Siegel modular forms (mod p) and algebraic modular forms

by

Alexandru Edgar Ghitza

Bachelor of Science, Mathematics, McGill University, 1999

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2003

Author . . . . 05/05/2003 . . . .
Department of Mathematics
April 28, 2003

Certified by . . . . May 5 2003 . . . .
Aise Johan de Jong
Professor of Mathematics
Thesis Supervisor

Accepted by . . . .
Pavel I. Etingof
Chairman, Department Committee on Graduate Students

2

Siegel modular forms (mod p) and algebraic modular forms

by

Alexandru Edgar Ghitza

Submitted to the Department of Mathematics
on April 28, 2003, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

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 $\mathbb{A}_B^\times / B^\times \to \bar{\mathbb{F}}_p$, 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.

Thesis Supervisor: Aise Johan de Jong
Title: Professor of Mathematics

Acknowledgments

First and foremost I thank my advisor, Johan de Jong. His intoxicating enthusiasm is surpassed only by his vast knowledge and his uncanny ability to find the very best angle for attacking a problem. It was a pleasure and a privilege to be his student.

I thank Benedict Gross for suggesting this thesis problem and for taking the time to discuss it with me at various stages of its development. I thank Frans Oort for teaching me – both in person and through his works – about moduli spaces of abelian varieties and the supersingular and superspecial loci. I thank my defense committee members, Michael Artin and Catherine O'Neil, for speaking to me about my thesis and therefore helping me sort out some of the thornier aspects. I thank Kevin Buzzard, Alberto De Sole, Nora Ganter, Gerard van der Geer, Morten Honsen, Max Lieblich, Marc-Hubert Nicole, Brian Osserman, Thomas Shemanske, David Sheppard, Damiano Testa, David Vogan, and Yu Yasufuku for patiently answering my various questions and for not making (too much) fun of me for asking them. I thank Henri Darmon, Eyal Goren, and the rest of the Montreal number theory group for asking me to talk about my research on several occasions.

On a personal note, I thank my roommates Alberto, François, and Peter for their great friendship that made 17 Harvard Terrace into a real home. I thank Nora for her love and support. I thank my parents, Julieta and Gheorghe, for their love and encouragement that I will never be able to repay properly.

6

Contents

Chapter 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 ℓ

prime to pN, one defines the Hecke operator T_ℓ 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_ℓ, $\ell \nmid pN$. 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 adèles on quaternion algebras. More precisely, let B be the quaternion algebra ramified at p and ∞ and let $\mathbb{A}_B^\times$ denote the group of adèles on B. Serre proved the following

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

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

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

such that $\rho(\mathrm{Frob}_\ell)$ has trace b_ℓ and determinant ℓ^{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 $\mathbb{A}_B^\times / B^\times \to \overline{\mathbb{F}}_p$. 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

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

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 $G = B^\times$, $\hat{G} = \mathrm{GL}_2$, 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 $G = \mathrm{GU}_g(B) =$ 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 Chapter 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 chapter.

We attack the generalization to higher dimensions in Chapter 3. After recalling the definition of Siegel modular forms, we briefly discuss properties of superspecial abelian varieties and of the algebraic group $\mathrm{GU}_g(B)$. 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 (mod p) of dimension g, level N and any weight ρ, are the same as the systems of Hecke eigenvalues coming from algebraic modular forms (mod p) of level N and any weight ρ_S on the group $\mathrm{GU}_g(B)$.

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 occuring 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 $\mathrm{GU}_g(B)$.

Chapter 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 $0 : S \to E$:

$$
\begin{array}{c}
E \\
\pi \Big\downarrow \Big) 0 \\
S
\end{array}
$$

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 $\mathrm{R}^1 \pi_*(\mathcal{O}_E)$.

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 $\mathrm{Aut}((\mathbb{Z}/N\mathbb{Z})^2_S) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

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 $\#(\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm1\})$ 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 $\mathbb{P}^1_{\mathbb{Z}[\frac{1}{N}]}$ 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 ω on $X(N)$ whose restriction to $Y(N)$ is $\omega_{\mathcal{E}/Y(N)}$ and whose sections over the completion $\mathbb{Z}[\frac{1}{N}, \zeta_N][[q]]$ at each cusp are precisely the $\mathbb{Z}[\frac{1}{N}, \zeta_N][[q]]$ multiples of the canonical differential of the Tate curve. The *Kodaira-Spencer isomorphism*

$$\left(\omega_{\mathcal{E}/Y(N)}\right)^2 \cong \Omega^1_{Y(N)/\mathbb{Z}[\frac{1}{N}]}$$

extends to an isomorphism

$$\omega^2 \cong \Omega^1_{X(N)/\mathbb{Z}[\frac{1}{N}]}(\log(X(N) - Y(N))).$$

A *modular form (mod p) of level N and weight k* is a global section of ω^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:

$$M_k(N) = \mathrm{H}^0(X, \omega^k).$$

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_ℓ, $\ell \nmid pN$. On the level of sheaves, we define $\mathcal{S}_k$ by the following

$$0 \to \omega^{k-(p-1)} \xrightarrow{\times A} \omega^k \to \mathcal{S}_k \to 0.$$

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

We take global sections and get the exact sequence

$$0 \to W_k(N) \to S_k(N) \to \mathrm{H}^1(X, \omega^{k-(p-1)}) \to \mathrm{H}^1(X, \omega^k) \to 0.$$

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

An $\mathbb{F}_q$-*structure* on an elliptic curve $E/\overline{\mathbb{F}}_p$ is an elliptic curve $E'/\mathbb{F}_q$ 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

$$
\begin{array}{ccc}
E & \xrightarrow{\;[-p]\;} & E \\
 & \searrow{\scriptstyle \mathrm{Fr}^2} & \big\uparrow{\scriptstyle \sim} \\
 & & E^{(p^2)},
\end{array}
$$

where $E^{(p^2)}$ is obtained by raising to the power p^2 the coefficients of a Weierstrass equation for E and $\mathrm{Fr}^2 : E \to E^{(p^2)}$ is the morphism $[x : y : z] \mapsto [x^{p^2} : y^{p^2} : z^{p^2}]$. Since $E \cong E^{(p^2)}$ we have $j(E) = j\left(E^{(p^2)}\right) = j(E)^{p^2}$, 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

$$
\begin{array}{ccc}
E'' & \xrightarrow{\;[-p]\;} & E'' \\
 & \searrow{\scriptstyle \pi''} & \big\uparrow{\scriptstyle \sim}{\scriptstyle \lambda} \\
 & & E'',
\end{array}
$$

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

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

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

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

We recall that the action of $G_{\mathbb{F}_{p^2}}$ 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

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

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 $G_{\mathbb{F}_{p^2}}$, it is fixed by the whole group therefore it is defined over $\mathbb{F}_{p^2}$. $\qquad \square$

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 $\overline{\mathbb{F}}_p$-isomorphism classes of triples (E, α, η), 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, α, η) as $[E, \alpha, \eta]$.

On the other hand, fix a supersingular elliptic curve E_0 over $\overline{\mathbb{F}}_p$ and let $\mathcal{O} = \mathrm{End}(E_0)$, $B = \mathrm{End}^0(E_0) = \mathcal{O} \otimes \mathbb{Q}$. 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 ℓ^n, where $\ell^n \| N$. Let $\mathcal{O}_p^\times(1)$ be the kernel of the map $\mathcal{O}_p^\times \to \mathbb{F}_{p^2}^\times$ given by reduction modulo the uniformizer π 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

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

For $\ell \nmid pN$ we have Hecke operators T_ℓ acting on both $\Sigma(N)$ and $\Omega(N)$ (see §2.5.1 for the definition). The main technical result of this chapter (whose proof is the object of the next sections) is

Theorem 2.2. There exists a bijection $\Sigma(N) \cong \Omega(N)$ which is compatible with

- the action of the Hecke operators T_ℓ, $\ell \nmid pN$,

- the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$,

- raising the level N.

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

$$f([E, \alpha, \lambda\eta]) = \lambda^{-k} f([E, \alpha, \eta]) \qquad \forall \lambda \in \mathbb{F}_{p^2}^\times.$$

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

$$f(\lambda[x]) = \lambda^{-k} f([x]) \qquad \forall \lambda \in \mathcal{O}_p^\times / \mathcal{O}_p^\times(1) = \mathbb{F}_{p^2}^\times.$$

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

$$S_k(N) \xrightarrow{\sim} M_k(\Omega(N))$$

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 $\overline{\mathbb{F}}_p$ has a canonical $\mathbb{F}_{p^2}$-structure. Therefore the cotangent space $\omega(E)$ has a canonical $\mathbb{F}_{p^2}$-structure and $\omega^{p^2-1}(E)$ has a canonical $\mathbb{F}_{p^2}$-basis. Hence for any k we can identify $\omega^k(E)$ with $\omega^{k+p^2-1}(E)$, and $S_k(N)$ with $S_{k+p^2-1}(N)$. $\qquad\square$

Lemma 2.4. Every sequence (a_ℓ) 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_ℓ) 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_ℓ.

Conversely, if (a_ℓ) 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

$$M_k(N) \to S_k(N)$$

is surjective. We now use Proposition 1.2.2 of [AS86] to conclude that (a_ℓ) is given by some $f \in M_k(N)$. $\qquad\square$

Let k vary. We conclude that there is a bijection between the systems of eigenvalues coming from

$$M_*(N) := \bigoplus_k M_k(N)$$

and those coming from

$$M_*(\Omega(N)) := \bigoplus_{k \bmod (p^2-1)} M_k(\Omega(N)).$$

If we let N vary, we get

$$\bigoplus_N M_*(N) = \left\{ \text{functions} \bigcup_N \Omega(N) \to \overline{\mathbb{F}}_p \right\}.$$

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 $\overline{\mathbb{F}}_p$. 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 $\overline{\mathbb{F}}_p$-vector space V, and let T_ℓ be endomorphisms of V that commute with the action of G. Let (a_ℓ) be a system of eigenvalues of the T_ℓ 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

$$\rho : G \to \mathrm{GL}(V),$$

where $G = \varprojlim G_j$ has the profinite topology and $\mathrm{GL}(V)$ has the discrete topology. The kernel of ρ 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

ρ factors as in the following diagram:

$$\begin{array}{ccc} G & \xrightarrow{\quad \rho \quad} & \mathrm{GL}(V) \\ & \searrow{\scriptstyle \pi} \quad \nearrow{\scriptstyle \bar{\rho}} & \\ & \bar{G}, & \end{array}$$

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_ℓ, 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. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

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

$$G_0 \xrightarrow{i_0} G_1 \xrightarrow{i_1} \ldots \to G_n \xrightarrow{i_n} \ldots,$$

where for all n, G_n is a finite commutative group scheme of rank p^{hn}, i_n is a group homo-

morphism and the following sequence is exact:

$$0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{p^n} G_{n+1}.$$

This definition was tailored specifically so that $A[p^\infty] = (A[p^n])$ 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 $f : G \to H$ is a system of group scheme homomorphisms $f_n : G_n \to H_n$ such that the following diagram commutes for all $n \geq 1$:

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

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 $\sigma : W \to W$ 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 $\mathbb{W}_n$ denote the n-th Witt group scheme. If G is a commutative k-group scheme, we define its *Dieudonné module* by

$$M(G) := \varinjlim \operatorname{Hom}_{k\text{-gp}}(G, \mathbb{W}_n) \oplus \left(W(\bar{k}) \otimes_{\mathbb{Z}} \operatorname{Hom}_{\bar{k}\text{-gp}}(G_{\bar{k}}, (\mathbb{G}_m)_{\bar{k}}) \right)^{\operatorname{Gal}(\bar{k}/k)}.$$

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, $M(G) := \varprojlim M(G_n)$ 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 $M^* := \operatorname{Hom}_W(M, W)$ 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 π, 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 $0 \subsetneq Wx \subset M$ 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 πW 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 ϕ 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.

$$\square$$

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 τ is an automorphism of k, $T : k \to k$ is a τ-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 $\mathcal{A}$-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 = $ 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 $\tilde{K}$ 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 $\tilde{K}$.

