha', \eta]) \) and \([x] = \gamma([\phi, \alpha, \eta]). \) By definition, \( x_\ell' = (k_\ell')^{-1} \circ \phi \) where \( k_\ell' : T_\ell E_0 \rightarrow T_\ell E \) is an isomorphism restricting to
\[
\begin{array}{ccc}
E_0[\ell^m] & \overset{k_\ell'}{\sim} & \Omega(\ell^m) \\
\alpha_0' \downarrow & & \alpha' \downarrow \\
(\mathbb{Z}/\ell^m\mathbb{Z})^2 & \overset{\sim}{\longrightarrow} & (\mathbb{Z}/\ell^n\mathbb{Z})^2.
\end{array}
\]
This defines the local component \( O^\times_\ell(N')x_\ell'. \) We can restrict \( k_\ell' \) even further to the \( \ell^m \)-torsion, and then by the definition of \( \alpha \) we have
\[
\begin{array}{ccc}
E_0[\ell^m] & \overset{k_\ell'}{\sim} & \Omega(\ell^m) \\
\alpha_0' \downarrow & & \alpha' \downarrow \\
(\mathbb{Z}/\ell^m\mathbb{Z})^2 & \overset{\sim}{\longrightarrow} & (\mathbb{Z}/\ell^n\mathbb{Z})^2.
\end{array}
\]
But this means that \( k_\ell' \) plays the role of \( k_\ell \) in the definition of \( x_\ell, \) so
\[
O^\times_\ell(N)x_\ell' = O^\times_\ell(N)x_\ell.
\]
This is precisely what the map \( \Omega(N') \rightarrow \Omega(N) \) looks like at \( \ell, \) so we're done.
Following a suggestion of Gross, we generalize the results of the previous section to dimension $g \geq 2$. More precisely, we link Siegel modular forms (mod $p$) to reductions modulo $p$ of modular forms on the algebraic group $\text{GU}_g(B)$, as defined in [Gro99].

Fix a prime $p$ and an integer $N > 1$ prime to $p$.

3.1. The geometric theory of Siegel modular forms. We review the basic definitions and results from [Cha86].

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

$$
A \xrightarrow{\pi} S,
$$

whose (geometric) fibers are connected of dimension $g$.

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

Let $\phi : A \to B$ be an isogeny of abelian schemes over $S$. Cartier duality (Theorem III.19.1 in [Oor75]) 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 $\lambda$ on $A$ induces a canonical non-degenerate skew-symmetric pairing

$$
A[N] \times A[N] \to \mu_N,
$$

which is also called the Weil pairing.

For our purposes, a level $N$ structure on $(A, \lambda)$ will be 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:

$$
\begin{array}{c}
A[N] \times A[N] \xrightarrow{(f,f)} (\mathbb{Z}/N\mathbb{Z})^{2g} \times (\mathbb{Z}/N\mathbb{Z})^{2g} \\
\downarrow \text{Weil} \quad \downarrow \text{std} \\
\mu_N \quad \sim \quad \mathbb{Z}/N\mathbb{Z}
\end{array}
$$

for some isomorphism $\mu_N \cong \mathbb{Z}/N\mathbb{Z}$.

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

$$
\begin{array}{ccc}
& Y & \\
\pi \downarrow & & 0 \\
\mathcal{A}_{g,N} & & \\
\end{array}
$$

be the corresponding universal abelian variety. Let $\mathcal{E} = 0^*(\Omega_Y/\mathcal{A}_{g,N})$; this is called the $Hodge$ $bundle$.

3.1.1. $Twisting$ $the$ $sheaf$ $of$ $differentials$. Let $X$ be a scheme and let $\mathcal{F}$ be a locally free $\mathcal{O}_X$-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 $\mathcal{F}$, then we have $\mathcal{F}|_{U_i} \cong (\mathcal{O}_X|_{U_i})^n$, and for all $i$ and $j$ we have isomorphisms $\mathcal{F}|_{U_i \cap U_j} \cong \mathcal{F}|_{U_j \cap U_i}$ given by $g_{ij} \in \text{GL}_n(\mathcal{O}_X|_{U_i \cap U_j})$ satisfying the usual cocycle identities.

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

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

The scheme $\mathcal{A}_{g,N}$ can be compactified in various ways (see [FC90]). Pick some compactification $\mathcal{A}_{g,N}^*$ and let $X$ denote its base-change to $\overline{\mathcal{F}}_p$. According to the Koecher principle, the Hodge bundle $\mathcal{E}$ extends uniquely to a locally free sheaf $\mathcal{E}$ on $X$.

Given a rational representation $\rho : \text{GL}_g \to \text{GL}_m$, the global sections of $\mathcal{E}_\rho$ are called $Siegel$ $modular$ $forms$ (mod $p$) of weight $\rho$ and level $N$ and they can be written

$$
M_\rho(N) = \Pi^0(X, \mathcal{E}_\rho) = \{ f : \{(A, \lambda, \alpha, \eta) \to \overline{\mathbb{F}}_p \mid f(A, \lambda, \alpha, M\eta) = \rho(M)^{-1}f(A, \lambda, \alpha, \eta), \forall M \in \text{GL}_g(\overline{\mathbb{F}}_p)\},
$$

where $\eta$ is a basis of invariant differentials on $A$.

3.1.2. $The$ $Kodaira$-$Spencer$ $isomorphism$. We recall the properties of the Kodaira-Spencer isomorphism. For a detailed account see §III.9 and §VI.4 in [FC90].

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

$$
\kappa : \mathcal{T}_S \to R^1 \pi_*(\mathcal{T}_A/S).
$$

If

$$
\begin{array}{ccc}
& A & \\
\pi \downarrow & & 0 \\
S & & \\
\end{array}
$$

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

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

The projection formula gives

$$
R^1 \pi_*(\pi^*(\mathcal{E}_{A/S})) = (R^1 \pi_*\mathcal{O}_A) \otimes_{\mathcal{O}_S} \mathcal{E}_{A/S}^\vee.
$$
Let $\pi^t : A^t \to S$ be the dual abelian scheme, then
$$R^1 \pi_* \mathcal{O}_A = 0^* (\mathcal{T}_{A^t/S}) = (E_{A^t/S})^\vee.$$ So the Kodaira-Spencer map can be written as follows:
$$\kappa : \mathcal{T}_S \to (E_{A^t/S})^\vee \otimes_{\mathcal{O}_S} E_{A^t/S}^\vee,$$
which after dualizing gives
$$\kappa^\vee : E_{A^t/S} \otimes_{\mathcal{O}_S} E_{A^t/S} \to \Omega^1_S.$$ Now suppose that $\lambda : A/S \to A^t/S$ is a principal polarization, i.e. an isomorphism. Then the pullback map $\lambda^* : E_{A^t/S} \to E_{A/S}$ is an isomorphism and we get a map
$$E_{A/S}^\otimes 2 \to \Omega^1_S.$$ This map factors through the projection map to $\text{Sym}^2(E_{A/S})$, and the resulting map
$$\text{Sym}^2(E_{A/S}) \to \Omega^1_S$$
is an isomorphism. In particular, in the notation of §3.1.1 we have a Hecke isomorphism $E_{\text{Sym}^2_{\text{std}}} \cong \Omega^1_X$, where $X = A^t_{g,N}$.

3.2. Superspecial abelian varieties. For a commutative group scheme $X$ over a field $K$ we define the $a$-number of $X$ by
$$a(X) = \dim_K \text{Hom}(\alpha_p, X).$$ If $K \subset L$ then $\dim_K \text{Hom}(\alpha_p, X) = \dim_L \text{Hom}(\alpha_p, X \otimes L)$ so $a(X)$ does not depend on the base field.

An abelian variety $A$ over $K$ of dimension $g \geq 2$ is said to be superspecial if $a(A) = g$. Let $k$ be an algebraic closure of $K$. By Theorem 2 of [Oor75], $a(A) = g$ if and only if
$$A \otimes k \cong E_1 \times \ldots \times E_g,$$where the $E_i$ are supersingular elliptic curves over $k$. On the other hand, for any $g \geq 2$ and any supersingular elliptic curves $E_1, \ldots, E_{2g}$ over $k$ we have (see Theorem 3.5 in [Shi79])
$$E_1 \times \ldots \times E_g \cong E_{g+1} \times \ldots \times E_{2g}.$$ 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.

**Lemma 3.1.** Let $A$ be a superspecial abelian variety over $\mathbb{F}_p$. 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 $\mathbb{F}_p$, then $A \cong E^g$. By Lemma 2.1 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
$$\pi_{A'} = \pi_{E'} \times \pi_{E'} \times \ldots \times \pi_{E'} = [-p]_{E'} \times \ldots \times [-p]_{E'} = [-p]_{A'}.$$ The functoriality statement follows from the corresponding statement in Lemma 2.1. Since any superspecial abelian variety over $\mathbb{F}_p$ is isomorphic to $E^g$, it suffices to consider a morphism $f : E^g \to E^g$. This is built of a bunch of morphisms $E \to E$, which by Lemma 2.1 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 $\mathbb{F}_p$. □
An easy consequence of the functoriality is that if \( A \) is a principal polarization on \( A \), there exists a principal polarization \( \lambda' \) of the canonical \( \mathbb{F}_p^2 \)-structure \( A' \) of \( A \) such that \( \lambda' \otimes \mathbb{F}_p^2 = \lambda \). We say that \((A', \lambda')\) is the canonical \( \mathbb{F}_p^2 \)-structure of \((A, \lambda)\).