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 $p^2 A^2 = 0 \neq -p$, 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 α_p. So we want to show that $E'[p]$ is not isomorphic to α_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 α_p^2 at the origin is twice the dimension of the tangent space to α_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 $\ker F = k m_1$ and pick $m_2 \in M$ such that $\{m_1, m_2\}$ is a basis of M, then $F = \left(\begin{smallmatrix} 0 & a_1 \\ 0 & a_2 \end{smallmatrix} \right) \sigma$. We impose $F^2 = 0$:

$$F^2 = \begin{pmatrix} 0 & a_1 a_2^p \\ 0 & a_2^{p+1} \end{pmatrix} \sigma^2 = 0 \Rightarrow a_2 = 0.$$

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

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

The Verschiebung is given a priori by some matrix

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

We impose $FV = VF = 0$:

$$\begin{aligned} FV &= \begin{pmatrix} b_{21}^p & b_{22}^p \\ 0 & 0 \end{pmatrix} = 0 \Rightarrow b_{21} = b_{22} = 0, \\ VF &= \left(\begin{smallmatrix} 0 & b_{11} \\ 0 & 0 \end{smallmatrix} \right) = 0 \Rightarrow b_{11} = 0. \end{aligned}$$

Therefore the matrix of V is of the form

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

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 λ. But we can find the actual value of λ by investigating $M_2 = M(E'[p^2])$.

The structure of $M(E'[p^n])$

We use Nakayama's lemma to lift the basis of k^2 to a basis of W_2^2. With respect to this basis the operators F and V look like

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

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

$$
\begin{aligned}
F^2 &= p\left(\begin{smallmatrix} a_{21}^p & a_{11}+a_{22}^p \\ 0 & a_{21} \end{smallmatrix}\right)\sigma^2 = -p\sigma^2 \Rightarrow a_{21} = -1, a_{11} = -a_{22}^p, \\
FV &= p\left(\begin{smallmatrix} b_{21}^p & b_{22}^p-\lambda^p a_{22}^p \\ 0 & -\lambda^p \end{smallmatrix}\right) = p \Rightarrow b_{21} = 1, \lambda = -1, a_{22} = -b_{22}, \\
VF &= p\left(\begin{smallmatrix} 1 & b_{22}^{1/p}+b_{11} \\ 0 & 1 \end{smallmatrix}\right) = p \Rightarrow b_{22} = -b_{11}^p.
\end{aligned}
$$

This implies that F and V are of the form

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

In particular,

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

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

$$I + pC, \quad \text{where } C = \left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{smallmatrix}\right) \in M_2(k).$$

The new matrix for the Frobenius will be

$$
\begin{aligned}
(I - p\left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{smallmatrix}\right))&\left(\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) + p\left(\begin{smallmatrix} -b_{11} & a_{12} \\ -1 & b_{11}^p \end{smallmatrix}\right)\right)\sigma(I + p\left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{smallmatrix}\right)) = \\
&= \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\sigma + p\left(\begin{smallmatrix} -b_{11}+c_{21}^p & a_{12}-c_{11}+c_{22}^p \\ -1 & b_{11}^p-c_{21} \end{smallmatrix}\right)\sigma.
\end{aligned}
$$

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

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

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

$$F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\sigma + p\begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}\sigma,$$
$$V = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}\sigma^{-1} + p\begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}\sigma^{-1},$$

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

$$F = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\sigma + p\begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}\sigma + p^2 A\sigma,$$
$$V = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}\sigma^{-1} + p\begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}\sigma^{-1} + p^2 B\sigma^{-1},$$

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

$$F^2 = p\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\sigma^2 + p^2\begin{pmatrix} a_{21}^p & a_{22}^p+a_{11} \\ 0 & a_{21} \end{pmatrix}\sigma^2 = -p\sigma^2 \Rightarrow a_{21} = 0, a_{11} = -a_{22}^p,$$
$$FV = p\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p^2\begin{pmatrix} b_{21}^p & b_{22}^p+a_{22}^p \\ 0 & \lambda^p \end{pmatrix} = p \Rightarrow b_{21} = 0, a_{22} = -b_{22}, \lambda = 0.$$

Therefore

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

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

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

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

$$
\begin{aligned}
F &= \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \sigma + p \left(\begin{smallmatrix} 0 & 0 \\ -1 & 0 \end{smallmatrix}\right) \sigma + p^n A \sigma, \\
V &= \left(\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}\right) \sigma^{-1} + p \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \sigma^{-1} + p^n B \sigma^{-1}.
\end{aligned}
$$

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

$$
\begin{aligned}
F^2 &= -p\sigma^2 + p^n \left(\begin{smallmatrix} a_{21}^p & a_{22}^p + a_{11} \\ 0 & a_{21} \end{smallmatrix}\right) \sigma^2 = -p\sigma^2 \Rightarrow a_{21} = 0, a_{11} = -a_{22}^p, \\
FV &= p + p^n \left(\begin{smallmatrix} b_{21}^p & b_{22}^p + a_{22}^p \\ 0 & 0 \end{smallmatrix}\right) = p \Rightarrow a_{22} = -b_{22}, a_{11} = b_{22}^p, b_{21} = 0, \\
VF &= p + p^n \left(\begin{smallmatrix} 0 & b_{22}^{1/p} + b_{11} \\ 0 & 0 \end{smallmatrix}\right) = p \Rightarrow b_{22} = -b_{11}^p,
\end{aligned}
$$

and conclude that

$$
A = \left(\begin{smallmatrix} -b_{11} & a_{12} \\ 0 & b_{11}^p \end{smallmatrix}\right), \quad B = \left(\begin{smallmatrix} b_{11} & b_{12} \\ 0 & -b_{11}^p \end{smallmatrix}\right).
$$

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

$$
(I - p^n \left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{smallmatrix}\right)) \left(\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) + p \left(\begin{smallmatrix} 0 & 0 \\ -1 & 0 \end{smallmatrix}\right) + p^n \left(\begin{smallmatrix} -b_{11} & a_{12} \\ 0 & b_{11}^p \end{smallmatrix}\right)\right) \sigma (I + p^n \left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{smallmatrix}\right)) =
$$

$$
= \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \sigma + p \left(\begin{smallmatrix} 0 & 0 \\ -1 & 0 \end{smallmatrix}\right) \sigma + p^n \left(\begin{smallmatrix} -b_{11} + c_{21}^p & a_{12} - c_{11} + c_{22}^p \\ 0 & b_{11}^p - c_{21} \end{smallmatrix}\right) \sigma.
$$

So if we let $c_{11} = a_{12} + c_{22}^p$ and $c_{21} = b_{11}^p$ then F is of the desired form.

The new matrix of the Verschiebung is

$$
\left(I - p^n \left(\begin{smallmatrix} a_{12} + c_{22}^p & c_{12} \\ b_{11}^p & c_{22} \end{smallmatrix}\right)\right) \left(\left(\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}\right) + p \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) + p^n \left(\begin{smallmatrix} b_{11} & b_{12} \\ 0 & -b_{11}^p \end{smallmatrix}\right)\right) \sigma^{-1} \left(I + p^n \left(\begin{smallmatrix} a_{12} + c_{22}^p & c_{12} \\ b_{11}^p & c_{22} \end{smallmatrix}\right)\right) =
$$

$$
= \left(\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}\right) \sigma^{-1} + p \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \sigma^{-1} + p^n \left(\begin{smallmatrix} 0 & \lambda \\ 0 & 0 \end{smallmatrix}\right) \sigma^{-1},
$$

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+1}^2 to W_{n+2}^2. Our operators are of the form

$$
\begin{aligned}
F &= \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\sigma + p\left(\begin{smallmatrix} 0 & 0 \\ -1 & 0 \end{smallmatrix}\right)\sigma + p^{n+1}A\sigma, \\
V &= \left(\begin{smallmatrix} 0 & -1 \\ 0 & 0 \end{smallmatrix}\right)\sigma^{-1} + p\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)\sigma^{-1} + p^n\left(\begin{smallmatrix} 0 & \lambda \\ 0 & 0 \end{smallmatrix}\right)\sigma^{-1} + p^{n+1}B\sigma^{-1}.
\end{aligned}
$$

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

$$
\begin{aligned}
F^2 &= -p\sigma^2 + p^{n+1}\left(\begin{smallmatrix} a_{21}^p & a_{22}^p + a_{11} \\ 0 & a_{21} \end{smallmatrix}\right)\sigma^2 = -p\sigma^2 \Rightarrow a_{21} = 0, a_{11} = -a_{22}^p, \\
FV &= p + p^{n+1}\left(\begin{smallmatrix} b_{21}^p & b_{22}^p + a_{22}^p \\ 0 & -\lambda^p \end{smallmatrix}\right) = p \Rightarrow b_{21} = 0, a_{22} = -b_{22}, \lambda = 0.
\end{aligned}
$$

This concludes the proof of the proposition. $\square$

A direct consequence of this is that

$$
M(E'[p^\infty]) = \left(W^2, F = \left(\begin{smallmatrix} 0 & 1 \\ -p & 0 \end{smallmatrix}\right)\sigma, V = \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)\sigma^{-1}\right).
$$

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

Corollary 2.11. Let $M = M(E'[p^\infty])$. Then $\operatorname{End}(M) = \mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$, where $\mathcal{O} = \operatorname{End}(E')$. 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 $g \in \operatorname{End}(M)$; 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

$$
\begin{aligned}
F \circ g &= \left(\begin{smallmatrix} 0 & 1 \\ -p & 0 \end{smallmatrix}\right)\sigma\left(\begin{smallmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{smallmatrix}\right) = \left(\begin{smallmatrix} g_{21}^p & g_{22}^p \\ -pg_{11}^p & -pg_{12}^p \end{smallmatrix}\right)\sigma, \\
g \circ F &= \left(\begin{smallmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -p & 0 \end{smallmatrix}\right)\sigma = \left(\begin{smallmatrix} -pg_{12} & g_{11} \\ -pg_{22} & g_{21} \end{smallmatrix}\right)\sigma.
\end{aligned}
$$

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

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

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

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

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

It remains to prove the last statement. Let $g = \left(\begin{smallmatrix} x & y \\ -py^p & x^p \end{smallmatrix} \right) \in \mathrm{End}(M)^\times = \mathcal{O}_p^\times$. Note that

$$M/FM = \left\{ \left(\begin{smallmatrix} 0 \\ a \end{smallmatrix} \right) + FM : a \in \mathbb{F}_{p^2} \right\}.$$

Let $\bar{x}$ be the reduction of x modulo π, then g restricts to multiplication by $\bar{x}^p$ on M/FM.

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

Corollary 2.12. Let E_1, E_2 be two supersingular elliptic curves over $\bar{\mathbb{F}}_p$ and let E_1', E_2' denote their canonical $\mathbb{F}_{p^2}$-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 $\lambda \in \mathbb{F}_{p^2}^\times$.

But then the matrix

$$\begin{pmatrix} \lambda^p & 0 \\ 0 & \lambda \end{pmatrix}$$

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

2.3.2   Local study of isogenies

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

$$B[\ell^n] \xrightarrow{\phi^\vee} A[\ell^n] \xrightarrow{\ell^{n-k}} A[\ell^n] \xrightarrow{d^{-1}} A[\ell^n].$$
$$\underbrace{\hspace{6cm}}_{f}$$

Note that

$$\phi \circ f = \phi \circ (d^{-1} \ell^{n-k} \phi^\vee) = (\deg \phi) d^{-1} \ell^{n-k} = \ell^n$$

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

$$f \circ \phi = (d^{-1}\ell^{n-k}\phi^\vee) \circ \phi = d^{-1}\ell^{n-k}(\deg \phi) = \ell^n,$$

so f factors as

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

$$f \downarrow \qquad \swarrow$$

$$K_{\ell,n}$$

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:

$$f(g(a)) = f(\phi(\ell^{-n}a)) = d^{-1}\ell^{n-k}\phi^\vee(\phi(\ell^{-n}a)) = d^{-1}\ell^{n-k}(\deg \phi)\ell^{-n}a = a,$$

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 ϕ is obtained by the usual argument from

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A[p^n] & \longrightarrow & A & \xrightarrow{\;p^n\;} & A & \longrightarrow & 0 \\
& & & & \phi\downarrow & & \phi\downarrow & & \\
0 & \longrightarrow & B[p^n] & \longrightarrow & B & \xrightarrow{\;p^n\;} & B & \longrightarrow & 0.
\end{array}
$$

Applying the Dieudonné functor M we get an exact sequence of left $\mathcal{A}$-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.

$\square$

Proposition 2.14. Let $\phi : A \to B$ be an isogeny of abelian varieties. For any prime $\ell \neq p$, ϕ 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 $\ell = p$, ϕ induces an injective 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 ϕ 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 $a_m = 0$. 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 $n \geq \mathrm{ord}_\ell \deg \phi$, the kernel $K_{\ell,n}$ of the restriction of ϕ to $A[\ell^n]$ is isomorphic to the cokernel $C_{\ell,n}$ of the same map. But for $n \geq \mathrm{ord}_\ell \deg \phi$ we have

$K_{\ell,n} = (\ker \phi)_{\ell}$, so in particular $C_{\ell,n}$ stabilizes. Therefore for $n \geq \operatorname{ord}_{\ell} \deg \phi$ we have

$$\operatorname{coker} T_{\ell}\phi = C_{\ell,n} \xrightarrow[\sim]{f} K_{\ell,n} = (\ker \phi)_{\ell},$$

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

$$
\begin{array}{ccccc}
\cdots \xrightarrow{p} M(B[p^3]) & \xrightarrow{p} & M(B[p^2]) & \xrightarrow{p} & M(B[p]) \\
{\scriptstyle M(\phi)} \downarrow & & {\scriptstyle M(\phi)} \downarrow & & {\scriptstyle M(\phi)} \downarrow \\
\cdots \xrightarrow{p} M(A[p^3]) & \xrightarrow{p} & M(A[p^2]) & \xrightarrow{p} & M(A[p])
\end{array}
$$

To show that $M(\phi)$ is injective, first note that $K_{p,n}$ is a subgroup scheme of $\ker \phi$ for all n. Since ϕ 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. $\qquad\square$

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

Lemma 2.15. Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$. Then a non-zero invariant differential on E defined over $\mathbb{F}_{p^2}$ is equivalent to a choice of 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 ω 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. $\square$

2.4 Construction of the bijection

Fix a supersingular elliptic curve E_0 over $\overline{\mathbb{F}}_p$ and let $\mathcal{O} = \mathrm{End}(E_0)$, $B = \mathrm{End}^0(E_0) = \mathcal{O} \otimes \mathbb{Q}$, $M_0 = M(E_0'[p^\infty])$, 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 ∞. 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, α_1, η_1), where E_1 is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$, $\alpha_1 : E_1[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ 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 $\overline{\mathbb{F}}_p$-isomorphism classes of triples (E_1, α_1, η_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, α_0, η_0) the set $\Sigma(N)$ can be identified with the set $\Sigma^0(N)$ of triples

$$\left(\phi_1 : E_0 \to E_1, \alpha_1 : E_1[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2, 0 \neq \eta_1 \in M_1/FM_1 \right),$$

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:

$$
\begin{array}{ccc}
E_1[N] & \xrightarrow{\;f\;} & E_2[N] \\
{\scriptstyle \alpha_1}\Big\downarrow{\scriptstyle \sim} & & {\scriptstyle \alpha_2}\Big\downarrow{\scriptstyle \sim} \\
(\mathbb{Z}/N\mathbb{Z})^2 & =\!=\!= & (\mathbb{Z}/N\mathbb{Z})^2.
\end{array}
\tag{2.1}
$$

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 ℓ^n, where $\ell^n \| N$. Let $\mathcal{O}_p^\times(1)$ be the kernel of the map $\mathcal{O}_p^\times \to \mathbb{F}_{p^2}^\times$ given by reduction modulo the uniformizer π 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

$$
\Omega(N) = U(1,N)\backslash \mathbb{A}_B^\times / B^\times.
$$

Since the level N is fixed throughout this section, we'll drop the reference to N and write simply Σ, Σ^0 and Ω for our finite sets. The purpose of the section is to exhibit a canonical bijection between Σ^0 and Ω.

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 $\mathrm{End}(T_\ell E_0) = \mathcal{O}_\ell := \mathcal{O} \otimes \mathbb{Z}_\ell$. 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

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

Set $x_\ell := k_{\ell,1}^{-1} \circ T_\ell \phi_1$, then $x_\ell \in \mathrm{End}(T_\ell E_0) = \mathcal{O}_\ell$. Note that x_ℓ is not necessarily invertible in $\mathcal{O}_\ell$! But it is nonzero, so $x_\ell \in B_\ell^\times$. 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 $\bar{k}_{\ell,1} : T_\ell E_0 \to T_\ell E_1$ be an isomorphism

extending $\alpha_1^{-1} \circ \alpha_0 : E_0[\ell^n] \to E_1[\ell^n]$. Let $u = (\tilde{k}_{\ell,1})^{-1} \circ k_{\ell,1} \in \mathrm{End}(T_\ell E_0)^\times = \mathcal{O}_\ell^\times$. Observe that u restricts to the identity on $E_0[\ell^n] = (T_\ell E_0)/\ell^n(T_\ell E_0)$, so actually $u \in \mathcal{O}_\ell^\times(N)$. 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 $[x_\ell] \in \mathcal{O}_\ell^\times(N)\backslash B_\ell^\times$. Moreover, $[x_\ell] = 1$ for all but finitely many ℓ.

We need to carry out the same program at the prime p. The isogeny $\phi_1 : E_0 \to E_1$ induces an injective 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 η_1 to η_0; by Corollary 2.11 $k_{p,1}$ is well-defined up to multiplication by $\mathcal{O}_p^\times(1)$. Set $x_p := M(\phi_1') \circ k_{p,1}^{-1} \in \mathrm{End}(M_0) = \mathcal{O}_p$, then we get $[x_p] \in \mathcal{O}_p^\times(1)\backslash B_p^\times$:

$$
\begin{array}{ccc}
M_1 & \xrightarrow{M(\phi_1')} & M_0 \\
& \searrow{\scriptstyle \sim}_{\ k_{p,1}} & \ \big\uparrow{\scriptstyle x_p} \\
& & M_0.
\end{array}
$$

So far, our construction associates to a triple $(\phi_1, \alpha_1, \eta_1)$ an element $[x] \in U(1,N)\backslash \mathbb{A}_B^\times$. 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

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

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

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

We can therefore write $\phi_1^{-1} = \hat{\phi}_1 \otimes \frac{1}{n}$ 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

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

$\square$

Therefore we cannot hope to get anything better than a map $\Sigma^0 \to U \backslash \mathbb{A}_B^{\times} / B^{\times}$. 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 (2.1) 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

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 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 $x = (x_v) \in \mathbb{A}_B^{\times}$. Let $\ell \neq p$. We have $x_\ell \in B_\ell^{\times} = \mathrm{End}(V_\ell E_0)^{\times}$, 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 $A_\ell \in \mathrm{GL}_2(\mathbb{Q}_\ell)$ which represents x_ℓ. 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 matrix corresponds to an endomorphism $y_\ell \in \mathrm{End}(T_\ell E_0)$ which is injective with finite cokernel C_ℓ. Let ℓ^k be the order of C_ℓ. Let K_ℓ be the kernel of the map induced by y_ℓ on

$E_0[\ell^k]$:

$$0 \to K_\ell \to E_0[\ell^k] \xrightarrow{y_\ell} E_0[\ell^k] \to C_\ell \to 0.$$

For $\ell = p$ we have $x_p \in B_p^\times = (\mathrm{End}(M_0) \otimes \mathbb{Q}_p)^\times$. 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 $a_i, b_j \in \mathrm{End}(M_0)$. 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 $y_p = a' + \pi b' \in \mathrm{End}(M_0)$. 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

$$M(E_0[p^k]) \xrightarrow{y_p} M(E_0[p^k]) \to C_p \to 0.$$

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

Since $x \in \mathbb{A}_B^\times$, $n_\ell = 0$ for all but finitely many ℓ. Therefore it makes sense to set $q := \prod \ell^{n_\ell} \in \mathbb{Q}^\times$ and $y := xq$; the ℓ-th component of y is precisely the y_ℓ above, and clearly $[x] = [y]$. Now set $K := \bigoplus K_\ell$, then K is a finite subgroup of E_0. So to the given $(x_v) \in \mathbb{A}_B^\times$ 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

$$
\begin{array}{ccccc}
0 \longrightarrow \ker \longrightarrow & E_0[\ell^m] & \xrightarrow{\phi} & (E_0/K)[\ell^m] \\
\| & \| & & \\
0 \longrightarrow \ker \longrightarrow & E_0[\ell^m] & \xrightarrow{y_\ell} & E_0[\ell^m].
\end{array}
$$

Due to the structure of ℓ^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

$$
\begin{array}{ccc}
0 \longrightarrow T_\ell E_0 & \xrightarrow{T_\ell \phi} & T_\ell(E_0/K) \\
\Big\| & & \Big\uparrow{\scriptstyle k_\ell} \wr \\
0 \longrightarrow T_\ell E_0 & \xrightarrow{y_\ell} & T_\ell E_0 .
\end{array}
$$

In particular, we can set $\alpha := \alpha_0 \circ k_\ell^{-1}$, then the isomorphisms $\alpha : (E_0/K)[\ell^n] \xrightarrow{\sim} (\mathbb{Z}/\ell^n \mathbb{Z})^2$ 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

$$
\begin{array}{ccccccc}
0 \longrightarrow & M & \xrightarrow{M(\phi)} & M_0 & \longrightarrow & \operatorname{coker} M(\phi) & \longrightarrow 0 \\
& \Big\downarrow{\scriptstyle k_p} \wr & & \Big\| & & \Big\downarrow \wr & \\
0 \longrightarrow & M_0 & \xrightarrow{y_p} & M_0 & \longrightarrow & C_p & \longrightarrow 0,
\end{array}
$$

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. δ is well-defined.