3.2.1. Isogenies. We need to define what it means for two principally polarized abelian varieties \((A_1, \lambda_1)\) and \((A_2, \lambda_2)\) to be isogenous. The natural tendency is to consider isogenies \( \phi : A_1 \to A_2 \) such that the following diagram commutes:

\[
\begin{array}{ccc}
A_1 & \xrightarrow{\phi} & A_2 \\
\lambda_1 \downarrow & \sim & \lambda_2 \downarrow \\
A_1' & \xleftarrow{\phi'} & A_2',
\end{array}
\]

i.e.

\[\phi' \circ \lambda_2 \circ \phi = \lambda_1.\]

But then \( \deg \phi = 1 \) so the only isogenies that satisfy this condition are isomorphisms. We therefore relax the condition by requiring \( \phi \) to satisfy

\[\phi' \circ \lambda_2 \circ \phi = m\lambda_1,\]

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

We now consider the local data given by the presence of a principal polarization. Let \((A, \lambda)\) be a \( g \)-dimensional principally polarized abelian variety defined over \( \mathbb{F}_p \). Let \( \ell \) be a prime different from \( p \) and set as usual \( \mathbb{Z}_\ell(1) = \lim \mu_{\ell^n} \). We have the canonical Weil pairing (see \S 12 of [Mil98] or \S 16 of [Mil86])

\[e_\ell : T_\ell A \times T_\ell A' \to \mathbb{Z}_\ell(1),\]

which is a non-degenerate \( \mathbb{Z}_\ell \)-bilinear map. When combined with a homomorphism of the form \( \alpha : A \to A' \) 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 \( \alpha \) is a polarization then \( e_\ell^\alpha \) 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

\[e_\ell^{f \circ \alpha \circ f}(a, a') = e_\ell^\alpha(f(a), f(a'))\]

for all \( a, a' \in T_\ell A, \alpha : B \to B' \).

Let \( \phi : (A_1, \lambda_1) \to (A_2, \lambda_2) \) be an isogeny of principally polarized abelian varieties. \( \phi \) 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 \( \ell \)-primary part (ker \( \phi \)) of ker \( \phi \). Since \( \phi' \circ \lambda_2 \circ \phi = m\lambda_1 \), we have

\[e_\ell^{\lambda_2}((T_\ell \phi)a, (T_\ell \phi)a') = e_\ell^{\phi' \circ \lambda_2 \circ \phi}(a, a') = e_\ell^{m\lambda_1}(a, a') = e_\ell(a, m\lambda_1 a') = e_\ell(a, \alpha a')^m = e_\ell^{\lambda_1}(a, a')^m.\]

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

What happens at \( p \)? 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:
\[ e(Fx, y) = e(x, Vy)^p. \]

A principal polarization on $A$ defines a principal quasi-polarization $e_p$ on the Dieudonné module $M$ of $A$ (see Jeff Achter’s thesis [Ach98] for references). If $A$ is defined over $\mathbb{F}_{p^2}$ then $e_p$ defines a hermitian form on $M/FM$ as follows:
\[ M/FM \times M/FM \to \mathbb{F}_{p^2} \]
\[ (x, y) \mapsto \langle x, y \rangle := e_p(x, Fy)^p \pmod{p}. \]

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.

3.2.2. Quaternion hermitian forms. Let $B$ be a quaternion algebra over a field $F$. Let $\tau$ 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 quaternion hermitian form is diagonalizable (see §2.2 in [Shi63]):

Proposition 3.2. For every quaternion hermitian form $f(x, y)$ 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 $1 \leq i, j \leq n$, where $\alpha_i \in F$. Moreover if $f$ is non-degenerate and the norm $N : B \to F$ 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 (see §3.4 of [Vig80]):

Theorem 3.3 (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 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 $\infty$, then $n(B) = \mathbb{Q}_{>0}$.

3.2.3. 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
\[ U_g(B) = \{ M \in \text{GL}_g(B) : M^* M = I \}, \]
\[ GU_g(B) = \{ M \in \text{GL}_g(B) : M^* M = \gamma(M) I, \gamma(M) \in F^\times \}. \]

These are algebraic groups over $F$: let $(f_{ij}) = M^* M$, then $U_g(B)$ is defined by the equations $f_{ij} = 0$ $(i \neq j)$, $f_{ii} = 1$, and $GU_g(B)$ is defined by the equations
\[ f_{ij} = 0 \text{ for } i \neq j, \quad f_{11} = f_{22} = \ldots = f_{gg} \]
(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:

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

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

**Lemma 3.4.** Let $K$ be a field. The subgroups $\text{GU}_g(M_2(K))$ and $\text{GSp}_{2g}(K)$ are conjugate inside $\text{GL}_{2g}(K)$. In particular, they are isomorphic and the $F$-algebraic group $\text{GU}_g(B)$ is an $F$-form of $\text{GSp}_{2g}$.

**Proof.** If $A = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in M_2(K)$, then the conjugate of $A$ is

$$\tilde{A} = \left( \begin{array}{cc} d & -c \\ -b & a \end{array} \right),$$

therefore the adjoint of $A$ is

$$A^* = \left( \begin{array}{cc} d & -c \\ -b & a \end{array} \right) = J_{2g}^{-1}AJ_{2g}.$$

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

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

therefore

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

I claim that there exists a permutation matrix $P$ such that $P^t \tilde{J}_{2g} P = J_{2g}$. If $g$ is odd (resp. even), let $P_1$ be the matrix corresponding to the product of transpositions

$$(2(2g - 1))(4(2g - 3)) \ldots ((g - 1)g), \ (\text{resp.} \ (2(2g - 1))(4(2g - 3)) \ldots (g(g + 1))),$$

then

$$P_1^t \tilde{J}_{2g} P_1 = \left( \begin{array}{cccccc} 1 & 0 & & & & 0 \\ & 1 & & & & 0 \\ & & \ddots & & & \vdots \\ & & & 1 & & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{array} \right),$$

respectively

$$P_1^t \tilde{J}_{2g} P_1 = \left( \begin{array}{cccccc} 1 & 0 & & & & 0 \\ & 1 & & & & 0 \\ & & \ddots & & & \vdots \\ & & & 1 & & 0 \\ & & & & 1 & 0 \\ & & & & & 1 \end{array} \right).$$

In both cases it is clear what permutation matrix $P_2$ will finish the job; set $P = P_2 P_1$ and the claim is proved.

We have $J_{2g} = P^t \tilde{J}_{2g} P$, so $\tilde{J}_{2g} = PJ_{2g}P^t$ and

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

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

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

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

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

so $M \in \text{GU}_g(M_2(K))$. Therefore $P^{-1} \text{GU}_g(M_2(K)) P = \text{GSp}_{2g}(K)$, as desired.
3.2.4. Algebraic modular forms (mod p). We give the definition of algebraic modular forms (mod p) on the group $G = GU_g(B)$, where $B$ is the quaternion algebra over $\mathbb{Q}$ ramified at $p$ and $\infty$. See [Gro99] and [Gro98] for more details.

The definition given by Gross requires $G$ to be a reductive algebraic group over $\mathbb{Q}$ which satisfies 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 $O(4g)$.

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 $\pi$ of $\mathcal{O}_p$, i.e.

$$1 \to U_p \to G(\mathcal{O}_p) \xrightarrow{\text{mod } \pi} GU_g(\mathbb{F}_p^2) \to 1.$$ 

For $\ell \neq p$, we set

$$U_\ell(N) := \{x \in G(\mathbb{Z}_\ell) : x \equiv 1 \pmod{\ell^n}, \ell^n \mid N\}.$$

The product

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

is an open compact subgroup of $G(\hat{\mathbb{Q}})$, called the level (\hat{\mathbb{Q}} is the ring of finite ad` eles). Set $\Omega(N) := U \backslash G(\hat{\mathbb{Q}})/G(\mathbb{Q})$. By Proposition 4.3 in [Gro99], the double coset space $\Omega(N)$ is finite.

Now let $\rho : GU_g(\mathbb{F}_p^2) \to GL(W)$ 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 $\rho$ and level $U$ on $G$ as follows:

$$M(\rho, U) := \{f : \Omega(N) \to W : f(\lambda g) = \rho(\lambda)^{-1}f(g) \text{ for all } \lambda \in GU_g(\mathbb{F}_p^2)\}.$$ 

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

3.2.5. Differentials defined over $\mathbb{F}_p^2$. We know from Lemma 3.1 that a principally polarized superspecial abelian variety $(A, \lambda)$ has a canonical $\mathbb{F}_p^2$-structure $(A', \lambda')$. We are therefore lead to consider invariant differentials on $A$ defined over $\mathbb{F}_p^2$.