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

$$
\begin{array}{ccccccc}
0 \longrightarrow & T_\ell E_0 & \xrightarrow{y_\ell} & T_\ell E_0 & \longrightarrow & C_\ell & \longrightarrow 0 \\
& \Big\uparrow{\scriptstyle u} & & \Big\| & & \Big\uparrow{\scriptstyle v_\ell} & \\
0 \longrightarrow & T_\ell E_0 & \xrightarrow{\bar{y}_\ell} & T_\ell E_0 & \longrightarrow & \bar{C}_\ell & \longrightarrow 0.
\end{array}
$$

The snake lemma gives

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

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

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & K_\ell & \longrightarrow & E_0[\ell^k] & \xrightarrow{y_\ell} & E_0[\ell^k] & \longrightarrow & C_\ell & \longrightarrow & 0 \\
& & \big\uparrow g_\ell & & \big\uparrow u_\ell & & \big\| & & \big\uparrow v_\ell & & \\
0 & \longrightarrow & \bar{K}_\ell & \longrightarrow & E_0[\ell^k] & \xrightarrow{\bar{y}_\ell} & E_0[\ell^k] & \longrightarrow & \bar{C}_\ell & \longrightarrow & 0,
\end{array}
$$

where u_ℓ is the restriction of u to $E_0[\ell^k]$ and g_ℓ is the restriction of u to $\bar{K}_\ell$. Note that $\operatorname{coker}(u_\ell : T_\ell E_0 \to T_\ell E_0) = \operatorname{coker}(u : E_0[\ell^k] \to E_0[\ell^k])$. Since there's no snake lemma for diagrams of long exact sequences, we split the above diagram in two:

$$
\begin{array}{ccccccc}
0 \longrightarrow K_\ell \longrightarrow E_0[\ell^k] \longrightarrow E_0[\ell^k]/\ker y_\ell \longrightarrow 0 & \qquad & 0 \longrightarrow \operatorname{Im} y_\ell \longrightarrow E_0[\ell^k] \longrightarrow C_\ell \longrightarrow 0 \\
\big\uparrow g_\ell \quad \big\uparrow u_\ell \quad\quad \big\uparrow h_\ell & & \big\uparrow h_\ell \quad\quad \big\| \quad\quad \big\uparrow v_\ell \\
0 \longrightarrow \bar{K}_\ell \longrightarrow E_0[\ell^k] \longrightarrow E_0[\ell^k]/\ker \bar{y}_\ell \longrightarrow 0 & & 0 \longrightarrow \operatorname{Im} \bar{y}_\ell \longrightarrow E_0[\ell^k] \longrightarrow \bar{C}_\ell \longrightarrow 0,
\end{array}
$$

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

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

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

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

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

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

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & K & \longrightarrow & E_0 & \xrightarrow{\phi} & E_0/K & \longrightarrow & 0 \\
& & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle u} & & \uparrow{\scriptstyle f} & & \\
0 & \longrightarrow & \bar{K} & \longrightarrow & E_0 & \xrightarrow{\bar{\phi}} & E_0/\bar{K} & \longrightarrow & 0.
\end{array}
$$

We apply the snake lemma and get an exact sequence

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

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

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

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

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

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

Now suppose $\bar{x} = x\ell$, $\ell \neq p$ (the case $\ell = p$ is analogous, even easier). If $\ell' \nmid \ell p$, then $\bar{x}_{\ell'} = x_{\ell'}\ell$ and $\bar{y}_{\ell'} = y_{\ell'}\ell$. Multiplication by ℓ is an isomorphism of $T_{\ell'}E_0$, so it induces an isomorphism $\bar{K}_{\ell'} \cong K_{\ell'}$ by applying the same argument as before on the diagram:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & K_{\ell'} & \longrightarrow & E_0[\ell'^k] & \xrightarrow{y_{\ell'}} & E_0[\ell'^k] & \longrightarrow & C_{\ell'} & \longrightarrow & 0 \\
& & \uparrow{\scriptstyle g_{\ell'}}{\scriptstyle\sim} & & \uparrow{\scriptstyle \ell}{\scriptstyle\sim} & & \| & & \uparrow{\scriptstyle v_{\ell'}}{\scriptstyle\sim} & & \\
0 & \longrightarrow & \bar{K}_{\ell'} & \longrightarrow & E_0[\ell'^k] & \xrightarrow{\bar{y}_{\ell'}} & E_0[\ell'^k] & \longrightarrow & \bar{C}_{\ell'} & \longrightarrow & 0.
\end{array}
$$

Something similar occurs at p. If $\ell' = \ell$, we get $\bar{x}_\ell = x_\ell\ell$ and $\bar{y}_\ell = y_\ell$ so $\bar{K}_\ell = K_\ell$. We have an isomorphism $\bar{K} \cong K$ so $E_0/\bar{K} \cong E_0/K$. We need to check that this isomorphism is compatible with the level structures and the differentials. Let $\ell' \nmid \ell p$, then we have a diagram

$$
\begin{array}{ccccc}
& & \overset{\ell}{\overset{\sim}{\frown}} & & \\
T_{\ell'}(E_0/K) & \xleftarrow{\;\;k_{\ell'}\;\;} & T_{\ell'}E_0 & \xrightarrow{\;\;\bar{k}_{\ell'}\;\;} & T_{\ell'}(E_0/\bar{K}) \\
{\scriptstyle\alpha}\downarrow & & {\scriptstyle\alpha_0}\downarrow & & \downarrow{\scriptstyle\bar{\alpha}} \\
(\mathbb{Z}/\ell'^n\mathbb{Z})^2 & = & (\mathbb{Z}/\ell'^n\mathbb{Z})^2 & = & (\mathbb{Z}/\ell'^n\mathbb{Z})^2.
\end{array}
$$

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

It remains to check the local choices. C_ℓ (therefore K_ℓ) depends on the chosen isomorphism $T_\ell E_0 \cong \mathbb{Z}_\ell^2$, and this can change y_ℓ by multiplication by an element of $\mathcal{O}_\ell^\times(N)$. Suppose we have another such candidate $\bar{y}_\ell = u_\ell y_\ell$, then we would get a commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & T_\ell E_0 & \xrightarrow{y_\ell} & T_\ell E_0 & \longrightarrow & C_\ell & \longrightarrow & 0 \\
& & \| & & \uparrow{\scriptstyle u_\ell}{\scriptstyle\sim} & & \uparrow{\scriptstyle v_\ell}{\scriptstyle\sim} & & \\
0 & \longrightarrow & T_\ell E_0 & \xrightarrow{\bar{y}_\ell} & T_\ell E_0 & \longrightarrow & \bar{C}_\ell & \longrightarrow & 0,
\end{array}
$$

from which we conclude as before that $\bar{K}_\ell \cong K_\ell$ and $E_0/\bar{K} \cong E_0/K$. For the level N

structure, we have the diagram

$$
\begin{array}{ccccc}
(E_0/K)[\ell^n] & \xrightarrow{k_\ell^{-1}} & E_0[\ell^n] & \xrightarrow{\alpha_0} & (\mathbb{Z}/\ell^n\mathbb{Z})^2 \\
\downarrow{\scriptstyle \sim} & & \| & & \| \\
(E_0/\bar{K})[\ell^n] & \xrightarrow{(\bar{k_\ell})^{-1}} & E_0[\ell^n] & \xrightarrow{\alpha_0} & (\mathbb{Z}/\ell^n\mathbb{Z})^2
\end{array}
$$

with top arrow α and bottom arrow $\bar\alpha$.

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

$\square$

Lemma 2.18. The map γ is bijective with inverse δ.

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

$$
0 \to T_\ell E_0 \xrightarrow{T_\ell\phi} T_\ell(E_0/K) \to \operatorname{coker} T_\ell\phi \to 0.
$$

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

We have just proved

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

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 π 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 δ, in which case $C_p = 1$ so the degree of the resulting isogeny is prime to p. $\square$

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

2.5 Compatibilities

This final section of the chapter consists of the proof of the following result:

Theorem 2.22. The canonical bijection $\gamma : \Sigma^0(N) \to \Omega(N)$ is compatible with the action of the Hecke algebra, with the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, and with the operation of raising the level.

2.5.1 Hecke action

In this section ℓ 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

$$\mathrm{Comm}(H) := \{g \in G : g^{-1}Hg \sim H\}.$$

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

$$HgH = \bigsqcup_{j=1}^{s} x_j g H = \bigsqcup_{j=1}^{s} Hg y_j,$$

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 $G = \mathrm{GL}_2(\mathbb{Q}_\ell)$, $H = \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathcal{H}_\ell = \mathcal{H}(\mathrm{GL}_2(\mathbb{Q}_\ell), \mathrm{GL}_2(\mathbb{Z}_\ell))$. We call $\mathcal{H}_\ell$ the *local Hecke algebra* at ℓ.

Take an isogeny $\phi : E_1 \to E_2$ whose degree is a power of ℓ. 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 $g \in G = \mathrm{GL}_2(\mathbb{Q}_\ell)$. Since g is defined only up to changes of bases for $T_\ell E_1$ and $T_\ell E_2$, ϕ actually defines a double coset HgH, where $H = \mathrm{GL}_2(\mathbb{Z}_\ell)$. In this situation we say that ϕ 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 ℓ-part of the determinant of any representative of HgH. The action of $\mathcal{H}_\ell$ on Σ^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 α_C is defined by the diagram

$$
\begin{array}{ccc}
E[N] & \xrightarrow[\sim]{\psi_C} & (E/C)[N] \\
{\scriptstyle \alpha} \downarrow & & \downarrow {\scriptstyle \alpha_C} \\
(\mathbb{Z}/N\mathbb{Z})^2 & =\!\!=\!\!= & (\mathbb{Z}/N\mathbb{Z})^2.
\end{array}
\tag{2.2}
$$

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

$$
\begin{array}{ccc}
E[N] & \xleftarrow{\hat{\psi}_C} & (E/C)[N] \\
{\scriptstyle \alpha} \downarrow & & \downarrow {\scriptstyle \alpha_C} \\
(\mathbb{Z}/N\mathbb{Z})^2 & \!\!=\!\!=\!\!=\!\! & (\mathbb{Z}/N\mathbb{Z})^2.
\end{array}
\tag{2.3}
$$

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

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

The algebra $\mathcal{H}_\ell$ acts on Ω by acting on the component Hx_l 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

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

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

$$
\begin{array}{ccc}
T_{\ell'}E_0 & \xrightarrow{T_{\ell'}\phi} T_{\ell'}E \xrightarrow[\sim]{T_{\ell'}\psi_C} & T_{\ell'}(E/C). \\
{\scriptstyle x_{\ell'}} \downarrow & {\scriptstyle k_{\ell'}} \nearrow & \\
T_{\ell'}E_0 & {\scriptstyle \sim} &
\end{array}
$$

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

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

$$
\begin{array}{ccccc}
M_C & \xrightarrow[\sim]{M(\psi'_C)} & M & \xrightarrow{M(\phi')} & M_0 \\
 & & & \searrow{\scriptstyle k_p} & \uparrow{\scriptstyle x_p} \\
 & & & \searrow{\scriptstyle \sim} & \\
 & & & & M_0.
\end{array}
$$

Let's figure out what happens at ℓ. 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_ℓ, y_C induces a map $z_C : T_\ell E_0 \to T_\ell E_0$. We have a diagram

$$
\begin{array}{ccccc}
T_\ell E_0 & \xrightarrow{T_\ell \phi} & T_\ell E & \xrightarrow{T_\ell \psi_C} & T_\ell(E/C). \\
{\scriptstyle x_\ell}\downarrow & {\scriptstyle \sim}\nearrow{\scriptstyle k_\ell} & \downarrow{\scriptstyle y_C} & {\scriptstyle \sim}\nearrow{\scriptstyle k_C} & \\
T_\ell E_0 & & T_\ell E & & \\
{\scriptstyle z_C}\downarrow & {\scriptstyle \sim}\nearrow{\scriptstyle k_\ell} & & & \\
T_\ell E_0 & & & &
\end{array}
$$

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 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 $z : T_\ell E_0 \to T_\ell E_0$, and hence induces via k_ℓ a map $y : T_\ell E \to T_\ell E$. We use the same construction as in the definition of the map δ in §2.4 (pages 39 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.

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 E of type $Hg^{-1}H$. This defines a new element of Σ^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 $[x_C] := \gamma([\hat{\psi}_C^{-1} \circ \phi, \alpha_C, \eta_C])$. If $(\ell', p\ell) = 1$, we have a diagram

$$
\begin{array}{ccccc}
T_{\ell'}E_0 & \xrightarrow{T_{\ell'}\phi} & T_{\ell'}E & \xleftarrow[\sim]{T_{\ell'}\hat{\psi}_C} & T_{\ell'}(E/C). \\
{\scriptstyle x_{\ell'}}\downarrow & {\scriptstyle k_{\ell'}}\nearrow & & & \\
T_{\ell'}E_0 & \scriptstyle\sim & & &
\end{array}
$$

Since $(T_{\ell'}\hat{\psi}_C)^{-1} \circ k_{\ell'} : T_{\ell'}E_0 \to T_{\ell'}(E/C)$ is an isomorphism restricting to $\alpha_C^{-1} \circ \alpha_0$ (see diagram (2.3)), we get that $[x_{C,\ell'}] = [x_{\ell'}]$. The situation at p is similar and we have $[x_{C,p}] = [x_p]$.

What about ℓ? As before, we fix $x_\ell \in Hx_\ell$ and with it the 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 $y_C := T_\ell\hat{\psi}_C \circ k_C$. Via the identification k_ℓ, y_C induces a map $z_C : T_\ell E_0 \to T_\ell E_0$. We have a diagram

$$
\begin{array}{ccccc}
T_\ell E_0 & \xrightarrow{T_\ell\phi} & T_\ell E & \xleftarrow{T_\ell\hat{\psi}_C} & T_\ell(E/C). \\
{\scriptstyle x_\ell}\downarrow & {\scriptstyle\sim}\nearrow_{k_\ell} & {\scriptstyle y_C}\uparrow & {\scriptstyle\sim}\nearrow_{k_C} & \\
T_\ell E_0 & & T_\ell E & & \\
{\scriptstyle z_C}\uparrow & {\scriptstyle\sim}\nearrow_{k_\ell} & & & \\
T_\ell E_0 & & & &
\end{array}
$$

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

2.5.2 Action of $GL_2(\mathbb{Z}/N\mathbb{Z})$

Within this section we'll write G to denote $GL_2(\mathbb{Z}/N\mathbb{Z})$. The group G acts on Σ^0 as follows:

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

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

$$
\begin{aligned}
G &\xrightarrow{\sim} \prod_\ell \mathcal{O}_\ell^\times(N)\backslash\mathcal{O}_\ell^\times \\
g &\mapsto \prod_\ell \mathcal{O}_\ell^\times(N)(\alpha_0^{-1} \circ g \circ \alpha_0),
\end{aligned}
$$

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

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

Lemma 2.24. The bijection $\gamma : \Sigma^0 \to \Omega$ is compatible with the action of $G = GL_2(\mathbb{Z}/N\mathbb{Z})$.

Proof. Let $\left[\prod \mathcal{O}_\ell^\times(N)x_\ell\right] := \gamma([\phi, \alpha, \eta])$ and $\left[\prod \mathcal{O}_\ell^\times(N)x'_\ell\right] := \gamma(g \cdot [\phi, \alpha, \eta]) = \gamma([\phi, g \circ \alpha, \eta])$. Pick some $\ell \neq p$ and set $H := \mathcal{O}_\ell^\times(N)$; 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 $k_\ell : T_\ell E_0 \to T_\ell E$ 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 is thus precisely what we need in order to define $x'_\ell = (k'_\ell)^{-1} \circ T_\ell\phi$. By the definition of k'_ℓ we have

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

which is what we wanted to show. □

2.5.3   Raising the level

Suppose $N' = dN$ for some positive integer d. A level N' structure $\alpha' : E[N'] \to (\mathbb{Z}/N'\mathbb{Z})^2$ 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 $d : E[N'] \to E[N]$, and there is a natural surjection $\pi : (\mathbb{Z}/N'\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2$ given by reduction mod N. We want to define an isomorphism $\alpha : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ that completes the following square

$$
\begin{array}{ccc}
E[N'] & \xrightarrow{\ \underset{\sim}{\alpha'}\ } & (\mathbb{Z}/N'\mathbb{Z})^2 \\
{\scriptstyle d}\downarrow & & \downarrow{\scriptstyle \pi} \\
E[N] & \xdashrightarrow{\ \alpha\ } & (\mathbb{Z}/N\mathbb{Z})^2.
\end{array}
$$

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 $[\phi, \alpha', \eta] \mapsto [\phi, \alpha, \eta]$ gives a map

$$
\Sigma^0(N') \to \Sigma^0(N).
$$

There is a similar map on the Ω's. We only need to consider primes $\ell | N'$. Here we have $\mathcal{O}_\ell^\times(N') \subset \mathcal{O}_\ell^\times(N)$ so we get maps $\mathcal{O}_\ell^\times(N')\backslash B_\ell^\times \to \mathcal{O}_\ell^\times(N)\backslash B_\ell$, which can be put together to form

$$
\Omega(N') \to \Omega(N).
$$

We want to show that the bijection γ commutes with these maps. This is clear at primes $\ell \nmid N'$, so suppose ℓ is a prime divisor of N'; say $\ell^m \| N$ and $\ell^n \| N'$. 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 $k'_\ell : T_\ell E_0 \to T_\ell E$ is an isomorphism restricting to

$$
\begin{array}{ccc}
E_0[\ell^n] & \xrightarrow{\ \underset{\sim}{k'_\ell}\ } & E[\ell^n] \\
{\scriptstyle \alpha'_0}\downarrow{\scriptstyle \sim} & & {\scriptstyle \alpha'}\downarrow{\scriptstyle \sim} \\
(\mathbb{Z}/\ell^n\mathbb{Z})^2 & =\!=\!= & (\mathbb{Z}/\ell^n\mathbb{Z})^2.
\end{array}
$$

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

$$
\begin{array}{ccc}
E_0[\ell^m] & \xrightarrow{\;\;k'_\ell\;\;}_{\sim} & E[\ell^m] \\
\alpha'_0 \downarrow \wr & & \alpha \downarrow \wr \\
(\mathbb{Z}/\ell^m\mathbb{Z})^2 & =\!=\!= & (\mathbb{Z}/\ell^m\mathbb{Z})^2.
\end{array}
$$

But this means that k'_ℓ plays the role of the k_ℓ in the definition of x_ℓ, so

$$
\mathcal{O}_\ell^\times(N)x'_\ell = \mathcal{O}_\ell^\times(N)x_\ell.
$$

This is precisely what the map $\Omega(N') \to \Omega(N)$ looks like at ℓ, so we're done.

Chapter 3

Siegel modular forms

Following a suggestion of Gross, we generalize the results of the previous chapter 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 $\mathrm{GU}_g(B)$, 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

$$
\begin{array}{c}
A \\
\pi \Big\downarrow \Big\rangle 0 \\
S,
\end{array}
$$

whose (geometric) fibers are connected of dimension g.

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

Let $\phi : A \to B$ be an isogeny of abelian schemes over S. Cartier duality (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 λ 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, λ) 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:

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

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

$$
\begin{array}{c}
Y \\
\pi \downarrow \!\! \Big) \, 0 \\
\mathcal{A}_{g,N}
\end{array}
$$

be the corresponding universal abelian variety. Let $\mathbb{E} = 0^*(\Omega_{Y/\mathcal{A}_{g,N}})$; 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 $g_{ij} \in \mathrm{GL}_n(\mathcal{O}_X|_{U_i \cap U_j})$ satisfying the usual cocycle identities.

Now suppose we are given a rational linear representation $\rho : \mathrm{GL}_n \to \mathrm{GL}_m$. 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 $\rho(g_{ij}) \in \mathrm{GL}_m(\mathcal{O}_X|_{U_i \cap U_j})$. 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* ρ. It is obvious that $\mathcal{F} = \mathcal{F}_{\mathrm{std}}$, where $\mathrm{std} : \mathrm{GL}_n \to \mathrm{GL}_n$ is the standard representation.

The correspondence $\rho \mapsto \mathcal{F}_\rho$ is a covariant functor from the category of rational linear representations of 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 $\overline{\mathbb{F}}_p$. According to the Koecher principle, the Hodge bundle $\mathbb{E}$ extends uniquely to a locally free sheaf $\mathbb{E}$ on X.

Given a rational representation $\rho : \mathrm{GL}_g \to \mathrm{GL}_m$, the global sections of $\mathbb{E}_\rho$ are called

Siegel modular forms (mod p) of weight ρ and level N and they can be written

$$M_\rho(N) = \mathrm{H}^0(X, \mathbb{E}_\rho)$$

$$= \left\{ f : \{[A, \lambda, \alpha, \eta]\} \to \overline{\mathbb{F}}_p^m \,|\, f(A, \lambda, \alpha, M\eta) = \rho(M)^{-1} f(A, \lambda, \alpha, \eta), \forall M \in \mathrm{GL}_g(\overline{\mathbb{F}}_p) \right\},$$

where η 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*

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

If

$$\begin{array}{c} A \\ \pi \left\downarrow\right) 0 \\ S, \end{array}$$

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

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

The projection formula gives

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

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

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

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

$$\kappa : \mathcal{T}_S \to (\mathbb{E}_{A^t/S})^\vee \otimes_{\mathcal{O}_S} \mathbb{E}_{A/S}^\vee,$$

which after dualizing gives

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

Now suppose that $\lambda : A/S \to A^t/S$ is a principal polarization, i.e. an isomorphism. Then the pullback map $\lambda^* : \mathbb{E}_{A^t/S} \to \mathbb{E}_{A/S}$ is an isomorphism and we get a map

$$\mathbb{E}_{A/S}^{\otimes 2} \to \Omega_S^1.$$

This map factors through the projection map to $\mathrm{Sym}^2(\mathbb{E}_{A/S})$, and the resulting map

$$\mathrm{Sym}^2(\mathbb{E}_{A/S}) \to \Omega_S^1$$

is an isomorphism. In particular, in the notation of §3.1.1 we have a Hecke isomorphism $\mathbb{E}_{\mathrm{Sym}^2 \, \mathrm{std}} \cong \Omega_X^1$, where $X = \mathcal{A}_{g,N}^*$.

3.2 Superspecial abelian varieties

For a commutative group scheme X over a field K we define the *a-number* of X by

$$a(X) = \dim_K \mathrm{Hom}(\alpha_p, X).$$

If $K \subset L$ then $\dim_K \mathrm{Hom}(\alpha_p, X) = \dim_L \mathrm{Hom}(\alpha_p, X \otimes L)$ 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 $\overline{\mathbb{F}}_p$. Then A has a canonical $\mathbb{F}_{p^2}$-structure A', namely the one whose geometric Frobenius is $[-p]$. The correspondence $A \mapsto A'$ is functorial.

Proof. Let E be a supersingular elliptic curve over $\overline{\mathbb{F}}_p$, then $A \cong E^g$. By Lemma 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

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

The functoriality statement follows from the corresponding statement in Lemma 2.1. Since any superspecial abelian variety over $\overline{\mathbb{F}}_p$ 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 $\overline{\mathbb{F}}_p$. $\square$

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

3.2.1 Isogenies

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

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

i.e.

$$\phi^t \circ \lambda_2 \circ \phi = \lambda_1.$$

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

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

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

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

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

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

$$
\begin{aligned}
e_\ell^\alpha : T_\ell A \times T_\ell A & \to & \mathbb{Z}_\ell(1) \\
(a, a') & \mapsto & e_\ell(a, \alpha a').
\end{aligned}
$$

If α is a polarization then e_ℓ^α is an alternating (also called symplectic) form, i.e.

$$e_\ell^\alpha(a', a) = e_\ell^\alpha(a, a')^{-1}$$

for all $a, a' \in T_\ell A$. If $f : A \to B$ is a homomorphism, then

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

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

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

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

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

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

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:

$$
\begin{aligned}
M/FM \times M/FM &\to \mathbb{F}_{p^2} \\
(x, y) &\mapsto \langle x, y \rangle := e_p(x, Fy)^p \pmod{p}.
\end{aligned}
$$

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 $\bar{}$ 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

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

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 ∞, 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

$$
\begin{aligned}
\mathrm{U}_g(B) &= \{M \in \mathrm{GL}_g(B) : M^*M = I\}, \\
\mathrm{GU}_g(B) &= \{M \in \mathrm{GL}_g(B) : M^*M = \gamma(M)I, \gamma(M) \in F^\times\}.
\end{aligned}
$$

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

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

(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:

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

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

where $J_{2g} = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$.

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

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

$$\bar{A} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

therefore the adjoint of A is

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

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

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

then

$$P_1^t \tilde{J}_{2g} P_1 = \begin{pmatrix} & & & & & & & \ddots^{\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}} \\ & & & & & \begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix} & & \\ & & & & 1 & & & \\ & & & -1 & & & & \\ & & \begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix} & & & & & \\ & \iddots & & & & & & \\ \begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix} & & & & & & & \end{pmatrix},$$

respectively

$$P_1^t \tilde{J}_{2g} P_1 = \begin{pmatrix} & & & & & \ddots^{\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}} \\ & & & \begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix} & & \\ & & \begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix} & & & \\ & \iddots & & & & \\ \begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix} & & & & & \end{pmatrix}.$$

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 $\tilde{J}_{2g} = P J_{2g} P^t$ and

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

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

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

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

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

so $M \in \mathrm{GU}_g(M_2(K))$. Therefore $P^{-1} \mathrm{GU}_g(M_2(K)) P = \mathrm{GSp}_{2g}(K)$, as desired.