**Lemma 3.5.** 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 $M/\text{FM}$ over $\mathbb{F}_p^2$.

**Proof.** The invariant differentials on $A$ defined over $\mathbb{F}_p^2$ are identified with $\omega(A')$, the invariant differentials on $A'$. We have $\omega(A') \cong \omega(E'[p^\infty]) \cong \omega(E')^g$. By Lemma 2.15 we know that

$$\omega(E') \cong M(E'[p^\infty])/\text{FM}(E'[p^\infty]),$$

and since $M(A'[p^\infty]) \cong M(E'[p^\infty])^g$ we conclude that

$$\omega(A') \cong M/\text{FM}.$$

Note that as we’ve seen in §3.2.1, the presence of a principal polarization $\lambda'$ on an $\mathbb{F}_p^2$-abelian variety $A'$ induces a hermitian form on the $g$-dimensional $\mathbb{F}_p^2$-vector space $M/\text{FM}$. We say that an invariant differential on $A$ defined over $\mathbb{F}_p^2$ is an invariant differential on $(A, \lambda)$ if it respects this hermitian structure. We can therefore conclude that
Corollary 3.6. Let \((A, \lambda)\) be a principally polarized superspecial abelian variety over \(\mathbb{F}_p\), let \((A', \lambda')\) be its canonical \(\mathbb{F}_p^2\)-structure and \(M = M(A'[p^\infty])\). Then giving a basis of invariant differentials on \((A, \lambda)\) defined over \(\mathbb{F}_p^2\) is equivalent to giving a hermitian basis of \(M/FM\) over \(\mathbb{F}_p^2\).

3.2.6. Dieudonné module of a superspecial abelian variety. We use the notation introduced in §2.3.1.

We want to describe the structure of the principally quasi-polarized Dieudonné module \(M = M(E'[p^\infty])\), where \(E'\) is a supersingular elliptic curve defined over \(\mathbb{F}_p^2\). What we need is a simple consequence of the following result (Proposition 6.1 from [LO98]):

**Proposition 3.7.** Let \(K\) be a perfect field containing \(\mathbb{F}_p^2\), and suppose \(\{M, \langle, \rangle\}\) 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

\[
M \cong M_1 \oplus M_2 \oplus \ldots \oplus M_d \quad (\langle M_i, M_j \rangle = 0 \text{ if } i \neq j),
\]

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 \(\langle x, Fx \rangle = p^r e\) for some \(r \in \mathbb{Z}\) and \(e \in W \setminus pW\) with \(e^p = -e\); or

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

**Corollary 3.8.** \(M(E'[p^\infty]) \cong A_{1,1}^g\) 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 \(\langle, \rangle\) defines a map \(M_0 \to M_0^\dagger\) given by \(z \mapsto f_z\), where \(f_z(v) := \langle z, v \rangle\). 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 \(f_x = p^r y^t, f_{Fx} = p^r(Fy)^t, f_y = -p^r x^t\) and \(f_{Fy} = -p^r(Fx)^t\). For instance

\[
f_{Fy}(Fx) = \langle Fy, Fx \rangle = \langle y, VFx \rangle^p = \langle y, px \rangle^p = -p\langle x, y \rangle^p = -p^{r+1}.
\]

But the map \(M_0 \to M_0^\dagger\) 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 \(\langle x, Fx \rangle = 1\).

**Corollary 3.9.** There exists an isomorphism \(\text{End}(M, e_0)^\times \cong \text{GU}_g(O_p)\), 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

\[
1 \to U_p \to \text{GU}_g(O_p) \to \text{GU}_g(\mathbb{F}_p^2) \to 1,
\]

where the surjective map is reduction modulo the uniformizer \(\pi\) of \(O_p\).

**Proof.** Recall the identification \(\text{End}(A_{1,1}) \cong O_p\) from the proof of Corollary 2.11:

\[
\varphi: \text{End}(A_{1,1}) \to O_p \quad \left(\begin{array}{cc} x & y \\ -py & x \end{array}\right) \mapsto x + \pi y.
\]

On the other hand, any \(T \in \text{End}(M) = \text{End}(A_{1,1}^g)\) is a \(2g \times 2g\) matrix made of \(2 \times 2\) blocks of the form

\[
T_{ij} = \left(\begin{array}{cc} x_{ij} & y_{ij} \\ -py_{ij} & x_{ij} \end{array}\right).
\]
Therefore we have an isomorphism
\[ \varphi : \text{End}(M)^* \rightarrow \text{GL}_g(\mathcal{O}_p) \]
\[ T \in (T_{ij})_{i,j} \mapsto (x_{ij} + \pi y_{ij})_{i,j}. \]

We want to prove that under this isomorphism, \( \text{End}(M, e_0)^* \) corresponds to \( \text{GU}_g(\mathcal{O}_p) \). For this we use Corollary 3.8, which says that the bilinear form \( e_0 \) is given by the block-diagonal matrix
\[ E_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \]

Therefore we have
\[ \text{End}(M, e_0)^* = \{ T \in \text{End}(M)^* : T^t E_0 T = \gamma E_0, \gamma \in \mathbb{Z}_p \}. \]

Note that for the \( 2 \times 2 \) block \( T_{ij} \) we have
\[ (\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array})^{-1} T_{ij} (\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}) = (\begin{array}{cc} x_{ij}^p - y_{ij} \\ y_{ij}^p \end{array})_{ij}, \]
which maps under \( \varphi \) to \( x_{ij}^p - \pi y_{ij} = x_{ij} + \pi y_{ij} = \varphi(T_{ij}) \), where \( \bar{\cdot} \) denotes the conjugation in the quaternion algebra \( B_p = \mathcal{O}_p \otimes \mathbb{Q}_p \). This means that \( E_0^{-1} T^t E_0 T \) maps to \( \varphi(T)^* \), where we write \( U^* = \bar{U}^t \). Putting it all together we conclude that for any \( T \in \text{End}(M)^* \) we have
\[ T \in \text{End}(M, e_0)^* \iff E_0^{-1} T^t E_0 T = \gamma \iff \varphi(T)^* \varphi(T) = \gamma \iff \varphi(T) \in \text{GU}_g(\mathcal{O}_p), \]
which is precisely what we wanted to show.

For the second part of the statement note that
\[ M/FM = \{(0, a_1, 0, a_2, \ldots, 0, a_g)^t + FM : a_i \in F_{p^2} \}. \]

Let \( T = (T_{ij}) \in \text{End}(M, e_0)^* \), then its induced map on \( M/FM \) is
\[ T((0, a_1, 0, a_2, \ldots, 0, a_g)^t + FM) = \left(0, \sum_j a_j \bar{x}_{1j}, \ldots, 0, \sum_j a_j \bar{x}_{gj}\right) + FM, \]
where \( \bar{x}_{ij} \) denotes the reduction modulo \( \pi \) of \( x_{ij} \). Therefore \( T \) induces the identity map on \( M/FM \) if and only if
\[ \begin{pmatrix} \bar{x}_{11} & \bar{x}_{12} & \cdots & \bar{x}_{1g} \\ \bar{x}_{21} & \bar{x}_{22} & \cdots & \bar{x}_{2g} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{x}_{g1} & \bar{x}_{g2} & \cdots & \bar{x}_{gg} \end{pmatrix} = 1. \]

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

3.3. Construction of the bijection. Let \( A \) be a superspecial abelian variety of dimension \( g \) over \( \mathbb{F}_p \). Let \( A' \cong E^g \) be its canonical \( \mathbb{F}_{p^2} \)-structure, then \( A \cong E^g \) for \( E := E' \otimes \mathbb{F}_p \). Until further notice, I 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 \( \lambda_0 := \lambda_0' \otimes \mathbb{F}_p \), let \( \alpha_0 : A[N] \rightarrow (\mathbb{Z}/N\mathbb{Z})^{2g} \) be a level \( N \) structure on \( A \), and let \( \eta_0 \) be a basis of invariant differentials on \( (A, \lambda_0) \) 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 \( \lambda_0 \), resp. \( \lambda_0' \) will be denoted \( e_0 \), resp. \( e_0' \).

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

\[
\begin{align*}
A \xrightarrow{f} A & \quad \quad \quad \quad \quad \quad \quad (A[N], e_1) \xrightarrow{f} (A[N], e_2) \\
\lambda_1 \sim & \quad \quad \lambda_2 \sim \quad \quad \quad \quad \quad \quad \quad \alpha_1 \sim \\
A^t \xleftarrow{\sim} & \quad \quad A^t & \quad \quad \quad \quad \quad \quad \quad ((\mathbb{Z}/N\mathbb{Z})^{2g}, \text{std}) \xrightarrow{\sim} ((\mathbb{Z}/N\mathbb{Z})^{2g}, \text{std}),
\end{align*}
\]

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

Let \(\mathcal{O} := \text{End}(E)\) and \(B := \mathcal{O} \otimes \mathbb{Q}\). Let \(G := \text{GU}_g(B)\), and recall the notation of §3.2.4. The purpose of this section is to construct a bijection between the finite sets \(\Sigma\) and \(\Omega = \Omega(N)\), generalizing the result of §2.4.