Since $B \otimes \bar{F} \cong M_2(\bar{F})$, we conclude that $\mathrm{GU}_g(B) \otimes \bar{F} \cong \mathrm{GSp}(\bar{F})$. □

3.2.4 Algebraic modular forms (mod p)

We give the definition of algebraic modular forms (mod p) on the group $G = \mathrm{GU}_g(B)$, where B is the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. 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 $\mathrm{O}(4g)$.

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

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

For $\ell \neq p$, we set

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

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

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

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

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

We know from Lemma 3.1 that a principally polarized superspecial abelian variety (A, λ) has a canonical $\mathbb{F}_{p^2}$-structure (A', λ'). 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/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 $\omega(A') \cong \omega(E'^g) \cong \omega(E')^g$. By Lemma 2.15 we know that

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

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

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

$\square$

Note that as we've seen in §3.2.1, the presence of a principal polarization λ' on an $\mathbb{F}_{p^2}$-abelian variety A' induces a hermitian form on the g-dimensional $\mathbb{F}_{p^2}$-vector space M/FM. We say that an invariant differential on A defined over $\mathbb{F}_{p^2}$ is an invariant differential on (A, λ) if it respects this hermitian structure. We can therefore conclude that

Corollary 3.6. Let (A, λ) be a principally polarized superspecial abelian variety over $\overline{\mathbb{F}}_p$, let (A', λ') be its canonical $\mathbb{F}_{p^2}$-structure and $M = M(A'[p^\infty])$. Then giving a basis of invariant differentials on (A, λ) defined over $\mathbb{F}_{p^2}$ is equivalent to giving a hermitian basis of M/FM over $\mathbb{F}_{p^2}$.

3.2.6   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 $M = M(E'[p^\infty]^g)$, 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

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

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 $\langle x, Fx \rangle = p^r \epsilon$ for some $r \in \mathbb{Z}$ and $\epsilon \in W \setminus pW$ with $\epsilon^\sigma = -\epsilon$; 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 $\langle x, Fx \rangle = \langle y, Fy \rangle = \langle x, Fy \rangle = \langle y, Fx \rangle = 0$.

Corollary 3.8. $M(E'[p^\infty]^g) \cong A_{1,1}^g$ 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 $M_0 \to M_0^t$ 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 $f_x = p^r y^t$, $f_{Fx} = p^{r+1}(Fy)^t$, $f_y = -p^r x^t$ and $f_{Fy} = -p^{r+1}(Fx)^t$. For instance

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

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

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

Corollary 3.9. There exists an isomorphism $\mathrm{End}(M, e_0)^\times \cong \mathrm{GU}_g(\mathcal{O}_p)$, such that the subgroup of symplectic automorphisms which lift the identity map on $(M/FM, e_0)$ is identified with U_p defined by the short exact sequence

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

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

Proof. Recall the identification $\mathrm{End}(A_{1,1}) \cong \mathcal{O}_p$ from the proof of Corollary 2.11:

$$\begin{aligned} \varphi : \mathrm{End}(A_{1,1}) &\to \mathcal{O}_p \\ \begin{pmatrix} x & y \\ -py^p & x^p \end{pmatrix} &\mapsto x + \pi y. \end{aligned}$$

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

$$T_{ij} = \begin{pmatrix} x_{ij} & y_{ij} \\ -py_{ij}^p & x_{ij}^p \end{pmatrix}.$$

Therefore we have an isomorphism

$$\begin{aligned} \varphi : \mathrm{End}(M)^\times &\to \mathrm{GL}_g(\mathcal{O}_p) \\ T = (T_{ij})_{i,j} &\mapsto (x_{ij} + \pi y_{ij})_{i,j}. \end{aligned}$$

We want to prove that under this isomorphism, $\mathrm{End}(M, e_0)^\times$ corresponds to $\mathrm{GU}_g(\mathcal{O}_p)$. For this we use Corollary 3.8, which says that the bilinear form e_0 is given by the block-diagonal

matrix

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

Therefore we have

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

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

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

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

$$T \in \operatorname{End}(M, e_0)^\times \iff E_0^{-1} T^t E_0 T = \gamma \iff \varphi(T)^* \varphi(T) = \gamma \iff \varphi(T) \in \operatorname{GU}_g(\mathcal{O}_p),$$

which is precisely what we wanted to show.

For the second part of the statement note that

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

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

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

where $\bar{x}_{ij}$ denotes the reduction modulo π of x_{ij}. Therefore T induces the identity map on

M/FM if and only if

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

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

3.3   Construction of the bijection

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

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

$$(3.1)$$

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

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

Lemma 3.10. Given any principal polarization λ on A, there exists an isogeny of principally polarized abelian varieties $\phi : (A, \lambda_0) \to (A, \lambda)$.

Proof. We want an isogeny $\phi : A \to A$ such that

$$\phi^t \circ \lambda \circ \phi = m\lambda_0$$

for some $m \in \mathbb{N}$.

There is an obvious bijective correspondence associating to a homomorphism $\psi : A \to A$ a matrix $\Psi \in M_g(\mathcal{O})$. Under this bijection, $\psi^t : A^t \to A^t$ corresponds to the adjoint Ψ^*. If $\phi : A \to A$ is an isogeny, then $\Phi \in \mathrm{GL}_g(B)$. If $\lambda : A \to A^t$ is a polarization, then $\lambda^t = \lambda$ so $\Lambda^* = \Lambda$. Also Λ is positive-definite. If λ is a principal polarization, then $\Lambda \in \mathrm{GL}_g(\mathcal{O})$ defines a positive-definite quaternion hermitian form f. By Proposition 3.2 we know that Λ can be diagonalized, i.e. there exists $M \in \mathrm{GL}_g(B)$ such that

$$M^{-1}\Lambda M = \mathrm{diag}(\alpha_1, \ldots, \alpha_g),$$

with $\alpha_i \in \mathbb{Q}$. The form f is positive-definite so $\alpha_i \in \mathbb{Q}_{>0}$. But the norm theorem 3.3 says that the norm map is surjective onto $\mathbb{Q}_{>0}$, so by the last part of Proposition 3.2 there exists $M' \in \mathrm{GL}_g(B)$ such that

$$(M')^{-1}\Lambda M' = I.$$

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

$$\phi^t \circ \lambda \circ \phi = n^2.$$

$\square$

We can now mimic our approach from Chapter 2. Lemma 3.10 allows us to identify $\tilde{\Sigma}$ with the set $\tilde{\Sigma}^0$ 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 (3.1).

Proposition 3.11. An isogeny $\phi_1 : (A, \lambda_0) \to (A, \lambda_1)$ defines for any prime $\ell \neq p$ an element $[x_\ell] \in U_\ell(N) \backslash G_\ell$. If $\ell \nmid \deg \phi_1$ then $[x_\ell] = 1$.

Proof. Pick a prime $\ell \neq p$ and let n satisfy $\ell^n \| N$. As we've seen in §3.2.1, ϕ induces an injective symplectic similitude $T_\ell \phi_1 : (T_\ell A, e_\ell^{\lambda_0}) \to (T_\ell A, e_\ell^{\lambda_1})$, with finite cokernel isomorphic to $(\ker \phi_1)_\ell$. To ease notation, we'll just write e_0 for $e_\ell^{\lambda_0}$ and e_1 for $e_\ell^{\lambda_1}$ (and we use the same letters for the corresponding Weil pairings on $A[\ell^n]$).

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

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

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

$$
\begin{array}{ccc}
(T_\ell A, e_0) & \xrightarrow{T_\ell \phi_1} & (T_\ell A, e_1) \\
x_\ell \downarrow & \nearrow{\scriptstyle k_{\ell,1}} & \\
(T_\ell A, e_0). & &
\end{array}
\tag{3.2}
$$

The map x_ℓ 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. $x_\ell \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) = G_\ell$. If $\ell \nmid \deg \phi$ then $T_\ell \phi$ is a symplectic isomorphism so we can take $x_\ell = 1$.

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

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

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

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

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

with finite cokernel. Let $k_{p,1} : (M, e_1) \to (M, e_0)$ be a symplectic isomorphism whose reduction $(M/FM, e_1) \to (M/FM, e_0)$ maps η_1 to η_0. Set $x_p := M(\phi_1') \circ k_{p,1}^{-1}$, then the map $x_p : (M, e_0) \to (M, e_0)$ is an injective symplectic similitude with finite cokernel. Hence x_p induces a symplectic isomorphism of $(M \otimes \mathbb{Q}_p, e_0)$, so by Corollary 3.9, x_p gives an element of $\mathrm{GU}_g(B_p)$. Since $k_{p,1}$ is well-defined up to multiplication by U_p, we have that ϕ_1 defines a element $[x_p] \in U_p \backslash \mathrm{GU}_g(B_p)$.

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

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

$$\phi_1^t \circ \lambda_1 \circ \phi_1 = m\lambda_0,$$
$$\tilde{\phi}_1^t \circ \lambda_1 \circ \tilde{\phi}_1 = \tilde{m}\lambda_0.$$

We treat ϕ_1, $\tilde{\phi}_1$ as quasi-isogenies, i.e. elements of $\mathrm{End}(A) \otimes \mathbb{Q}$. Let $n = \deg \phi_1$, then

we have that as quasi-isogenies:

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

We can therefore write $\phi_1^{-1} = \hat{\phi}_1 \otimes \frac{1}{n}$ and we'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

$$u = \phi_1^{-1} \circ \tilde{\phi}_1 \in (\mathrm{End}(A) \otimes \mathbb{Q})^{\times}.$$

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

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

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

The next lemma says that we have indeed constructed a map

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

Lemma 3.13. The map γ is well-defined.

Proof. We need to show that γ only depends on the isomorphism class $[\phi_1, \alpha_1, \eta_1]$. Suppose $f : (\phi_1, \alpha_1, \eta_1) \to (\phi_2, \alpha_2, \eta_2)$ is an isomorphism of triples. By Lemma 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

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 ϕ_1. The exact same thing happens at the prime p. $\square$

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

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

For $\ell = p$ we have $x_p \in \mathrm{GU}_g(B_p) = (\mathrm{End}(M, e_0) \otimes \mathbb{Q}_p)^\times$. Write $x_p = a + \pi b$, where $a, b \in M_g(L_p)$ and $\pi^2 = -p$. We have

$$a = \sum_i a_i \otimes \frac{1}{p^i},$$
$$b = \sum_j b_j \otimes \frac{1}{p^j}.$$

with $a_i, b_j \in \mathrm{End}(M, e_0)$. Let $n_p \in \mathbb{Z}$ be the smallest integer such that

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

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

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

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

Since $x \in G(\hat{\mathbb{Q}})$, $n_\ell = 0$ for all but finitely many ℓ. Therefore it makes sense to set $q := \prod \ell^{n_\ell} \in \mathbb{Q}^\times$ and $y := xq$; the ℓ-th component of y is precisely the y_ℓ 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 λ on A such that ϕ is an isogeny of polarized abelian varieties. For $\ell \neq p$, our construction gives for any positive integer m

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

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

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

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

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

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

For $\ell = p$ we have similarly

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

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

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

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

Proposition 3.14. The map δ is well-defined.

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

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

The snake lemma gives

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

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

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

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

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & K_\ell & \longrightarrow & (A[\ell^k], e_0) & \longrightarrow & (A[\ell^k], e_0)/\ker y_\ell & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle g_\ell} & & \uparrow{\scriptstyle u_\ell} & & \uparrow{\scriptstyle h_\ell} & & \\
0 & \longrightarrow & \bar{K}_\ell & \longrightarrow & (A[\ell^k], e_0) & \longrightarrow & (A[\ell^k], e_0)/\ker \bar{y}_\ell & \longrightarrow & 0,
\end{array}
\tag{3.3}
$$

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \text{Im}\, y_\ell & \longrightarrow & (A[\ell^k], e_0) & \longrightarrow & C_\ell & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle h_\ell} & & \| & & \uparrow{\scriptstyle v_\ell} & & \\
0 & \longrightarrow & \text{Im}\, \bar{y}_\ell & \longrightarrow & (A[\ell^k], e_0) & \longrightarrow & \bar{C}_\ell & \longrightarrow & 0,
\end{array}
\tag{3.4}
$$

where I have taken the liberty of using the same label h_ℓ for two maps which are canonically

isomorphic. We first apply the snake lemma to diagram 3.4 and get

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

Using this information together with the snake lemma in diagram 3.3 gives

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

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

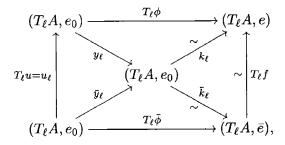Let $g = \bigoplus g_\ell : \bar{K} \to K$ and let $f : (A, \bar{\lambda}) \to (A, \lambda)$ be defined by the diagram

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

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

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

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

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

$$
\begin{array}{ccc}
(T_\ell A, e_0) & \xrightarrow{\quad T_\ell \phi \quad} & (T_\ell A, e) \\
\big\uparrow{\scriptstyle T_\ell u = u_\ell} & \underset{y_\ell}{\searrow} \quad (T_\ell A, e_0) \quad \underset{k_\ell}{\nearrow}{\scriptstyle \sim} & \sim \big\uparrow{\scriptstyle T_\ell f} \\
 & \underset{\bar{y}_\ell}{\nearrow} \qquad \underset{\bar{k}_\ell}{\searrow}{\scriptstyle \sim} & \\
(T_\ell A, e_0) & \xrightarrow{\quad T_\ell \bar{\phi} \quad} & (T_\ell A, \bar{e}),
\end{array}
$$

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

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

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

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

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

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

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

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

Since the top "triangle" commutes, we see that the level structures commute with the

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

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

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

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

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

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

Lemma 3.15. The map γ is bijective with inverse δ.

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

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

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

We have just proved

Theorem 3.16. There is a canonical bijection $\tilde{\Sigma}^0 \to \Omega$.

3.4 Compatibilities

We now turn to the proof of the following result:

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

3.4.1 Hecke action

In this section ℓ 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 ℓ-*isogeny* if its degree is a power of ℓ. Such ϕ induces a symplectic similitude

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

which gives an element $g \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$. Since g is defined only up to changes of symplectic bases for $T_\ell A_1$ and $T_\ell A_2$, ϕ actually defines a double coset HgH, where $H = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. We say that ϕ is *of type* HgH. If C is a finite ℓ-subgroup of an abelian variety A and λ is a principally polarization on A, there exists a principal polarization λ_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.

Since $(\mathrm{GSp}_{2g}(\mathbb{Q}_\ell), \mathrm{GSp}_{2g}(\mathbb{Z}_\ell))$ 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 $G = \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ and $H = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$.

If $HgH \in \mathcal{H}_\ell$, we denote by $\det(HgH)$ the ℓ-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 $[(A, \lambda_0) \xrightarrow{\phi} (A, \lambda), \alpha, \eta] \in \tilde{\Sigma}^0$. The abelian variety A/C is also superspecial, so it can be identified with A. We denote by ψ_C the composition $A \to A/C \cong A$, and we denote by λ_C the principal polarization induced on the image A. We set

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

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

$$
\begin{array}{ccc}
(A[N], e) & \xrightarrow[\sim]{\psi_C} & (A[N], e_C) \\
{\scriptstyle \alpha} \downarrow & & \downarrow {\scriptstyle \alpha_C} \\
((\mathbb{Z}/N\mathbb{Z})^{2g}, \mathrm{std}) & =\!=\!= & ((\mathbb{Z}/N\mathbb{Z})^{2g}, \mathrm{std}).
\end{array}
\tag{3.5}
$$

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

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

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

The action is defined by

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

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

$$(A[N], e) \xleftarrow[\sim]{\hat{\psi}_C} (A[N], e_C) \qquad (3.6)$$

$$\alpha \downarrow \qquad\qquad\qquad \alpha_C \downarrow$$

$$((\mathbb{Z}/N\mathbb{Z})^{2g}, \text{std}) =\!=\!= ((\mathbb{Z}/N\mathbb{Z})^{2g}, \text{std}).$$

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

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

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

Lemma 3.18. The bijection $\gamma : \bar{\Sigma}^0 \to \Omega$ 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

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

Proof. Let $HgH \in \mathcal{H}_\ell$, 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

$$(T_{\ell'}A, e_0) \xrightarrow{T_{\ell'}\phi} (T_{\ell'}A, e) \xrightarrow[\sim]{T_{\ell'}\psi_C} (T_{\ell'}A, e_C).$$

$$x_{\ell'} \downarrow \quad\nearrow{\scriptstyle k_{\ell'}}_{\sim}$$

$$(T_{\ell'}A, e_0)$$

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

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

$$(M, e_C) \xrightarrow[\sim]{M(\psi'_C)} (M, e) \xrightarrow{M(\phi')} (M, e_0)$$

$$(M, e_0).$$

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

$$(T_\ell A, e_0) \xrightarrow{T_\ell \phi} (T_\ell A, e) \xrightarrow{T_\ell \psi_C} (T_\ell A, e_C).$$

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

It remains to show that the map $C \mapsto Hz_C$ gives a bijection between the set of subgroups C of A of type HgH and the set of right cosets Hz contained in HgH. We start by constructing an inverse map. Let $Hz \subset HgH$ and pick a representative z. This corresponds to a map $z : (T_\ell A, e_0) \to (T_\ell A, e_0)$, and hence induces via k_ℓ a map $y : (T_\ell A, e) \to (T_\ell A, e)$. We use the same construction as in the definition of the inverse map δ in §3.3 (pages 77 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 $C \mapsto z_C$ 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 $\tilde{\Sigma}^0$ which we denote by $[\hat{\psi}_C^{-1} \circ \phi, \alpha_C, \eta_C]$ (by a slight abuse of notation since $\hat{\psi}_C$ is not invertible as an isogeny). Let $[x_C] := \gamma([\hat{\psi}_C^{-1} \circ \phi, \alpha_C, \eta_C])$. If $(\ell', p\ell) = 1$, we have a diagram

$$(T_{\ell'}A, e_0) \xrightarrow{T_{\ell'}\phi} (T_{\ell'}A, e) \xleftarrow[\sim]{T_{\ell'}\hat{\psi}_C} (T_{\ell'}A, e_C).$$

$$x_{\ell'} \downarrow \quad \overset{k_{\ell'}}{\underset{\sim}{\nearrow}}$$

$$(T_{\ell'}A, e_0)$$

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

What about ℓ? As before, we fix $x_\ell \in Hx_\ell$ and with it the symplectic isomorphism $k_\ell : (T_\ell A, e_0) \to (T_\ell A, e)$. Choose a symplectic isomorphism $k_C : (T_\ell A, e) \to (T_\ell A, e_C)$ and set $y_C := T_\ell\hat{\psi}_C \circ k_C$. Via the identification k_ℓ, y_C induces a map $z_C : (T_\ell A, e_0) \to (T_\ell A, e_0)$. We have a diagram

$$(T_\ell A, e_0) \xrightarrow{T_\ell\phi} (T_\ell A, e) \xleftarrow{T_\ell\hat{\psi}_C} (T_\ell A, e_C).$$

$$x_\ell \downarrow \quad \overset{\sim}{\underset{k_\ell}{\nearrow}} \quad \uparrow y_C \quad \overset{\sim}{\underset{k_C}{\nearrow}}$$

$$(T_\ell A, e_0) \qquad\qquad (T_\ell A, e)$$

$$z_C \uparrow \quad \overset{\sim}{\underset{k_\ell}{\nearrow}}$$

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

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

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

Within this section we'll write G to denote $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$. The group G acts on $\tilde{\Sigma}^0$ as follows:

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

The action on Ω is more delicate. It is easy to see that since $U_\ell = \mathrm{Aut}(T_\ell A, e_0)$, we have $U_\ell(N)\backslash U_\ell = \mathrm{Aut}(A[\ell^n], e_0)$, where $\ell^n\|N$. Our fixed symplectic isomorphism

$$\alpha_0 : (A[N], e_0) \to ((\mathbb{Z}/N\mathbb{Z})^{2g}, \mathrm{std})$$

identifies G with $\mathrm{Aut}(A[N], e_0)$ via $g \mapsto \alpha_0^{-1} \circ g \circ \alpha_0$. Therefore we get an identification

$$
\begin{aligned}
G &\xrightarrow{\sim} \prod_\ell U_\ell(N)\backslash U_\ell \\
g &\mapsto \prod_\ell U_\ell(N)(\alpha_0^{-1} \circ g \circ \alpha_0),
\end{aligned}
$$

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

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

Lemma 3.19. The bijection $\gamma : \tilde{\Sigma}^0 \to \Omega$ is compatible with the action of $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$.

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

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

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'_ℓ we have

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

which is what we wanted to show. □

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

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

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 π respect the symplectic structure, α is a symplectic isomorphism. We conclude that $[\phi, \lambda, \alpha', \eta] \mapsto [\phi, \lambda, \alpha, \eta]$ gives a map

$$\tilde{\Sigma}^0(N') \to \tilde{\Sigma}^0(N).$$

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

$$\Omega(N') \to \Omega(N).$$

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

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

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

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

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

3.5   Restriction to the superspecial locus

Let V be an $\overline{\mathbb{F}}_p$-vector space and let $\rho : \mathrm{GU}_g(\mathbb{F}_{p^2}) \to \mathrm{GL}(V)$ be a representation. A *superspecial modular form*[1] of weight ρ and level N is a function $f : \Sigma \to V$ satisfying

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

---

[1] This is not standard terminology.

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

$$S_{\rho \otimes \tau} = S_\rho \otimes S_\tau.$$

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

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

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

$$0 \to \mathrm{H}^0(X, \mathcal{I} \otimes \mathbb{E}_\rho) \to \mathrm{H}^0(X, \mathbb{E}_\rho) \to \mathrm{H}^0(X, i_* \mathcal{O}_\Sigma \otimes \mathbb{E}_\rho) = \mathrm{H}^0(\Sigma, i^* \mathbb{E}_\rho) \to \mathrm{H}^1(X, \mathcal{I} \otimes \mathbb{E}_\rho).$$

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

$$0 \to \mathrm{H}^0(X, \mathcal{I} \otimes \mathbb{E}_\rho) \to M_\rho(N) \xrightarrow{r} S_{\mathrm{Res}\,\rho} \to H^1(X, \mathcal{I} \otimes \mathbb{E}_\rho),$$

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

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 $\mathrm{Spec}\,A$. Let $\mathcal{G}$ be a coherent sheaf on X. Then

(a) for each $i \geq 0$, $\mathrm{H}^1(X, \mathcal{G})$ 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 $n \geq n_0$

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

Let $\omega = \Lambda^g \mathbb{E} = \mathbb{E}_{\det}$; it is an ample invertible sheaf (see Theorem V.2.5 in [FC90]).

Then for $n \gg 0$ we have

$$\mathrm{H}^1(X, (\mathcal{I} \otimes \mathbb{E}_\rho) \otimes \omega^n) = 0,$$

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

$$r : M_{\rho \otimes \det^n}(N) \to S_{\mathrm{Res}(\rho \otimes \det^n)}.$$

3.5.1   Lifting weights

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

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

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

We now extend this to

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

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

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

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

$$
\mathbb{G}_m(\mathbb{F}_q) \quad \to \quad \mathrm{GL}(V)
$$
$$
\lambda \quad \mapsto \quad \begin{pmatrix} \lambda^{a_1} & & \\ & \ddots & \\ & & \lambda^{a_n} \end{pmatrix}
$$

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 $A \in \mathrm{SL}_g(\mathbb{F}_{p^2})$, then the fact that $\rho_s(A)$ commutes with $\rho_m(\lambda)$ forces A to have the same shape as $\rho_m(\lambda)$ (i.e. it is block-diagonal with blocks of the same dimensions as $\rho_m(\lambda)$). Since this holds for all $A \in \mathrm{SL}_g(\mathbb{F}_q)$, we conclude that as an $\mathrm{SL}_g(\mathbb{F}_q)$-module, V has a direct sum decomposition

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

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 invariant under both $\mathrm{SL}_g(\mathbb{F}_q)$ and $\mathbb{G}_m(\mathbb{F}_q)$, contradicting the hypothesis that V is an irreducible representation of $\mathrm{GL}_g(\mathbb{F}_q)$. So $\mathbb{G}_m(\mathbb{F}_q)$ acts by scalars on V, say $\rho_m(\lambda)v = \lambda^a v$ for some $a \in \mathbb{Z}/(q-1)\mathbb{Z}$.