**Lemma 3.10.** Given any principal polarization \(\lambda\) 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 \(\Psi^*\). If \(\phi : A \to A\) is an isogeny, then \(\Phi \in \text{GL}_g(B)\). If \(\lambda : A \to A^t\) is a polarization, then \(\lambda^t = \lambda\) so \(\Lambda^* = \Lambda\). Also \(\Lambda\) is positive-definite. If \(\lambda\) is a principal polarization, then \(\Lambda \in \text{GL}_g(\mathcal{O})\) defines a positive-definite quaternion hermitian form \(f\). By Proposition 3.2 we know that \(\Lambda\) can be diagonalized, i.e. there exists \(M \in \text{GL}_g(B)\) such that

\[
M^{-1} \Lambda M = \text{diag}(\alpha_1, \ldots, \alpha_g),
\]

with \(\alpha_i \in \mathbb{Q}\). The form \(f\) is positive-definite so \(\alpha_i \in \mathbb{Q}_{>0}\). But the norm theorem 3.3 says that the norm map is surjective onto \(\mathbb{Q}_{>0}\), so by the last part of Proposition 3.2 there exists \(M' \in \text{GL}_g(B)\) 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 \(Q \in \text{GL}_g(B)\). 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 \(\Phi\). Since \(\Phi \in \text{GL}_g(B)\) and the fixed principal polarization \(\lambda_0\) corresponds to the identity matrix, we conclude that \(\phi\) is an isogeny and

\[
\phi^t \circ \lambda \circ \phi = n^2.
\]

\(\square\)

We can now mimic our approach from §2. Lemma 3.10 allows us to identify \(\hat{\Sigma}\) with the set \(\hat{\Sigma}^0\) consisting of isomorphism classes of triples

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

where \((A, \lambda_0) \xrightarrow{\phi} (A, \lambda)\) is an isogeny of principally polarized abelian varieties and isomorphism is defined by the diagrams (4).

**Proposition 3.11.** An isogeny \(\phi_1 : (A, \lambda_0) \to (A, \lambda_1)\) defines for any prime \(\ell \neq p\) an element \([x_\ell] \in U_1(N) \backslash G_\ell\). If \(\ell \mid \text{deg } \phi_1\) then \([x_\ell] = 1\).
Lemma 3.12. Any two isogenies

Proof. Pick a prime $\ell \neq p$ and let $n$ satisfy $\frac{\ell^n}{\ell^{2n}}$. As we’ve seen in §3.2.1, $\phi$ 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’ll just write $e_\ell^{\lambda_0}$ and $e_\ell^{\lambda_1}$ (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

$$
(A[\ell^n], e_0) \xrightarrow{k_{\ell,1}} (A[\ell^n], e_1)
$$

$$
\alpha_0 \sim \alpha_1 \sim
$$

$$(\mathbb{Z}/\ell^n \mathbb{Z})^{2g} \to (\mathbb{Z}/\ell^n \mathbb{Z})^{2g}.$$

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

$$
(T_\ell A, e_0) \xrightarrow{T_\ell \phi_1} (T_\ell A, e_1)
$$

$$
x_\ell \sim
$$

$$(T_\ell A, e_0).$$

The map $x_\ell$ is not necessarily invertible, but since it’s injective with finite cokernel it defines a symplectic automorphism of $(V_\ell A, e_0)$, i.e. $x_\ell \in \text{GSp}_{2g}(\mathbb{Q}_\ell) = G_\ell$. If $\ell \nmid \deg \phi_1$ then $T_\ell \phi_1$ is a symplectic isomorphism so we can take $x_\ell = 1$.

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

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

Note that $\nu$ restricts to the identity on $A[\ell^n]$ so actually $\nu \in U_\ell(N)$. Conversely, if $\nu \in U_\ell(N)$ then $k_{\ell,1} \circ \nu^{-1} : (T_\ell A, e_0) \to (T_\ell A, e_1)$ is a symplectic isomorphism restricting to $\alpha_1^{-1} \circ \alpha$. Therefore $\phi_1$ gives us a well-defined element $[x_\ell] \in U_\ell(N) \backslash G_\ell$.

What happens at $p$? The isogeny $\phi_1$ 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 $\eta_1$ to $\eta_0$. 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 3.9, $x_p$ gives an element of $\text{GU}_g(B_p)$. Since $k_{p,1}$ is well-defined up to multiplication by $U_p$, we have that $\phi_1$ defines an element $[x_p] \in U_p \backslash \text{GU}_g(B_p)$.

Lemma 3.12. 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 $U \in \text{GU}_g(B)$.

Proof. Suppose $\phi_1, \tilde{\phi}_1$ satisfy

$$
\phi_1' \circ \lambda_1 \circ \phi_1 = m\lambda_0,
$$

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

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

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

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

$$U^*U = \Phi_1^*(\Phi_1^{-1})^* \Phi_1^{-1} \tilde{\phi}_1 = \Phi_1^* \left( \frac{1}{m} A_1 \right) \tilde{\phi}_1 = \frac{m}{m} I$$

so $U \in \mathit{GU}_g(B)$.

The next lemma says that we have indeed constructed a map

$$\gamma : \hat{\Sigma}_0 \to \Omega = U \backslash G(\hat{\mathbb{Q}})/G(\mathbb{Q}).$$

**Lemma 3.13.** The map $\gamma$ is well-defined.

**Proof.** We need to show that $\gamma$ 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 3.12 we can assume without loss of generality that $\phi_2 = f \circ \phi_1$. For $\ell \neq p$, we get the following diagrams

$$\begin{array}{ccc}
(T_\ell A, e_0) & \xrightarrow{T_\ell \phi_2} & (T_\ell A, e_1) \\
| \downarrow x_\ell & \sim & \downarrow k_{\ell,1} \\
(T_\ell A, e_0) & \sim & (T_\ell A, e_0)
\end{array} \quad \begin{array}{ccc}
(A[\ell^n], e_0) & \xrightarrow{k_{\ell,1}} & (A[\ell], e_1) \\
| \downarrow \alpha_1 & \sim & \downarrow \alpha_2 \\
(Z/\ell^n\mathbb{Z})^{2g} & \sim & (Z/\ell^2\mathbb{Z})^{2g}
\end{array}$$

where $k_{\ell,2} := T_\ell f \circ k_{\ell,1}$. It is now clear that we end up with the same $x_\ell \in \mathcal{O}_\ell^\times (N)\backslash B_\ell^\times$ as the one obtained from $\phi_1$. The exact same thing happens at the prime $p$. \hspace{1cm} \Box

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 $x_\ell \in G(\ell) = \mathit{GSp}_{2g}(\ell) = \mathit{Aut}(V_\ell, e_0)$. Let $n_\ell \in \mathbb{Z}$ be the smallest integer such that $y_\ell := \ell^n x_\ell \in \mathit{GSp}_{2g}(\ell) = \mathit{End}(T_\ell A, e_0)$. The endomorphism $y_\ell$ is injective with finite cokernel $C_\ell$. Let $\ell^k$ be the order of $C_\ell$. Let $K_\ell$ be the kernel of the map induced by $y_\ell$ 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 $x_p \in \mathit{GU}_g(B_p) = (\mathit{End}(M, e_0) \otimes \mathbb{Q}_p)^\times$. Write $x_p = a + \pi b$, where $a, b \in M_g(L_p)$ and $\pi^2 = -p$. We have

$$a = \sum_i a_i \otimes 1_{p^i},$$

$$b = \sum_j b_j \otimes 1_{p^j},$$

with $a_i, b_j \in \mathit{End}(M, e_0)$. 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 $y_p = a' + \pi b' \in \mathit{End}(M, e_0)$. 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 $x \in G(\hat{Q})$, $n_\ell = 0$ for all but finitely many $\ell$. Therefore it makes sense to set $q := \prod \ell^{n_\ell} \in \hat{Q}^\times$ and $y := xq$; the $\ell$-th component of $y$ is precisely the $y_\ell$ above, and clearly $[x] = [y]$. Now set $K := \bigoplus K_\ell$, 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 $\lambda$ on $A$ such that $\phi$ is an isogeny of polarized abelian varieties. For $\ell \neq p$, our construction gives for any positive integer $m$

$$0 \to \ker \to (A[\ell^m], e_0) \overset{\phi}{\to} (A[\ell^m], e) \to (A[\ell^m], e_0).$$

Due to the structure of $\ell^m$-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

$$0 \to (T_\ell A, e_0) \overset{T_\ell \phi}{\to} (T_\ell A, e) \to (T_\ell A, e_0) \overset{y_\ell}{\to} C_\ell \to 0.$$  

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

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

for $\ell | N$ piece together to give a level $N$ structure on $(A, \lambda)$. 
For $\ell = p$ we have similarly

$$0 \to (M, e) \overset{y_p}{\to} (M, e_0) \to \ker\lambda \to 0.$$  

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

The next result tells us that we have indeed constructed a map

$$\delta : \Omega \to \tilde{\Sigma}^0.$$

**Proposition 3.14.** The map $\delta$ is well-defined.

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

$$0 \to (T_\ell A, e_0) \overset{y_\ell}{\to} (T_\ell A, e_0) \to C_\ell \to 0.$$  

The snake lemma gives

$$\ker v_\ell = 0, \quad \ker v_\ell \cong \ker u.$$
Let $\ell^k$ be the order of $C_\ell$, then we can restrict the above diagram to the $\ell^k$-torsion and get

$$
\begin{align*}
0 \rightarrow K_\ell \rightarrow (A[\ell^k], e_0) & \rightarrow (A[\ell^k], e_0)/\ker y_\ell \rightarrow 0 \\
& \uparrow g_\ell \quad \uparrow u_\ell \quad \uparrow h_\ell \\
0 \rightarrow \bar{K}_\ell \rightarrow (A[\ell^k], e_0) & \rightarrow (A[\ell^k], e_0)/\ker \bar{y}_\ell \rightarrow 0,
\end{align*}
$$

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

$$
(6) \quad \begin{align*}
0 \rightarrow K_\ell \rightarrow (A[\ell^k], e_0) & \rightarrow (A[\ell^k], e_0)/\ker y_\ell \rightarrow 0 \\
& \uparrow g_\ell \\
0 \rightarrow \bar{K}_\ell \rightarrow (A[\ell^k], e_0) & \rightarrow (A[\ell^k], e_0)/\ker \bar{y}_\ell \rightarrow 0,
\end{align*}
$$

$$
(7) \quad \begin{align*}
0 \rightarrow \text{Im } y_\ell \rightarrow (A[\ell^k], e_0) & \rightarrow C_\ell \rightarrow 0 \\
& \uparrow h_\ell \\
0 \rightarrow \text{Im } \bar{y}_\ell \rightarrow (A[\ell^k], e_0) & \rightarrow \bar{C}_\ell \rightarrow 0,
\end{align*}
$$

where I have taken the liberty of using the same label $h_\ell$ for two maps which are canonically isomorphic. We first apply the snake lemma to diagram 7 and get

$$
\ker h_\ell = 0, \quad \text{coker } h_\ell \cong \ker v_\ell.
$$

Using this information together with the snake lemma in diagram 6 gives

$$
\ker g_\ell \cong \ker u_\ell, \quad 0 \rightarrow \coker g_\ell \rightarrow \coker u_\ell \rightarrow \coker h_\ell \rightarrow 0.
$$

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

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

$$
\begin{align*}
0 \rightarrow K \rightarrow (A, \lambda_0) & \rightarrow (A, \lambda) \rightarrow 0 \\
& \downarrow g \\
0 \rightarrow \bar{K} \rightarrow (A, \lambda_0) & \rightarrow (A, \lambda) \rightarrow 0,
\end{align*}
$$

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

$$
0 \rightarrow \ker g \rightarrow \ker u \rightarrow \ker f \rightarrow \coker g = 0 \rightarrow \coker u = 0 \rightarrow \coker f \rightarrow 0.
$$

But the map $\ker g \rightarrow \ker u$ is the sum of the isomorphisms $\ker g_\ell \cong \ker u_\ell$, so $\ker u \rightarrow \ker f$ is the zero map; therefore $\ker f = 0$. Clearly $\coker f = 0$, so $f$ is an isomorphism.
We check that this isomorphism preserves level $N$ structures. We have a diagram

\[
\begin{array}{ccc}
(T_\ell A, e_0) & \xrightarrow{\ell_\phi} & (T_\ell A, e) \\
\downarrow \scriptstyle{T_\ell u = u_\ell} & & \downarrow \scriptstyle{T_\ell f} \\
(T_\ell A, e_0) & \xrightarrow{T_\ell \phi} & (T_\ell A, \bar{e}),
\end{array}
\]

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 $(A, \lambda)$ and $(A, \bar{\lambda})$ are defined in such a way that the inner squares in the following diagram commute:

\[
\begin{array}{ccc}
(A[\ell^n], e) & \xrightarrow{f} & (A[\ell^n], \bar{e}) \\
\downarrow \scriptstyle{\sim} & & \downarrow \scriptstyle{\sim} \\
(A[\ell^n], e_0) & \xrightarrow{\sim} & (A[\ell^n], \bar{e}) \\
\downarrow \scriptstyle{\sim} & & \downarrow \scriptstyle{\sim} \\
((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \text{std}) & \xrightarrow{\sim} & ((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \text{std}) \\
\end{array}
\]

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 $x = x_\ell$, $\ell \neq p$ (the case $\ell = p$ is analogous, even easier). If $\ell' \nmid \ell p$, then $x_{\ell'} = x_\ell \ell'$ and $y_{\ell'} = y_\ell \ell'$. Multiplication by $\ell$ 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:

\[
\begin{array}{ccc}
0 & \longrightarrow & K_{\ell'} \\
\downarrow \scriptstyle{g_{\ell'}} & & \downarrow \scriptstyle{v_{\ell'}} \\
0 & \longrightarrow & (A[\ell^k], e_0) \\
\end{array}
\]

Something similar occurs at $p$. If $\ell' = \ell$, we get $x_{\ell'} = x_\ell \ell'$ and $y_{\ell'} = y_\ell \ell'$ so $\bar{K}_{\ell} = K_{\ell}$. We have an isomorphism $\bar{K} \cong K$ so $(A, \lambda) \cong (A, \bar{\lambda})$. 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

\[
\begin{array}{ccc}
(T_{\ell'} A, e) & \xrightarrow{k_{\ell'}} & (T_{\ell'} A, e_0) \\
\downarrow \scriptstyle{\sim} & & \downarrow \scriptstyle{\sim} \\
(T_{\ell'} A, \bar{e}) & \xrightarrow{k_{\ell'}} & (T_{\ell'} A, \bar{e}) \\
\downarrow \scriptstyle{\sim} & & \downarrow \scriptstyle{\sim} \\
((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \text{std}) & \xrightarrow{\sim} & ((\mathbb{Z}/\ell^n\mathbb{Z})^{2g}, \text{std})
\end{array}
\]

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 $K_{\ell} = K_{\ell}$ 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 $C_{\ell}$ (therefore $K_{\ell}$) depends on the chosen isomorphism $(T_{\ell'} A, e_0) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, and this can change $y_\ell$ 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
Theorem 3.17. the same kernel as \( GSp \) Hecke algebra, with the action of \( GSp \) forming an ad` ele \( N \) structure and the invariant differential will stay the same. Compatibilities.

3.4. Therefore \( y \)

We see from diagram (3.3) that \( p \)

and a similar argument holds for the \( \eta \) and \( \eta \).

\[ \text{Lemma 3.15. The map } \gamma \text{ is bijective with inverse } \delta. \]

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

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

We see from diagram (3.3) that \( y_\ell = k_\ell^{-1} \circ T_\ell \phi \), where \( k_\ell \) is an isomorphism that restricts to \( \alpha^{-1} \circ \alpha_0 \). Therefore \([y_\ell] \) is exactly the local element that’s 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 \( x_\ell \) forming an adèle \( x \). We have \( \ker \phi = \prod_\ell \coker x_\ell \). Now when we apply \( \delta \) we already have \( x_\ell \in \text{GSp}_{2g}(\mathbb{Z}_\ell) \) so \( y_\ell = x_\ell \) and \( K = \bigoplus \coker x_\ell = \ker \phi \). We get an isogeny \((A, \lambda_0) \to (A, \lambda)\) which has the same kernel as \( \phi \), therefore \((A, \lambda, \lambda) \cong (A, \lambda)\). It is clear from the construction of \( \delta \) that the level \( N \) structure and the invariant differential will stay the same.

We have just proved

**Theorem 3.16. There is a canonical bijection \( \hat{\Sigma}^0 \to \Omega \).**

3.4. Compatibilities. We now turn to the proof of the following result:

**Theorem 3.17. The canonical bijection \( \gamma : \hat{\Sigma}^0(N) \to \Omega(N) \) is compatible with the action of the Hecke algebra, with the action of \( \text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z}) \), and with the operation of raising the level.**

3.4.1. Hecke action. In this section \( \ell \) will denote a fixed prime not dividing \( pN \).

An isogeny of polarized abelian varieties \( \phi : (A_1, \lambda_1) \to (A_2, \lambda_2) \) is said to be an \( \ell \)-isogeny if its degree is a power of \( \ell \). Such \( \phi \) induces a symplectic similitude

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

which gives an element \( g \in \text{GSp}_{2g}(\mathbb{Q}_\ell) \). Since \( g \) is defined only up to changes of symplectic bases for \( T_\ell A_1 \) and \( T_\ell A_2 \), \( \phi \) actually defines a double coset \( HgH \), where \( H = \text{GSp}_{2g}(\mathbb{Z}_\ell) \). We say that \( \phi \) is of type \( HgH \). If \( C \) is a finite \( \ell \)-subgroup of an abelian variety \( A \) and \( \lambda \) is a principally polarization on \( A \), there exists a principal polarization \( \lambda_C \) on \( A/C \) that makes the quotient isogeny \( A \to A/C \) into an isogeny of principally polarized abelian varieties. We say that \( C \) is of type \( HgH \) if the quotient isogeny \((A, \lambda) \to (A/C, \lambda_C)\) is of type \( HgH \).
42 Since \((\text{GSp}_{2g}(\mathbb{Q}_\ell), \text{GSp}_{2g}(\mathbb{Z}_\ell))\) is a Hecke pair (see §3.3.1 of [AZ95]), we can talk about the local Hecke algebra \(\mathcal{H}_\ell := \mathcal{H}(G, H)\), where \(G = \text{GSp}_{2g}(\mathbb{Q}_\ell)\) and \(H = \text{GSp}_{2g}(\mathbb{Z}_\ell)\).

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

\[
T_{HgH}(\{(A, \lambda_0) \overset{\phi}{\to} (A, \lambda), \alpha, \eta\}) := \sum_{C \in \text{type } HgH} [(A, \lambda_0) \overset{\phi}{\to} (A, \lambda) \overset{\psi_C}{\to} (A, \lambda_C), \alpha, \eta_C],
\]

where \(\eta_C := M(\hat{\psi}_C^{-1})(\eta)\), and \(\alpha_C\) is defined by the diagram

\[
(A[N], e) \xrightarrow{\psi_C} (A[N], e_C) \xrightarrow{\alpha} ((\mathbb{Z}/N\mathbb{Z})^2, \text{std}) \xrightarrow{\alpha_C} ((\mathbb{Z}/N\mathbb{Z})^2, \text{std}).
\]

Note that these definitions make sense because \((\deg \hat{\psi}_C, pN) = 1\).