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

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

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

tion

$$\bar{\rho} : \mathrm{GL}_g(\overline{\mathbb{F}}_p) \;\;\to\;\; \mathrm{GL}(V)$$
$$M \;\;\mapsto\;\; \bar{\rho}_m(\det M) \cdot \bar{\rho}_s\left((\det M)^{-1}M\right).$$

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

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

Consider the linear transformation $\bar{\rho}_s(\zeta)$. It is diagonalizable if and only if its minimal polynomial has distinct roots. But the transformation satisfies $X^g - 1 = 0$, which has distinct roots, and hence the minimal polynomial will also have distinct roots. So we can choose a basis for V such that $\bar{\rho}_s(\zeta)$ is diagonal. If it has at least two distinct diagonal entries, we can apply the same argument as before to conclude that since it commutes with all of $\bar{\rho}_s(\mathrm{SL}_g(\overline{\mathbb{F}}_p))$ the representation $\bar{\rho}_s$ is reducible, which is a contradiction. So

$$\bar{\rho}_s(\zeta) = \zeta^b, \qquad \text{for some } b \in \mathbb{Z}/g\mathbb{Z}.$$

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

$$(\zeta^b)^m = \bar{\rho}_s(\zeta^m) = \bar{\rho}_m(\zeta^m) = (\zeta^m)^{\bar{a}}.$$

This implies that $m\bar{a} \equiv mb$ (mod g), i.e. $\bar{a} \equiv b$ (mod d). Since $d = (g, q-1)$ and $d|(\bar{a} - b)$

there exist integers u, v such that $\bar{a} - b = ug + v(q-1)$ and therefore

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

which is what we wanted. □

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

Corollary 3.23. Given an irreducible representation $\tau : \mathrm{GU}_g(\mathbb{F}_{p^2}) \to \mathrm{GL}(W)$, there exists an irreducible rational representation $\bar{\rho} : \mathrm{GL}_g(\overline{\mathbb{F}}_p) \to \mathrm{GL}(V)$ such that $\tau \subset \mathrm{Res}\,\bar{\rho}$.

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

3.5.2 Proof of the main result

We have come to the main result of the chapter. Recall the notation $U_\ell(N) = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)(N)$ for $\ell \neq p$, $U_p = \ker(\mathrm{GU}_g(\mathcal{O}_p) \to \mathrm{GU}_g(\mathbb{F}_{p^2}))$ 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 ρ, are the same as the systems of Hecke eigenvalues coming from algebraic modular forms (mod p) of level U and any weight ρ_Σ on the group $\mathrm{GU}_g(B)$.

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

(after tensoring with $\mathbb{E}_\rho$ and taking global sections) a map

$$\bar{r} : \mathrm{H}^0(X, \mathcal{I} \otimes \mathbb{E}_\rho) \to \mathrm{H}^0(X, \mathcal{I}/\mathcal{I}^2 \otimes \mathbb{E}_\rho).$$

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

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

which gives us a long exact sequence that starts with

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

If $r_1(\bar{f}) = 0$ then $\bar{f} \in \mathrm{H}^0(X, \mathcal{I}^2/\mathcal{I}^3 \otimes \mathbb{E}_\rho)$ and we can similarly consider $r_2(\bar{f})$, $r_3(\bar{f})$ etc. There exists some n such that $r_n(\bar{f}) \neq 0$. Let $f_S = r_n(\bar{f}) \in \mathrm{H}^0(\Sigma, i^*(\mathcal{I}^n/\mathcal{I}^{n+1} \otimes \mathbb{E}_\rho))$. Note that $\mathcal{I}^n/\mathcal{I}^{n+1} = \mathrm{Sym}^n(\mathcal{I}/\mathcal{I}^2)$ and that $i^*(\mathcal{I}/\mathcal{I}^2) = i^*(\Omega_X^1)$. Recall from §3.1.2 the Kodaira-Spencer isomorphism $\Omega_X^1 \cong \mathbb{E}_{\mathrm{Sym}^2\,\mathrm{std}}$. We conclude that $f_S \in S_{\mathrm{Res}((\mathrm{Sym}^{2n}\,\mathrm{std})\otimes\rho)}$. So our process associates to a Siegel modular form f of weight ρ a superspecial modular form f_S of weight $\mathrm{Res}((\mathrm{Sym}^{2n}\,\mathrm{std}) \otimes \rho)$ for some integer n depending on f. Moreover, since the restrictions r_i and the Kodaira-Spencer isomorphism are Hecke maps, we conclude that f_S is a Hecke eigenform with the same eigenvalues as f.

Now let f_S be a superspecial Siegel modular form of weight $\rho_S : \mathrm{GU}_g(\mathbb{F}_{p^2}) \to \mathrm{GL}_m(\overline{\mathbb{F}}_p)$. By applying Corollary 3.23 we get a rational representation $\bar{\rho} : \mathrm{GL}_g \to \mathrm{GL}_m$ such that $\rho_S \subset \mathrm{Res}\,\bar{\rho}$. By functoriality we get $S_{\rho_S} \subset S_{\mathrm{Res}\,\bar{\rho}}$. We know that the map

$$r : M_{\bar{\rho}\otimes\det^n}(N) \to S_{\mathrm{Res}(\bar{\rho}\otimes\det^n)}$$

is surjective for $n \gg 0$, and therefore there exists an integer k such that

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

is surjective. Since this map is also Hecke-invariant, we conclude from Proposition 1.2.2 of [AS86] that any system of Hecke eigenvalues that occurs in S_{ρ_S} also occurs in $M_{\bar{\rho}\otimes\det^{k(p^2-1)}}$.

So far we showed that the systems of Hecke eigenvalues given by Siegel modular forms (mod p) of all weights are the same as the systems of Hecke eigenvalues given by superspecial modular forms S_{ρ_S} of all weights. By Theorem 3.17 we know that S_{ρ_S} is isomorphic as a Hecke module to the space of algebraic modular forms (mod p) of weight ρ_S, and we're done. □

3.5.3 Agreement with the definition of Gross

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

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

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

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

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

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

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

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

$G \xrightarrow{\rho} \mathrm{GL}(V) \hookrightarrow \mathrm{GL}(V \otimes \overline{\mathbb{F}}_p)$. The map

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

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

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

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

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 φ 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 $v_\sigma := \varphi^{-1}(v e_{\sigma^{-1}})$. We have

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

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

Lemma 3.26. Suppose L/K is a finite Galois extension with Galois group G. The map

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

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

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

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

$$\sum_{i,j} c_{ij}\sigma_k(\alpha_i)\alpha_j = 0 \quad \text{for all } k. \tag{3.7}$$

Let A be the $n \times n$ matrix whose (i,j)-th entry is $\sigma_i(\alpha_j)$, and let c be the column vector whose i-th entry is $\sum_j c_{ij}\alpha_j$. Then the system (3.7) can be written as $Ac = 0$. But it is an easy consequence of independence of characters (see Corollary VI.5.4 in [Lan93]) that

$A \in \mathrm{GL}_n(L)$, therefore we must have $c = 0$, i.e.

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

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

Bibliography

[Ach98] Jeffrey D. Achter. *Stratifications on moduli spaces of abelian varieties in positive characteristic*. PhD thesis, University of Pennsylvania, 1998. Available at http://www.math.columbia.edu/~achter/.

[AS86] Avner Ash and Glenn Stevens. Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues. *J. Reine Angew. Math.*, 365:192–220, 1986.

[AZ95] A. N. Andrianov and V. G. Zhuravlëv. *Modular forms and Hecke operators*. American Mathematical Society, Providence, RI, 1995. Translated from the 1990 Russian original by Neal Koblitz.

[Cha86] Ching-Li Chai. Siegel moduli schemes and their compactifications over $\mathbb{C}$. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 231–251. Springer, New York, 1986.

[Del71] Pierre Deligne. Formes modulaires et représentations ℓ-adiques. In *Séminaire Bourbaki, exposé 355*, volume 179 of *Lecture notes in mathematics*, pages 139–172. Springer-Verlag, Berlin, 1971.

[Dem72] Michel Demazure. *Lectures on p-divisible groups*, volume 302 of *Lecture notes in mathematics*. Springer-Verlag, Berlin, 1972.

[DG70] Michel Demazure and Pierre Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Masson & Cie, Éditeur, Paris, 1970. Avec un appendice *Corps de classes local* par Michiel Hazewinkel.

[FC90]   Gerd Faltings and Ching-Li Chai. *Degeneration of abelian varieties.* Springer-Verlag, Berlin, 1990. With an appendix by David Mumford.

[Fon77] Jean-Marc Fontaine.   *Groupes p-divisibles sur les corps locaux.*   Société Mathématique de France, Paris, 1977. Astérisque, No. 47-48.

[Gro90] Benedict H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. J.*, 61(2):445–517, 1990.

[Gro98] Benedict H. Gross. Modular forms (mod p) and Galois representations. *Internat. Math. Res. Notices*, (16):865–875, 1998.

[Gro99] Benedict H. Gross. Algebraic modular forms. *Israel J. Math.*, 113:61–93, 1999.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52 of *Graduate texts in mathematics.* Springer-Verlag, New York, 1977.

[Kat73] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, volume 350 of *Lecture notes in mathematics*, pages 69–190. Springer, Berlin, 1973.

[Lan93] Serge Lang. *Algebra.* Addison-Wesley, Reading, MA, third edition, 1993.

[LO98]   Ke-Zheng Li and Frans Oort. *Moduli of supersingular abelian varieties*, volume 1680 of *Lecture notes in mathematics.* Springer-Verlag, Berlin, 1998.

[Mil86] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[Mil98] J. S. Milne. Abelian varieties. Lecture notes at http://www.jmilne.org/, July 1998.

[Oor66] Frans Oort. *Commutative group schemes*, volume 15 of *Lecture notes in mathematics.* Springer-Verlag, Berlin, 1966.

[Oor75] Frans Oort. Which abelian surfaces are products of elliptic curves? *Math. Ann.*, 214:35–47, 1975.

[SD73] H. P. F. Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, volume 350 of *Lecture notes in mathematics*, pages 1–55. Springer, Berlin, 1973.

[SD76] H. P. F. Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms II. In *Modular functions of one variable, V (Internat. Conference, Univ. Bonn, 1976)*, volume 601 of *Lecture notes in mathematics*, pages 63–90. Springer, Berlin, 1976.

[Ser87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[Ser96] Jean-Pierre Serre. Two letters on quaternions and modular forms (mod p). *Israel J. Math.*, 95:281–299, 1996. With introduction, appendix and references by R. Livné.

[Shi63] Goro Shimura. Arithmetic of alternating forms and quaternion hermitian forms. *J. Math. Soc. Japan*, 15:33–65, 1963.

[Shi79] Tetsuji Shioda. Supersingular $K3$ surfaces. In *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, pages 564–591. Springer, Berlin, 1979.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate texts in mathematics*. Springer-Verlag, New York, 1986.

[Ste63] Robert Steinberg. Representations of algebraic groups. *Nagoya Math. J.*, 22:33–56, 1963.

[Tat66]   John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*,
          2:134–144, 1966.

[Tat68]   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 Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of
          Lecture notes in mathematics. Springer, Berlin, 1980.

Index