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

\[
\begin{array}{ccc}
A & \xleftarrow{\hat{\psi}_C} & A \\
\downarrow{\lambda} & & \downarrow{\lambda_C} \\
A' & \xrightarrow{(\hat{\psi}_C)^\prime} & A'.
\end{array}
\]

The action is defined by

\[
T_{HgH}(\{(A, \lambda_0) \overset{\phi}{\to} (A, \lambda), \alpha, \eta\}) := \sum_{C \in \text{type } Hg^{-1}H} [(A, \lambda_0) \overset{\phi}{\to} (A, \lambda) \overset{\hat{\psi}_C^\prime}{\to} (A, \lambda_C), \lambda_C, \alpha_C, \eta_C],
\]

where \(\eta_C := M(\hat{\psi}_C')^{-1}(\eta)\), and \(\alpha_C\) is defined by the diagram

\[
(A[N], e) \xleftarrow{\hat{\psi}_C^\prime} (A[N], e_C) \xrightarrow{\alpha} ((\mathbb{Z}/N\mathbb{Z})^2, \text{std}) \xrightarrow{\alpha_C} ((\mathbb{Z}/N\mathbb{Z})^2, \text{std}).
\]

The algebra \(\mathcal{H}_\ell\) acts on \(H \setminus G\) as follows: let \(HgH = \bigsqcup_i Hg_i\), let \(Hx \in H \setminus G\) and choose a representative \(x \in Hx\). Then there exist representatives \(g_i \in Hg_i\) such that

\[
T_{HgH}(Hx) = \sum_i Hg_ix.
\]

The algebra \(\mathcal{H}_\ell\) acts on \(\Omega\) by acting on the component \(Hx_\ell\) of \([x]\) \in \Omega.

**Lemma 3.18.** The bijection \(\gamma : \tilde{\Sigma}^0 \to \Omega\) is compatible with the action of the local Hecke algebra \(\mathcal{H}_\ell\), i.e. for all \(HgH \in \mathcal{H}_\ell\) and \([\phi, \alpha, \eta]\) we have

\[
\gamma(T_{HgH}([\phi, \alpha, \eta])) = T_{HgH}(\gamma([\phi, \alpha, \eta])).
\]
Proof. Let \( HgH \in \mathcal{H}_T \), let \( [(A, \lambda_0) \xrightarrow{\phi} (A, \lambda), \alpha, \eta] \in \Sigma^0 \) and let \( [x] = \gamma([\phi, \alpha, \eta]) \).

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

\[
\begin{array}{ccc}
(T_{\ell'} A, e_0) & \xrightarrow{T_{\ell'} \phi} & (T_{\ell'} A, e) \\
\downarrow{x_{\ell'}} & & \downarrow{x_{\ell}} \\
(T_{\ell'} A, e_0) & \xrightarrow{k_{\ell'}} & (T_{\ell'} A, e_C).
\end{array}
\]

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 (8)), we get that \( [x_{C, \ell'}] = [x_{\ell'}] \).

A similar argument, based on the following diagram, shows that \( [x_{C, \ell}] = [x_{\ell}] \):

\[
\begin{array}{ccc}
(M, e_C) & \xrightarrow{M(\psi_C)} & (M, e) \\
\downarrow{k_{\ell}} & & \downarrow{x_{\ell}} \\
(M, e_0) & \xrightarrow{k_{p}} & (M, e_0).
\end{array}
\]

Let’s figure out what happens at \( \ell \). 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 \( y_C = k_{C}^{-1} \circ T_{\ell} \psi_C \). Via the identification \( k_{\ell}, y_C \) induces a map \( z_C : (T_{\ell} A, e_0) \to (T_{\ell} A, e_0) \). We have a diagram

\[
\begin{array}{ccc}
(T_{\ell} A, e_0) & \xrightarrow{T_{\ell} \phi} & (T_{\ell} A, e) \\
\downarrow{x_{\ell}} & & \downarrow{z_C} \\
(T_{\ell} A, e_0) & \xrightarrow{k_{\ell}} & (T_{\ell} A, e).
\end{array}
\]

\[
\begin{array}{ccc}
(T_{\ell} A, e) & \xrightarrow{T_{\ell} \psi_C} & (T_{\ell} A, e_C) \\
\downarrow{y_C} & & \downarrow{k_{C}} \\
(T_{\ell} A, e) & \xrightarrow{k_{\ell}} & (T_{\ell} A, e).
\end{array}
\]

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 \( k_{\ell} \) 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 \( \delta \) in §3.3 (pages 37 and following) 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 \( C \mapsto Hz_C \) is now the same as the proof of Lemma 3.15.

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 \( \hat{\Sigma}^0 \) 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 \([x_C] := \gamma([\psi_C^{-1}_G, \phi, \alpha_C, \eta_C])\). If \((\ell', p\ell) = 1\), we have a diagram

\[
\begin{array}{c}
(T_{\ell'} A, e_0) \xrightarrow{T_{\ell'} \phi} (T_{\ell'} A, e) \xleftarrow{T_{\ell'} \hat{\psi}_C} (T_{\ell'} A, e_C).
\end{array}
\]

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 (9)), we get that \([x_{C,\ell'}] = [x_{\ell'}]\). The situation at \(p\) is similar and we have \([x_{C,p}] = [x_p]\).

What about \(\ell\)? As before, we fix \(x_{\ell} \in Hx_0\) 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 \(y_C := T_{\ell} \hat{\psi}_C \circ k_C\). Via the identification \(k_{\ell}, y_C\) induces a map \(z_C : (T_{\ell} A, e_0) \to (T_{\ell} A, e_0)\). We have a diagram

\[
\begin{array}{c}
(T_{\ell} A, e_0) \xrightarrow{T_{\ell} \phi} (T_{\ell} A, e) \xleftarrow{T_{\ell} \hat{\psi}_C} (T_{\ell} A, e_C).
\end{array}
\]

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 \(\det(HgH) > 1\).

3.4.2. Action of \(\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})\). Within this section we’ll write \(G\) to denote \(\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})\). The group \(G\) acts on \(\tilde{\Omega}^0\) as follows:

\[g \cdot [\phi, \lambda, \alpha, \eta] := [\phi, \lambda, g \circ \alpha, \eta].\]

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

\[G \xrightarrow{\sim} \prod_{\ell} U_{\ell}(N) \setminus U_{\ell}\]

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

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

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

Lemma 3.19. The bijection \(\gamma : \tilde{\Omega}^0 \to \Omega\) is compatible with the action of \(\text{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})\).
Proof. Let \( \prod U_\ell(N)x_\ell := \gamma(\phi, \lambda, \alpha, \eta) \). and

\[
\prod U_\ell(N)x_\ell' := \gamma(g \cdot [\phi, \lambda, \alpha, \eta]) = \gamma([\phi, \lambda, g \circ \alpha, \eta]).
\]

Pick some \( \ell \neq p \) and set \( H := U_\ell(N) \); 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 \( k_\ell' := k_\ell \circ (\alpha_0^{-1}\circ g \circ \alpha_0) \) 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 \( k_\ell' \) 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. \( \square \)

3.4.3. Raising the level. Suppose \( N' = dN \) for some positive integer \( d \). A level \( N' \) structure

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

on the principally polarized abelian variety \((A, \lambda)\) induces a level \( N \) structure on \((A, \lambda)\) 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

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

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

\[
\Sigma^0(N') \to \Sigma^0(N).
\]

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

\[
\Omega(N') \to \Omega(N).
\]

We want to show that the bijection \( \gamma \) commutes with these maps. This is clear at primes \( \ell \nmid N' \), so suppose \( \ell \) is a prime divisor of \( N' \); say \( \ell^m \| N \) and \( \ell^0 \| N' \). Choose elements \([\phi, \lambda, \alpha', \eta] \in \Sigma^0(N') \), \([x'] := \gamma([\phi, \lambda, \alpha', \eta]) \) and \([x] := \gamma([\phi, \lambda, \alpha, \eta]) \). 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

\[
\begin{array}{ccc}
(A[\ell^m], e_0) & \xrightarrow{k'_\ell} & (A[\ell^m], e) \\
\sim \downarrow & & \downarrow \sim \\
((\mathbb{Z}/\ell^m\mathbb{Z})^{2g}, \text{std}) & \xrightarrow{\alpha'} & ((\mathbb{Z}/\ell^0\mathbb{Z})^{2g}, \text{std}).
\end{array}
\]
This defines the local component \( U_\ell(N')x'_\ell \). We can restrict \( k'_\ell \) even further to the \( \ell^m \)-torsion, and then by the definition of \( \alpha \) we have

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

But this means that \( k'_\ell \) plays the role of the \( k_\ell \) in the definition of \( x_\ell \), 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 \( \ell \), so we’re done.

### 3.5. Restriction to the superspecial locus.
Let \( V \) be an \( \mathbb{F}_p \)-vector space and let \( \rho : \text{GU}_g(\mathbb{F}_p^2) \to \text{GL}(V) \) be a representation. A superspecial modular form\(^1\) of weight \( \rho \) and level \( N \) is a function \( f : \Sigma \to V \) satisfying

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

The space of all such forms will be denoted \( S_\rho \). If \( \tau \) is a subrepresentation of \( \rho \), then \( S_\tau \subset S_\rho \). If \( \rho \) and \( \tau \) are representations, then

\[
S_\rho \otimes \tau = S_\rho \otimes S_\tau.
\]

Let \( \mathcal{I} \) denote the ideal sheaf of \( i : \Sigma \to X \), i.e. the kernel in:

\[
0 \to \mathcal{I} \to O_X \to i_*O_\Sigma \to 0.
\]

The sheaf \( \mathcal{I} \) is coherent (by Proposition II.5.9 of [Har77]). Given one of our sheaves \( E_\rho \), we obtain after tensoring and taking cohomology

\[
0 \to H^0(X, \mathcal{I} \otimes E_\rho) \to H^0(X, \mathcal{I} \otimes E_\rho) \to H^0(X, i_*O_\Sigma \otimes E_\rho) = H^0(\Sigma, i^*E_\rho) \to H^1(X, \mathcal{I} \otimes E_\rho).
\]

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

\[
0 \to H^0(X, \mathcal{I} \otimes E_\rho) \to M_\rho(N) \xrightarrow{\text{Res}} S_\text{Res}_\rho \to H^1(X, \mathcal{I} \otimes E_\rho),
\]

where \( \text{Res} \) restricts representations on \( \text{GL}_g \) to the finite subgroup \( \text{GU}_g(\mathbb{F}_p^2) \).

We’ll use the following result to determine when the map \( r \) is surjective:

**Theorem 3.20** (Serre, see Theorem III.5.2 in [Har77]). Let \( X \) be a projective scheme over a noetherian ring \( A \), and let \( \mathcal{F} \) be a very ample invertible sheaf on \( X \) over \( \text{Spec} \ A \). Let \( \mathcal{G} \) be a coherent sheaf on \( X \). Then

(a) for each \( i \geq 0 \), \( H^1(X, \mathcal{G}) \) is a finitely generated \( A \)-module;

(b) there is an integer \( n_0 \), depending on \( \mathcal{G} \), such that for each \( i > 0 \) and each \( n \geq n_0 \)

\[
H^i(X, \mathcal{G} \otimes \mathcal{F}^n) = 0.
\]

Let \( \omega = \Lambda^g \mathcal{E} = \mathcal{E}_{\det} \); it is an ample invertible sheaf (see Theorem V.2.5 in [FC90]). Then for \( n \gg 0 \) we have

\[
H^1(X, (\mathcal{I} \otimes E_\rho) \otimes \omega^n) = 0,
\]

so for \( n \gg 0 \), \( r \) is a surjective map

\[
r : M_{\rho \otimes \det^n}(N) \to S_{\text{Res}(\rho \otimes \det^n)}.
\]

\(^1\)This is not standard terminology.
3.5.1. **Lifting weights.** If $H$ is a subgroup of a group $G$, we say that a representation $\rho$ of $H$ lifts to $G$ if there exists a representation $\tilde{\rho}$ of $G$ such that $\rho = \text{Res} \tilde{\rho}$. It is clear that if $\rho$ lifts to $\tilde{\rho}$ and $\tau$ lifts to $\tilde{\tau}$, then $\rho \oplus \tau$ lifts to $\tilde{\rho} \oplus \tilde{\tau}$.

Let $q$ be some power of $p$. The following is a direct consequence of Theorems 6.1 and 7.4 from [Ste63]:

**Proposition 3.21.** Every irreducible representation of $\text{SL}_g(\mathbb{F}_q)$ lifts to a unique irreducible rational representation of $\text{SL}_g(\mathbb{F}_p)$.

We now extend this to

**Proposition 3.22.** Every irreducible representation of $\text{GL}_g(\mathbb{F}_q)$ lifts to an irreducible rational representation of $\text{GL}_g(\mathbb{F}_p)$.

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

Via the canonical embeddings $\text{SL}_g(\mathbb{F}_q) \subset \text{GL}_g(\mathbb{F}_q)$ and $\mathbb{G}_m(\mathbb{F}_q) \subset \text{GL}_g(\mathbb{F}_q)$, $\rho$ induces representations $\rho_s : \text{SL}_g(\mathbb{F}_q) \to \text{GL}(V)$ and $\rho_m : \mathbb{G}_m(\mathbb{F}_q) \to \text{GL}(V)$, such that $\text{Im} \rho_s$ commutes with $\text{Im} \rho_m$. Since $\text{GL}_g(\mathbb{F}_q) = \text{SL}_g(\mathbb{F}_q) \cdot \mathbb{G}_m(\mathbb{F}_q)$ and $\text{SL}_g(\mathbb{F}_q) \cap \mathbb{G}_m(\mathbb{F}_q) = \mu_g(\mathbb{F}_q)$, we also have that $\rho_s(\zeta) = \rho_m(\zeta)$ for all $\zeta \in \mu_g(\mathbb{F}_q)$.

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

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

$$\lambda \mapsto \left( \begin{array}{ccc} \lambda^{a_1} & & \\ & \ddots & \\ & & \lambda^{a_n} \end{array} \right)$$

with $a_i \in \mathbb{Z}/(q - 1)\mathbb{Z}$. I 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 $A \in \text{SL}_g(\mathbb{F}_p^2)$, 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 $A \in \text{SL}_g(\mathbb{F}_q)$, we conclude that as an $\text{SL}_g(\mathbb{F}_q)$-module, $V$ has a direct sum decomposition

$$V = V_1 \oplus \ldots \oplus V_j$$

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 is invariant under both $\text{SL}_g(\mathbb{F}_q)$ and $\mathbb{G}_m(\mathbb{F}_q)$, contradicting the hypothesis that $V$ is an irreducible representation of $\text{GL}_g(\mathbb{F}_q)$. 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 $\rho_m$ is completely reducible and that any choice of $\tilde{a} \in \mathbb{Z}$ with $\tilde{a} \equiv a \pmod{q - 1}$ yields a completely reducible lift $\tilde{\rho}_m : \mathbb{G}_m(\mathbb{F}_p) \to \text{GL}(V)$ given simply by $\lambda \mapsto \lambda^{\tilde{a}}$. Note that $\tilde{\rho}_m$ is a rational representation. Later on we’ll need to choose a lift of $a$ to $\tilde{a} \in \mathbb{Z}$ that suits us better.

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

By Proposition 3.21, $\rho_s$ lifts to an irreducible rational $\tilde{\rho}_s : \text{SL}_g(\mathbb{F}_p) \to \text{GL}(V)$. Since $\mathbb{G}_m$ acts by scalars, $\text{Im} \tilde{\rho}_m$ commutes with $\text{Im} \tilde{\rho}_s$. I claim that the maps $\rho_m$ and $\tilde{\rho}_s$ agree on $\mu_g(\mathbb{F}_p) = \text{SL}_g(\mathbb{F}_p) \cap \mathbb{G}_m(\mathbb{F}_p)$. Assuming this is true, we can construct a rational representation

$$\tilde{\rho} : \text{GL}_g(\mathbb{F}_p) \to \text{GL}(V)$$

$$M \mapsto \tilde{\rho}_m(\det M) \cdot (\det M)^{-1} \tilde{\rho}_s((\det M)^{-1} M).$$
Since the restriction of \( \tilde{\rho} \) to \( \text{SL}_g(\mathbb{F}_p) \) is \( \text{SL}_g(\mathbb{F}_p) \), we conclude that \( \tilde{\rho} \) is irreducible.

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

Consider the linear transformation \( \tilde{\rho}_s(\zeta) \). 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 \( \tilde{\rho}_s(\zeta) \) 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 \( \text{SL}_g(\mathbb{F}_p) \) the representation \( \tilde{\rho}_s \) is reducible, which is a contradiction. So

\[
\tilde{\rho}_s(\zeta) = \zeta^b, \quad \text{for some } b \in \mathbb{Z}/g\mathbb{Z}.
\]

We want to show that \( \tilde{\rho}_m(\zeta) = \tilde{\rho}_s(\zeta) \), i.e. that we can choose \( a \in \mathbb{Z} \) such that \( a \equiv b \pmod{g} \). Let \( d = (g, q - 1) \) and write \( g = dm, \ q - 1 = dn \). We have \((\zeta^m)^d = \zeta^g = 1 \) so \((\zeta^m)^{d^{-1}} = (\zeta^md)^n = 1 \) so \( \zeta^m \in \mathbb{F}_q \). Therefore \( \zeta^m \in \mu_g(\mathbb{F}_q) \) and hence

\[
(\zeta^b)^m = \tilde{\rho}_s(\zeta^m) = \tilde{\rho}_m(\zeta^m) = (\zeta^m)^a.
\]

This implies that \( m\tilde{a} \equiv mb \pmod{g} \), i.e. \( \tilde{a} \equiv b \pmod{d} \). Since \( d = (g, q - 1) \) and \( d|\tilde{a} - b \) there exist integers \( u, v \) such that \( \tilde{a} - b = u\tilde{g} + v(q - 1) \) and therefore

\[
(\tilde{a} - v(q - 1)) \equiv b \pmod{g},
\]

which is what we wanted. \( \square \)

Note that in contrast with Proposition 3.21 the lift of \( \rho \) to \( \text{GL}_g(\mathbb{F}_p) \) is not unique. Fix some lift \( \tilde{\rho} \), then any lift can be written in the form \( \text{det}^m \tilde{\rho} \), where \( m \) is a common multiple of \( g \) and \( q - 1 \).

**Corollary 3.23.** Given an irreducible representation \( \tau : \text{GU}_g(\mathbb{F}_p^2) \to \text{GL}(W) \), there exists an irreducible rational representation \( \tilde{\rho} : \text{GL}_g(\mathbb{F}_p) \to \text{GL}(V) \) such that \( \tau \subset \text{Res } \tilde{\rho} \).

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

3.5.2. **Proof of the main result.** We have come to the main result of the section. Recall the notation \( U_\ell(N) = \text{GSp}_{2g}(\mathbb{Z}_\ell)(N) \) for \( \ell \neq p \), \( U_p = \ker(\text{GU}_g(\mathbb{O}_p) \to \text{GU}_g(\mathbb{F}_p^2)) \) and

\[
U = U_p \times \prod_{\ell \neq p} U_\ell(N).
\]

**Theorem 3.24.** Fix a dimension \( g > 1 \), a level \( N \geq 3 \) and a prime \( p \) not dividing \( N \). The systems of Hecke eigenvalues coming from Siegel modular forms (mod \( p \)) of dimension \( g \), level \( N \) and any weight \( \rho \), are the same as the systems of Hecke eigenvalues coming from algebraic modular forms (mod \( p \)) of level \( U \) and any weight \( \rho_S \) on the group \( \text{GU}_g(B) \).

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

\[
\tilde{\tau} : H^0(X, \mathcal{I} \otimes E_\rho) \to H^0(X, \mathcal{I}/\mathcal{I}^2 \otimes E_\rho).
\]

Consider \( \tilde{f} \in H^0(X, \mathcal{I}/\mathcal{I}^2 \otimes E_\rho) \). We have an exact sequence

\[
0 \to \mathcal{I} \otimes \mathcal{I}/\mathcal{I}^2 \otimes E_\rho \to \mathcal{I}/\mathcal{I}^2 \otimes E_\rho \to i_*\mathcal{O}_\Sigma \otimes \mathcal{I}/\mathcal{I}^2 \otimes E_\rho \to 0
\]
which gives us a long exact sequence that starts with

\[ 0 \to \text{H}^0(X, \mathcal{I}^2/\mathcal{I}^3 \otimes \mathbb{E}_p) \to \text{H}^0(X, \mathcal{I}/\mathcal{I}^2 \otimes \mathbb{E}_p) \xrightarrow{\text{res}_*} \text{H}^0(\Sigma, \mathcal{I}/\mathcal{I}^2 \otimes \mathbb{E}_p)). \]

If \( r_1(f) = 0 \) then \( f \in \text{H}^0(X, \mathcal{I}^2/\mathcal{I}^3 \otimes \mathbb{E}_p) \) and we can similarly consider \( r_2(f), r_3(f) \) etc. There exists some \( n \) such that \( r_n(f) \neq 0 \). Let \( f_S = r_n(f) \in \text{H}^0(\Sigma, \mathcal{I}/\mathcal{I}^2 \otimes \mathbb{E}_p)). \) Note that \( \mathcal{I}^n/\mathcal{I}^{n+1} = \text{Sym}^n(\mathcal{I}/\mathcal{I}^2) \) and that \( \mathcal{I}/\mathcal{I}^2 = \mathcal{I}/\mathcal{I}^2 \). Since this map is also Hecke-invariant, we conclude from Proposition 1.2.2 of [AS86] that any system of Hecke eigenvalues that occurs in \( \mathcal{I}/\mathcal{I}^2 \) is surjective. Then there exists an \( I \) such that \( \mathcal{I}/\mathcal{I}^2 \cong \mathbb{E}_{\text{Sym}^2} \) and that \( \mathcal{I}/\mathcal{I}^2 = \mathcal{I}/\mathcal{I}^2 \). By Corollary 3.23 we get a rational representation \( \overline{\mathcal{I}} \) which gives us a long exact sequence that starts with

\[ f \in \text{GL}(\mathcal{I}/\mathcal{I}^2 \otimes \mathbb{E}_p) \]

for some integer \( n \)

where \( \text{GL}(\mathcal{I}/\mathcal{I}^2 \otimes \mathbb{E}_p) \)

is surjective for \( n \geq 0 \), and therefore there exists an integer \( k \) such that

\[ \rho \otimes \text{Sym}^k(\mathcal{I}/\mathcal{I}^2) = 0 \]

is surjective. Since this map is also Hecke-invariant, we conclude from Proposition 1.2.2 of [AS86] that any system of Hecke eigenvalues that occurs in \( S_{\text{res}} \) also occurs in \( M_{\rho \otimes \text{Sym}^k(\mathcal{I}/\mathcal{I}^2)} \).

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 \( S_{\text{res}} \) of all weights. By Theorem 3.17 we know that \( S_{\text{res}} \) is isomorphic as a Hecke module to the space of algebraic modular forms (mod \( p \)) of weight \( \rho_{\text{res}} \), and we're done. \( \square \)

3.5.3. Agreement with the definition of Gross. In this section we'll write \( G = \text{GU}_g(\mathbb{F}_p) \).

Recall from §3.2.4 that Gross defines algebraic modular forms (mod \( p \)) as follows: let \( \rho : G \to \text{GL}(V) \) be an irreducible representation where \( V \) is a finite-dimensional vector space over \( \mathbb{F}_p \), then set

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

For comparison, our spaces of modular forms on \( \Omega \) are defined as

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

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

The purpose of this section is to show that the spaces \( M(\rho) \) and \( M(\tau) \) for varying \( \rho \) and \( \tau \) 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 \( f \in M(\rho) \otimes \mathbb{F}_p \) such that \( T(f) = a_T f \) for all \( T \). Let \( \rho \otimes \mathbb{F}_p \) denote the composition \( G \to \text{GL}(V) \to \text{GL}(V \otimes \mathbb{F}_p) \). The map

\[ M(\rho) \otimes \mathbb{F}_p \to M(\rho \otimes \mathbb{F}_p) \]

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

Conversely, suppose that \( (a_T : T) \) is a system of Hecke eigenvalues coming from \( M(\tau) \) for some \( \tau : G \to \text{GL}(W) \), \( W \) a finite-dimensional \( \mathbb{F}_p \)-vector space. Then there exists \( f \in M(\tau) \) such that
\[ \Phi(f) = a_T f \] 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 \( \tau' : G \to \text{GL}(W') \) such that \( \tau' \otimes \mathbb{F}_p = \tau \). Similarly, \( \Omega \) 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 \( M(\tau') \otimes \mathbb{F}_p \cong M(\tau) \). 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 3.25.** Suppose \( L/K \) is a finite Galois extension with Galois group \( G \) and \( V \) is a finite-dimensional vector space over \( L \). Let \( T \) 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 \( T \)-eigenvector \( v \) has system of eigenvalues \( \{ a_T : T \in T \} \), then for every \( \sigma \in G \) there exists an eigenvector \( v_\sigma \in V_K \) with system of eigenvalues \( \{ \sigma(a_T) : T \in T \} \).

Let’s 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 3.25.** The isomorphism \( \varphi \) of the next lemma induces an isomorphism of \( L \)-vector spaces

\[
\varphi : L \otimes_K V \to \bigoplus_{\sigma \in G} V_{e\sigma}
\]

\[
\alpha \otimes w \mapsto \sum_{\sigma \in G} \sigma(\alpha) w_{e\sigma}.
\]

Let \( v_\sigma := \varphi^{-1}(ve_{\sigma^{-1}}) \). 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 \( v_\sigma \) is an eigenvector of \( T \) with eigenvalue \( \sigma(a_T) \), and this holds for all \( T \in T \).

**Lemma 3.26.** 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 \( \varphi \) 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 \( \varphi \) is injective.

Let \( \{ \alpha_1, \ldots, \alpha_n \} \) be a basis of \( L \) as a \( K \)-vector space. Then \( \{ \alpha_i \otimes \alpha_j : 1 \leq i, j \leq n \} \) 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

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

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 \( i \)-th entry is \( \sum_j c_{ij} \alpha_j \). Then the system (10) can be written as \( Ac = 0 \). But it is an easy consequence of independence of characters (see Corollary VI.5.4 in [Lan93]) that \( A \in \text{GL}_n(L) \), therefore we must have \( c = 0 \), i.e.

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

Since the \( \alpha_j \) are linearly independent we conclude that \( c_{ij} = 0 \) for all \( i \) and \( j \), hence \( \varphi \) is injective. \( \Box \)
[Pat68] John Tate. Classes d’isogénie des variétés abéliennes sur un corps fini (d’après T. Honda). In Séminaire Bourbaki, 21e année, 1968/69, pages Exp. No. 352, 95–110. Soc. Math. France, Paris, 1968.

[Vig80] Marie-France Vigneras. Arithmétique des algèbres de quaternions, volume 800 of Lecture notes in mathematics. Springer, Berlin, 1980.

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139
E-mail address: aghitza@math.mit.edu